In the Boxing Ring

Network Box 技术咨讯

from Mark Webb-Johnson, CTO Network Box

歡迎閱讀2013年5月刊的 **In the Boxing Ring**

這個月，我們將會詳細地探讨分布式拒绝服务(DDoS)。对于DDoS， 正如对待大多数的紧急状况一樣（例如一次成功的駭客攻擊，或者網站的篡改）， 最好能事先做好預防準備。我們將探討針對DDoS攻擊如何做好相應的準備。

第四頁是這個月針對NBRS-3.0發佈的新特性和修復補丁的詳情。在未來幾年內，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。

同時這個月也是我們把NBRS-5.0归入发布周期的第一個月，我們將會在下個月（六月）開始報告NBRS-5.0的特性和和NBRS-3.0的增强功能.

Network Box技術總監,
2013年**5**月 **Network BOX**
Mark Webb-Johnson

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 期 概 要

如何成為一個 Prepper

（DDoS攻擊中的生存者）

分散式拒絕服務 (DDoS): 不可想像，IT管理員心中的恐懼。

Preppers: 生存者。積極作出應急準備的個人或團體。

當有人問起關於DDoS攻擊和 Network Box 對此可以如何更好地說明客戶，我總會給他們同樣的回答------“你的事前準備做的如何？”. 對於DDoS ， 正如對待大多數的緊急狀況一樣（例如一次成功的駭客攻擊，或者網站的篡改）， 事先做好預防準備是最好的選擇。試想這種攻擊的可能性，需要提前做好書面計畫如何應對這樣的攻擊，然後歸檔，當這種攻擊發生時可以按照計畫去應對。這就是“如何成為Prepper（DDoS攻擊中的生存者）”

攻擊的來源

對於你們的網路大多數DDoS攻擊都是外部的攻擊，內部攻擊是比較容易處理的（找出肇事者並且將其屏蔽），可是對於外部的攻擊卻很難去控制（因為不能輕易地找出肇事者，而當他用橫跨 100個國家的 10,000台不同的機器去進行攻擊時候，要將他遮罩非常困難。對於這樣外部的攻擊，你所能做的有： 一、讓他緩解下來（減少對你的網路提供服務的影響）；二、提供線索去識別攻擊的來源給到上級供應商和（可選）法律起訴。

外部攻擊一般而言分為以下兩種類型:

