In the Boxing Ring

Network Box 技術資訊

Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年10月刊的《In The Boxing Ring》

發佈了 Network Box NBRS-5.0 WAF+之後，我們收到很多關於傳統 IDS/IDP 系統和 Network Box WAF+區別的諮詢。兩者用來保護 web 伺服器哪一個更好呢？這個月的專題我們將來回答這個問題。

在第 5、6 頁，我們將詳細介紹本月發佈的 NBRS-5.0 週二補丁及 NBRS-5.0 路線圖的月度進度報告。

第 7 頁是本月補丁日發佈的 NBRS-3.0 改進的詳情。在可預見的未來幾年，我們將繼續 NBRS-3.0 的開發和支援，這一頁將讓您瞭解到我們核心產品的動態資訊。

最後，Network Box 很高興地的宣佈我們會在這個月底發佈新的 Network Box 5 硬體。新硬體將會支援 Network Box NBRS-5.0 UTM+ 和 Anti-DDoS WAF+系統。

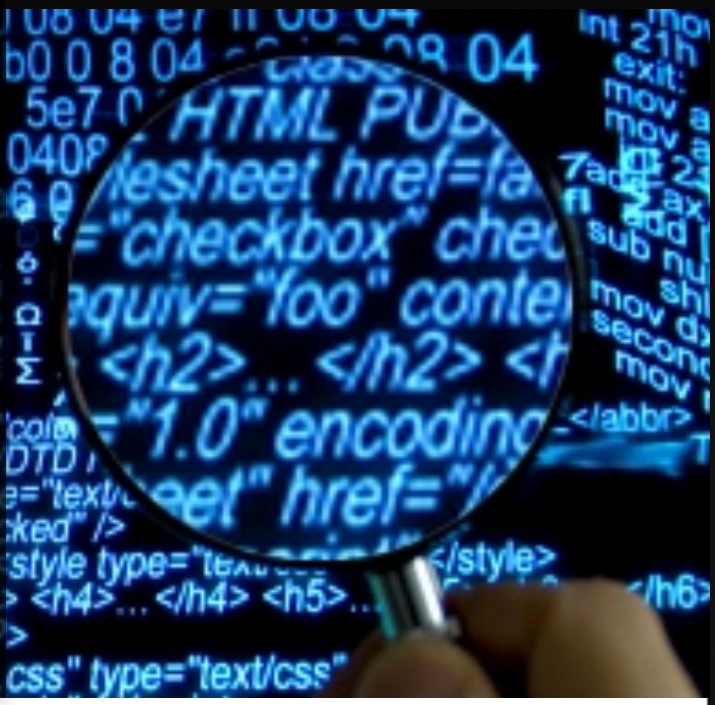
Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
October 2013

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社交網站對關注我們：

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 期 摘 要

IDS/IPS 對比 WAF



發佈了 Network Box NBRS-5.0 WAF+之後，我們收到很多關於傳統 IDS/IDP 系統和 Network Box WAF+區別的諮詢。兩者用來保護 web 伺服器哪一個更好呢？

這個專題文章將來回答這個問題

IDS/IPS 工作原理

入侵偵測/防禦系統工作在網路層，通常以透明的方式。它們接收網路包並嘗試重建這些包建立的通訊會話。它們可以提供高層協定解碼，但自己始終在網路層面操作。

在資料包層面，我們來看看一個典型的經 80 埠連接到 web 伺服器的 HTTP 會話。提取我們感興趣的一個會話，下面就是 IDS/IPS 系統在網路層面看到的：

```
09:35:57.858874 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [S], seq 893507093, win 65535, options [mss
1460,nop,wscale 4,nop,nop,TS val 3712851838 ecr 0,sackOK,eol], length 0
09:35:57.862643 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [S.], seq 2557492822, ack 893507094, win 42900, options
[mss 1430,nop,nop,sackOK,nop,wscale 6], length 0
09:35:57.862817 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 1, win 16384, length 0
09:35:57.862873 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [P.], seq 1:146, ack 1, win 16384, length 145
09:35:57.866990 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], ack 146, win 669, length 0
09:35:57.881756 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 1:1431, ack 146, win 669, length 1430
09:35:57.881881 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 1431:2861, ack 146, win 669, length 1430
09:35:57.881883 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 2861:4291, ack 146, win 669, length 1430
09:35:57.881904 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 2861, win 16205, length 0
09:35:57.881916 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 4291, win 16384, length 0
09:35:57.882176 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 4291:5721, ack 146, win 669, length 1430
09:35:57.882250 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 5721:7151, ack 146, win 669, length 1430
09:35:57.882252 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 7151:8581, ack 146, win 669, length 1430
09:35:57.882271 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 7151, win 16205, length 0
09:35:57.882325 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 8581, win 16384, length 0
09:35:57.882499 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [.], seq 8581:10011, ack 146, win 669, length 1430
09:35:57.882532 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [P.], seq 10011:11259, ack 146, win 669, length 1248
09:35:57.882550 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 11259, win 16216, length 0
09:35:57.883065 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [F.], seq 146, ack 11259, win 16384, length 0
09:35:57.886031 IP 74.125.128.147.80 > 10.8.2.100.65132: Flags [F.], seq 11259, ack 147, win 669, length 0
09:35:57.886067 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags [.], ack 11260, win 16384, length 0
```

