利用 Netflow 與 ARP 識別異常流量之簡易方法與設計

梁明章
國家高速網路與計算中心
liangmc@narlabs.org.tw

摘要

本文將說明 TWAREN NOC 因應 AIOps 學習所需，提出幾個從全網路流量中識別出異常流量的簡易方法，以產出可確定為異常的流量資料集用來教導 AIOps 軟體認識異常，加快學習，並以實作的難度與消耗資源的角度，從易到難逐步說明利用 Netflow 資料與 ARP 資訊識別異常流量的作法給各校網管同仁參考。

關鍵詞：AIOps、Netflow、ARP、異常流量。

1. 前言

TWAREN[1] NOC 的網管系統以自行開發為主，經歷十多年開發經驗，我們的網管系統早已涵蓋電路、設備異常的偵測、品質的監測等等，且在多年前就已經開始異常使用行為偵測的研究，由於 NOC 的角色定位，過往的研發多以「即時偵測、快速反應處理」為主軸，為了提供前述的多項網管功能，我們利用五十多台中階伺服器建構了大資料平台，結合傳統 SQL 與 NoSQL 共同打造整個網管體系，這些年我們的系統已經達成可以在大規模惡意行為發作十分鐘左右就自動察覺，並且自動觸發骨幹攔截機制丟棄封包，使惡意者的攻擊無法實際到達連線單位，不過目前我們只會自動封鎖大規模的惡意來源，對於 DDoS 的受害者我們不敢採取自動機制，因為不確定受害者是否願意被清洗或保護。

除了在骨幹層面的全域偵測與防守，我們也逐漸擴展研究如何協助保護連線單位，或是提供訊息給連線單位，以 Dashboard 或網頁報表圖表等方式呈現，甚至是告警。

然而，針對連線單位的這些偵測與保護，都需要額外的計算與儲存資源，TWAREN NOC 不可能持續擴充資源去支應，因此，我們想在本文中提出一些簡易的方法與構想，分享給連線單位網管，有興趣的學校網管或許能夠依此開發出一些自用的偵測系統，這是本文的目的之一。

近年來，AIOps (Artificial Intelligence for IT Operations，協助 IT 運作的人工智慧) 逐漸形成趨勢，然而如果把全部的網路流量都送給 AIOps 去學習卻不事先識別正常流量集跟異常流量集，將會使 AIOps 的學習很沒效率，甚至學不出有用的成果也極有可能，因此，若能先識別出已確定為異常的流量來餵給 AIOps 學習何為異常，由 AIOps 去掉異常之後再學習分類，然後人類再以經驗知識從結果再區分正常與異常，再回饋給 AIOps，可以讓 AIOps 進步得更快，所以本文將會重點說明，如何用比較容易，或者是代價成本較低的方法識別出異常流量，識別結果可以是 Netflow[2]資料，也可以是尚未被彙整統計的封包表頭資料，甚至也可以是最原始的封包流，就看採用的 AIOps 軟體能接受哪種輸入而定。以上就是本文的重點。

主要內容

本文會先從最容易識別異常流量的方法談起，也就是利用未使用網段的方法開始，其架構與方法最容易實現，而且識別出的流量就是確定異常的，不需要消耗太多的運算資源。接著，再逐步推進到已經使用的網段中，利用未使用的個別 IP 來識別出異常流量，這裡將涉及 Netflow 的查詢與運算，到第三階段，由於可能需要獲得、處理與保存 Gateway 設備的 ARP (Address Resolution Protocol，位址解析協定)[3] 資訊，比較難找到既有的軟體來用，本文會依照實現的難度逐步說明於後續章節。

1.1 利用未使用網段識別異常流量

骨幹 NOC，或是配發 IP 比較多的單位，例如 Class B 級的單位，手中必然會留有一些網段沒有配發使用，這些預留給臨時任務，或是預留給未來可能會來的新申請單位的網段，在尚未配發使用之前是空置沒有設定 Gateway 的狀態，正常情況下不應該有相關的流量產生，然而，因為整個單位對外網宣告的是 Super-Block-Nets 整塊網段，網路上有非常多惡意掃描、偵測與入侵的行為，只要目標涉及到這些未使用網段，他們就會流入到領域內來，換言之，只要這些未使用網段出現傳輸，就必然是異常流量，因此利用未使用網段來偵測並獲取異常流量，可說是最簡單且物美價廉的方法，而且這些會觸及未使用網段的異常行為，通常也同時會波及已經配發使用的網段，甚至可以考慮立即送給防護機制將此惡意來源封鎖，快速反應保護網路降低損失。