1. 偽造發件者源地址並試圖耗盡寬頻資源。

2. 不試圖欺騙發送者來源地址，而主要是拖垮輸出寬頻或資源。

雖然抵禦各種類型的技術截然不同，但是對於這樣的攻擊，規劃的方法是相似的。

拒絕服務你的互聯網服務提供者（ISP）

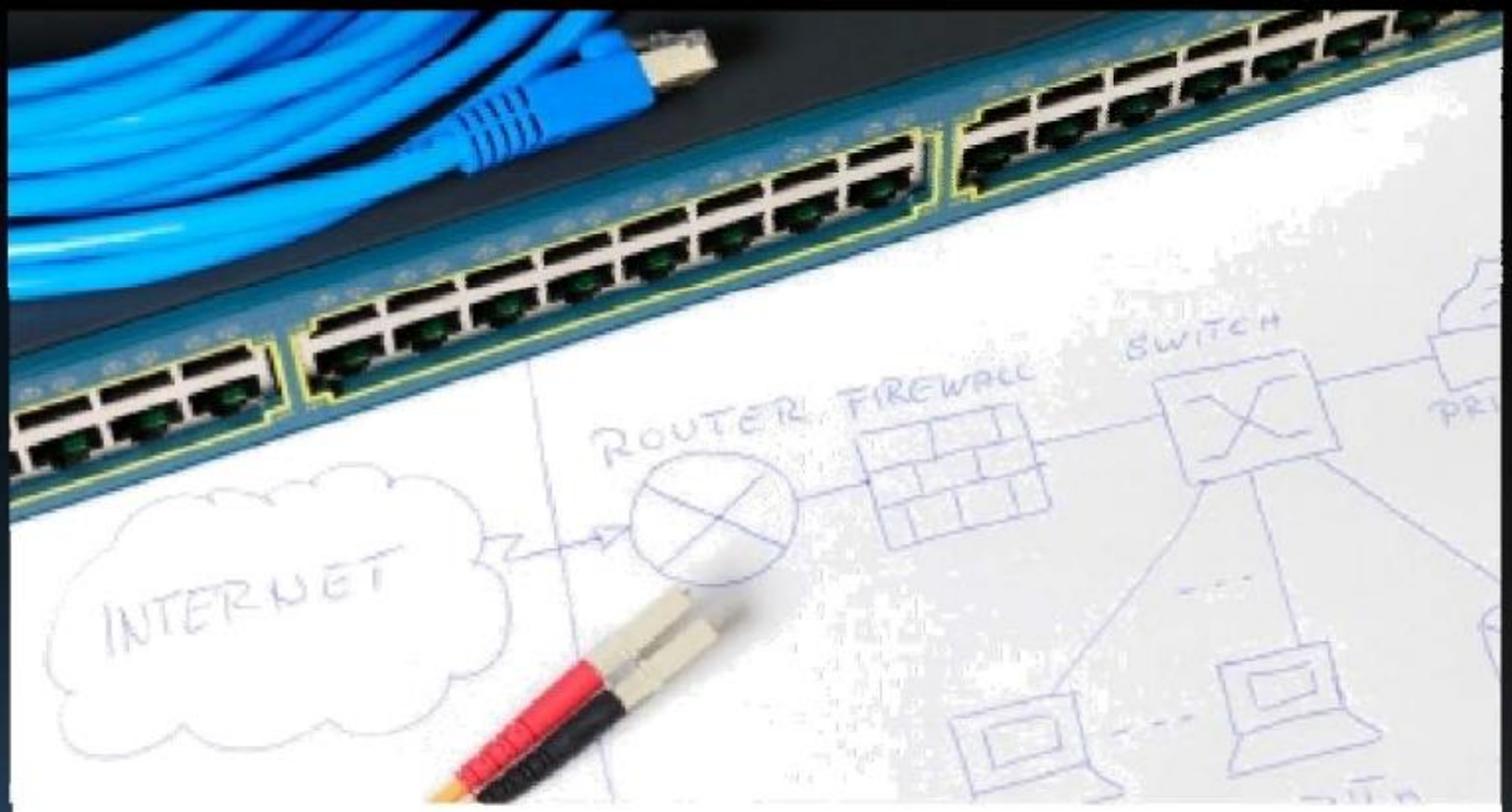
無論什麼樣的計畫，DDos緩解的第一步都是要和你的互聯網服務提供者(ISP)洽談。這些攻擊是來自他們的網路而對你產生威脅，有的ISP只關心自己的網路而不是說明你。ISP在上游網路對你實施封鎖（切斷你與互聯網的連接），這是前所未聞的事情。假如你的ISP真的這麼做，不管你對你的網路做什麼，儘管你把任何保護都落實到位了，你的ISP對你拒絕服務。

一個常規的ISP有以下規則：

· 第一次被DDoS攻擊的IP將會被封鎖至少一天

· 第一次攻擊隨後的三個月內，如果再次收到DDoS攻擊的IP將會被封鎖至少4天。

這些攻擊的IP位址（通常都是被攻擊者），並不是真正的攻擊者。如果你正在使用上述的ISP，當你第一次成為被DDoS攻擊的受害者時，你的網路會被斷開至少一天；從第一次攻擊隨後的三個月內如果再次收到DDoS攻擊，你的網路將被斷開至少4天。



所以,第一步規劃DDoS時要告訴你的ISP，並找出DDoS攻擊的策略環境。跟ISP確認狀態並和你一起解決,未經你明確許可不會阻止你的IP位址。

I P地址–
越多越好

下一步是看你已經分配的IP地址（或擁有自己，如果夠大）將提供什麼公共服務，對於這些已有的IP地址。儘量保持一個空閒的、大的位址集區，並為這些服務保持DNS TTL（DNS生存時間）記錄（如果有必要，允許你快速切換IP位址）。