首先是一個 10.8.2.100 -> 74.125.128.147 的 SYN 包，接著是回來的 SYN+ACK,接著是 ACK,這是傳統的 TCP/IP 連接的 3 次握手。然後是來來往往的 TCP/IP 資料，伴隨著確認包，還可能有一些重傳、重複包等等，這些都發生在 IP 層面。最後是一個 10.8.2.100 -> 74.125.128.147 的 FIN 包，接著是 FIN+ACK 和最後一個 ACK—到此 TCP/IP 連接關閉。

一個好的 IDP/IPS 系統會從網路層開始，嘗試重組資料包成資料流程（這裡指 TCP/IP 流）。一旦有了這個流和所已知的協定，系統會嘗試解碼協定資料。讓我們看看其中第 4 個包：

```
09:35:57.862873 IP 10.8.2.100.65132 > 74.125.128.147.80: Flags
[P.], seq 1:146, ack 1, win 16384, length 145
0x0000:  4500 00b9 f888 4000 4006 0000 0a08 0264  E.....@.@......d
0x0010:  4a7d 8093 fe6c 0050 3541 d616 9870 3e57  J}...l.P5A...p>W
0x0020:  5018 4000 d827 0000 4745 5420 2f20 4854  P.@..'..GET./.HT
0x0030:  5450 2f31 2e31 0d0a 5573 6572 2d41 6765  TP/1.1..User-Age
0x0040:  6e74 3a20 6375 726c 2f37 2e32 342e 3020  nt:.curl/7.24.0.
0x0050:  2878 3836 5f36 342d 6170 706c 652d 6461  (x86_64-apple-da
0x0060:  7277 696e 3132 2e30 2920 6c69 6263 7572  rwin12.0).libcur
0x0070:  6c2f 372e 3234 2e30 204f 7065 6e53 534c  l/7.24.0.OpenSSL
0x0080:  2f30 2e39 2e38 7820 7a6c 6962 2f31 2e32  /0.9.8x.zlib/1.2
0x0090:  2e35 0d0a 486f 7374 3a20 3734 2e31 3235  .5..Host:.74.125
0x00a0:  2e31 3238 2e31 3437 0d0a 4163 6365 7074  .128.147..Accept
0x00b0:  3a20 2a2f 2a0d 0a0d 0a                   :.*/*....
```

開頭是乙太網、IP 和 TCP 封裝，真正的資料從偏移量 0x0028 開始，包含下面的內容：

```
GET / HTTP/1.1
User-Agent: curl/
7.24.0 (x86_64-apple-
darwin12.0) libcurl/
7.24.0.OpenSSL/
0.9.8x.zlib/1.2.5
Host: 74.125.128.147
Accept: */*
```

這是個 HTTP 請求，對請求、頭部和參數都可以被 IDS/IPS 的高層協議解碼器解碼。

大部分 IDS/IPS 的麻煩是從應用層開始，這也是為什麼多數 IDS/IPS 止步於此的原因。應用層的編碼、傳輸非常複雜，傳統的 IDP/IPS 系統只到而不進入應用層。一個 IDS/IPS 系統可以看到應用流量但不能理解它。IDS/IPS 系統只是盲目的在原始包和重組的流資料包上應用特徵匹配，而實際並不理解這些資料本身。

WAF
工作原理

WAF 系統，比如 Network Box Anti-DDoS WAF+，是從 IDS/IPS 結束的位置開始的。Web 應用防火牆完整解碼 HTTP web 協定，並理解協定中請求和回應的意義。

這包括：

- WAF 操作流資料，並把相關聯的流一起處理（比如，從同一個 web 用戶端到同一個 web 應用的請求一起處理）
- WAF 系統不僅保護 HTTP 也保護 HTTPS 協定通訊。
- 特定 web 格式比如 HTML,JSON 和 XML 在 WAF 有對應的模組處理。
- 不像 SMTP、POP3、FTP 協定，HTTP 協定是用來傳遞應用的，而 WAF 理解傳遞過程和應用本身。
- web 請求可以包含頭部和主體，WAF 理解並完整解碼這些請求。不僅解碼頭部，WAF 可以解碼提交的表單字段和所附檔。
- 請求和主體可以被編碼成多種格式，WAF 都可以完全解碼。
- 主體可以進行進一步的分析（比如病毒掃描）。