通常，DDoS僵屍網路不遵循緩存DNS記錄的互聯網標准 他們將長時間的攻擊相同的IP地址，直到你切換到一個不同的IP。

分散式
服務

接下來,試圖分散你的服務。取決於那些你必須保持內部和那些可以卸載到一個不同的網路(或希望是多個不同的網路)。在不同的資料中心發佈你的服務,在遭受到攻擊時你能提供可用性。單一的服務如DNS也適合分佈(和UDP的基礎,很容易欺騙源或反射攻擊)。

資源
規劃

你的Web伺服器或防火牆需要使用50%的資源來處理網絡流量，剩餘50%的資源在遭受DDoS攻擊的情況下可能很快就消耗完了。你需要足夠的設備來處理攻擊請求，這跟平時是不一樣的。

這樣規劃可能是昂貴的，所以需要計算以確定什麼是合理水準的傳入請求和傳出答覆。你有可用的頻寬，你必須提供公開服務的複雜性。然後，用這些計算確定你需要什麼樣的資源能夠滿足請求量。

這不只是
關於BOX

DDoS攻擊的規劃不只是在你的網路前面放置BOX來防護DDos。如果你的ISP故障了或者上游寬頻被占滿，即使是最好的DDoS攻擊緩解設備也不會有很好的效果。

軍人有一句格言：提前計畫和準備可以預防較差的表現 ，堅持這樣的勸告可能節省你一天的時間。

一旦你的計畫到位，傳達給你的合作夥伴（互聯網服務提供者，安全和其他服務提供者），以及內部。然後，將檔存檔，應該在發生不可預料的情況時能找到並按計劃實施。

Network Box Certified ISO 9001 / ISO 20000 / ISO 27001 Security Operations Centre

2013 5月 特点

星期二，2013年5月7日，Network Box將發佈補丁進行改進和修正。各區域的NOC將在未來7天以分階段的方式推出新功能。這個月，NBRS-3.0，其中包括：

各種內部NOC系統的改進

各種Box Office支援系統（主要是內部）的增強

修正定期PDF報告系統中的網路輸送量。此前我們報告的是平均網路流量，通過所有網路介面，但這種情況導致的問題是，這些網路介面的配置，一但有介面斷開（無數據）就會降低平均值。這個月的修改是報告每個介面資料的總量。

在大多數情況下，上述變化應該不會影響到正在運行的服務。然而，在某些情況下（取決於配置），一些設備可能需要重啟。如果有必要您當地的NOC會安排聯繫你。

還要注意的是這個月是我們正在把NBRS-5.0引進到我們週二發佈補丁的第一個月。從下個月（6月）開始，我們將一起報告NBRS-5.0特點和NBRS-3.0的增強功能。

如果你需要以上任何的進一步資訊，請聯繫您當地的NOC，他們將安排部署和聯絡。

Network Box 2013國際資訊科技博覽

2013 4月13－16

Network Box參加2013國際資訊科技博覽展。 Network Box在HKICT被極力推薦，因為Network Box獲得了2013最佳商務（產品）金獎，Network Box抗DDoS攻擊的WAF+系統被授予2013年最佳商務大獎;。

PC3 白金品牌
2013 獲獎

2013年4月23日，Network Box獲得了PC3白金品牌獎。這是由公眾投票，使用線上投票系統獲得的。

APRIL 2013 NUMBERS

Key Metric	#	% difference (since last month)
PUSH Updates	654	+71.7
Signatures Released	444,621	-7.2
Firewall Blocks (/box)	951,342	+5.1
IDP Blocks (/box)	108,709	+1.7
Spams (/box)	16,347	+12.7
Malware (/box)	627	-30.7
URL Blocks (/box)	175,867	-10.3
URL Visits (/box)	3,598,943	-8.4

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