比如，讓我們來檢查一個最近從荷蘭發到 www.network-box.com 的 web 請求。下麵是請求：

```
POST /phppath/php?-d+allow_url_include%3Don+-d+safe_mode%3Doff+-d+suhosin.simulation%3Don+-d+disable_functions%3D
%22%22+-d+open_basedir%3Dnone+-d+auto_prepend_file%3Dphp%3A%2f%2finput+-n HTTP/1.1
User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; tr-TR) AppleWebKit/533.20.25 (KHTML, like Gecko) Version/5.0.4
Safari/533.20.27
Content-Type: application/x-www-form-urlencoded
Host: www.network-box.com
Content-Length: 2634

(2,634 byte HTML form provided, but not shown)
```

不僅解碼頭部，WAF 可以解碼所附的表單甚至是表單字段。它發現了下列問題：

1. PHP Injection Attack - OWASP_AppSensor/CIE4 OWASP_TOP_10/A1 OWASP_TOP_10/A6 PCI/6.5.2 WASCTC/WASC-15 WASCTC/WASC-25 WEB_ATTACK/HTTP_RESPONSE_SPLITTING WEB_ATTACK/PHP_INJECTION
2. SQL Comment Sequence Detected - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
3. SQL Hex Encoding Identified - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
4. SQL Injection Attack: SQL Operator Detected - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
5. Blind SQL Injection Attack - OWASP_AppSensor/CIE1 OWASP_TOP_10/A1 PCI/6.5.2 WASCTC/WASC-19 WEB_ATTACK/SQL_INJECTION
6. SQL Character Anomaly Detection Alert - Repetative Non-Word Characters
7. Restricted SQL Character Anomaly Detection Alert - Total # of special characters exceeded
8. Detects MySQL comment-/space-obfuscated injections and backtick termination - WEB_ATTACK/SQLI
9. Detects SQL benchmark and sleep injection attempts including conditional queries - WEB_ATTACK/SQLI
10. Detects basic SQL authentication bypass attempts 2/3 - WEB_ATTACK/SQLI
11. Detects MySQL comments, conditions and ch(a)r injections - WEB_ATTACK/SQLI
12. Detects classic SQL injection probings 2/2 - WEB_ATTACK/SQLI
13. XSS Attack Detected
14. IE XSS Filters - Attack Detected

Web 請求頭和主體中共發現 14 種可疑屬性。

相對 IDS/IPS 系統在不理解具體請求意義的情況下使用基於單一的匹配結果實施阻止或允許策略，WAF 可以基於異常評分系統—類似垃圾郵件識別系統的做法，WAF 給每個檢測結果一個分數—並對會話基於總的異常檢測得分來實施允許或阻止策略。分數檢測可在 web 會話的 4 個部分進行（請求頭部，請求主體，回應頭部，回應主體）。

在上面的 web 請求實例中異常得分是 158 分（SQL 注入類 54 分，XSS 跨站腳本類 25 分），此請求因超過閾值 10 而被阻止（超過 15 倍）。

結論

那麼 IDS/IPS 與 WAF 的區別是什麼呢？簡單的說 IDS/IPS 系統工作在網路和應用層間而 WAF 完全工作在應用層中。IDS/IPS 可以提供有限的應用層協定支援，WAF 則精通於保護 web 協定和運行在這些協定上的應用。

IDS/IPS 可以為大量的協定提供保護而 WAF 則聚焦在 HTTP web 這一協定來提供完整的全方位保護。

Network Box 第 5 版
NBRS-5.0

2013 年 10 月 1 日星期二，Network Box 將發佈一系列週二補丁日更新和修復。這些改進主要用於支援新的 web 用戶端安全模組。

NBRS-5.0 特性
2013 年 10 月

我們這個月的主要工作是擴展和加強現有的安全模組，為接下來的 NBRS-5 UTM+服務包發佈作準備。各區域 NOC 會在接下來的 7 日內逐步實施這些更新。這個月為 NBRS-5.0 發佈了超過 50 項改進和修復，主要有：

- my.network-box.com 管理介面中 BOX 時區支援
- my.network-box.com 線上報告系統中支援詳細記錄查詢
- RAID 磁片陳列系統管理改進
- 允許特徵包單獨重新同步（也可全部同步）
- 擴展支援在配置變更旁可錄入管理注釋
- 為警告頁面和資訊提供自訂模版機制
- 新的統一隔離支持
- 支援跟蹤系統日誌資訊
- 擴展網路高可用系統
- 支持 box 自身發起連接的網路位址轉譯，同經過 box 的連接一樣
- 橋接模式下的代理支援基礎
- 擴展應用識別
- 改進代理系統記憶體管理
- 修正高優先順序掃描作業（比如 HTTP）的超時系統

在多資料情況下，上述變更不會需要重啟或影響正在運行的服務。但根據配置的不同，在某些情況也可能需要重啟設備，必要時您所屬的本地 NOC 會同您聯繫安排。

如您需要以上的進一步的資訊，請聯繫您當地的 NOC. 他們會安排溝通交流和部署。

Network Box Version Five
NBRS-5.0

NBRS-5.0
路線圖

我們現在進入了 NBRS-5.0 路線圖的上升階段。主要的開發工作已經完成，我們在做最後的開發，打包和剩餘安全模組的 beta 測試。

上個月的週二補丁日發佈了我們的 SURF SCAN 產品，包括 web 用戶端惡意軟體防護和內容過濾支援，完成提供完善的用戶端和伺服器內容防護功能。本月的週二補丁日，我們發佈了我們 NBRS-5.0 的應用識別框架的公開測試版。最近一個月我們將發佈我們的郵件掃描產品，之後是剩餘的其它模組，最終使 NBRS-5.0 達到並超過全功能的 NBRS-3.0 UTM+產品。一旦到達這個階段，我們會開始提供現有 NBRS-3.0 客戶升級到 NBRS-5.0 的服務。

NBRS 主要版本（NBRS-1.0,NBRS-3.0,NBRS-5.0 等）包括 5 年以上的長期支持，所以現在只是 NBRS-5.0 的開始。得益於 NBRS-5.0 新架構我們將提供一些非常令人興奮的新產品來說明我們提升您線上網路的安全。

1. 基本平臺

在 2012 年夏天，我們完成了 NBRS-5.0 基礎平臺和支撐架構的發佈。這成為一系列產品的代碼基礎，並構成了 NBRS-5.0 各產品的基礎架構。

2. WAF+

我們接著發佈了 Anti-DDoS WAF+服務包。這個服務包提供了一些原來 NBRS-3.0 所沒有的保護 DMZ 及雲基礎 web 伺服器倖免於互聯網攻擊新功能。它整合了網路防火牆，web 應用防火牆，DDoS 防護以及協議轉換（IPv4-IPv6/IPv6-IPv4 橋接）功能于一個服務包中。

3. SURF SCAN

為提供 web 應用防火牆，我們需要設計構建一個代理機制來理解 web 的 HTTP 協議。我們現在還在調整並將結合我們先進的掃描技術以構成下一代 NBRS-5.0 產品：SURF SCAN. 它將為基於 web 的用戶端流覽 Internet 上的 web 伺服器提供保護。它也將支援病毒防護及網站、內容分類，並提供豐富的報告功能。

4. APP SCAN

以上面為基礎上我們將發佈 APP SCAN，也是我們開發了一段時間的應用識別系統。通過獨立工作或者與 SURF SCAN 配合，APP SCAN 能夠在網路層面識別應用，在資料流程中提取中繼資料和內容。根據獲取的資訊實施病毒掃描和策略控制。

5. MAIL SCAN

到這裡，我們已經有了完善的 web 伺服器和 LAN 用戶端支持，我們將發佈我們的郵件伺服器防護產品 MAIL SCAN.它將提供對使用 SMTP,POP3 和 IMAP4 協定的郵件的掃描功能。

6. UTM+

通過發佈一系列安全模組來實現比如 QoS（服務品質控制），VPN，集群，HA 等最終完成 UTM+相應的功能。其中一些模組會在準備好時隨同之前的一些服務一起發佈。

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

NBRS-3.0 新特性

2013 年 10 月

2013 年 10 月 1 日星期二，Network Box 發佈了這次的週二補丁日改進及修復更新包，各區域 NOC 將會在此之後的 7 天內安排這些新功能的發佈和更新工作。這個月的更新補丁包包括：

- 修定 my.network-box.com 中 Web 代理/配置/策略下的組名顯示
- 補充完善 NOC 關於主備 DNS 配置
- iOS 推送通知系統性能改進
- Box Office 和支援系統的多種改進（多為內部）。

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

Network Box 5 發佈會

我們會在這個月底發佈新的 Network Box 5 硬體，以適配新的 NBRS-5.0 UTM+(統一威脅管理系統 Plus)和 Anti-DDoS WAF+(抗分散式拒絕服務攻擊 Plus)安全管理服務。新的系列硬體平臺將提供世界級的安全，極高的性能以及久級考驗的業務連續性。

SEPTEMBER 2013 NUMBERS

關鍵指標	資料	與上月差比（%）
PUSH Updates	543	+9.7
Signatures Released	518,028	-15.7
Firewall Blocks (/box)	900,198	-1.8
IDP Blocks (/box)	103,886	+4.4
Spams (/box)	16,854	-11.9
Malware (/box)	540	+3.1
URL Blocks (/box)	163,030	+1.7
URL Visits (/box)	3,335,801	+6.0

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