想獲取未使用網段的流量，如果只是想獲取 Netflow，那只需要週期性以未使用網段為目的位址當搜尋條件從 Netflow 資料中查詢即可獲得，這方法無論是骨幹 NOC 或連線學校只要是有收取 Netflow 資料的都能做，如此簡單就能獲得異常的流量資訊，可惜就是這種異常類別主要是大量掃描與探測類的行為，有所偏向不全面，然而這方法仍不失為最簡單的方式。

再來，週期性以未使用網段為來源位址從 Netflow 中搜尋，若是出現連線紀錄，那表示有人假冒偷用，這種行為必定是非法或惡意的，若是單位的網管人員，應該做進一步的追索，因為做此行為的機器通常是被駭客入侵操控的肉雞，盡早抓到盡早清除，避免在防火牆內繼續擴散感染，

追索方法須利用 Netflow 關聯回溯到最初始發的路由器介面，再來就是進入 LAN 端透過 ARP 查找，我們會在後面章節繼續說明 ARP。

上述方法雖然簡單易得，但因為只有 Netflow 資訊，不會保存入侵程式碼或惡意 URL 之類的訊息，若是想獲取進一步的封包，我們有建議的幾種架構方法，如下**圖 1**，為了節省 Router 珍貴的介面，我們可以利用一個802.1Q 的 Multi-Vlan port 連線一個 Switch，以下**圖 1**為例，接往 Switch 的連線切成三個 Vlan，然後 Switch 將 Vlan 分開個別指向下屬設備(Sensor，Honeypot，Sniffer…等等)，每一個 Vlan 訂為一個 netmask /30的 WAN 網段 (如下**圖 1**中的10.x.x.x/30)，WAN 的一端 IP 位址設定在 Router 端，如10.1.1.1/30，而 WAN 的另外一端 IP 位址則設定在 Switch 下接設備上，如 Sensor 的 10.1.1.2/30，然後在 Router 那邊用 Static Route 設定某個未使用網段，例如140.110.16.0/22 via 10.1.1.2，而 Router 再把這個 Static Route 轉宣告進 IGP (Interior Gateway Protocol，內部閘道協定)送給領域內其他內部 Router，但是不要對外宣告到互聯網取。在正常的網路設定情境，未配發網段的封包應該流去預設的垃圾桶 Router 然後消失，在本文則利用 IGP 內部路由的方式將未配發網段導向 Sensor、Sniffer 等分析器的 WAN port，這些分析器可以是 Netflow 產生器，也可以是 HoneyPot，也可以是資安設備，重點在於，一旦這些機器收到流量，就是百分百的異常流量，這些確定的異常流量，可以作為 AIOps 的訓練資料，比較敏感脆弱的單位甚至可以直接送訊號去觸發資安防護機制將此異常來源的封包全數攔截拋棄，這樣的自動反應保護機制算是相當快速。

而下**圖 1**中右側接往某 NPB 設備只是一個舉例，假設單位只有一台設備可以做這些任務，那自然沒必要特地接一台 Switch，直接接去該設備就好。

至於802.1Q 也非必要，直接將多個未使用網段通通靜態指向同一個 Next-Hop 也是可行的，下**圖 1**中特別舉例802.1Q 只是考慮到後端如果還要個別轉送封包到其他設備，那麼有 VLAN 切隔會比較好區分。

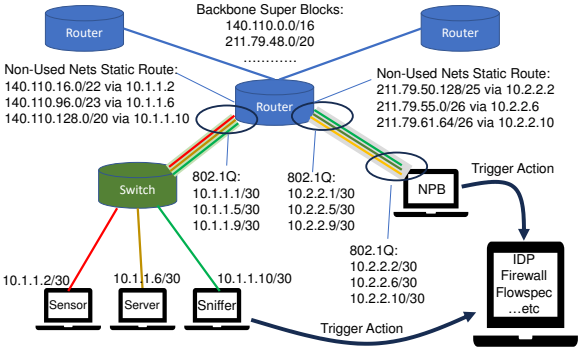

圖 1 利用未使用網段識別異常流量的架構圖

然而，利用未使用網段識別出來的異常流量，只能說是異常，並不一定是惡意行為，至少有三種非惡意情況，說明如下：

狀況一，本網內有惡意使用者(或被駭客操控的肉雞)以未使用的網段 IP 做來源位址對外傳送封包進行攻擊，而本網的網路設備如果沒有開啟 RPF (Reverse path forwarding，逆向路徑轉發)的檢查機制(RFC 3704)，就會允許這個不合法的來源 IP 封包通過並轉入骨幹傳送出去，實務上網路設備比較少去啟用這個檢查，因為對效能有影響。而被攻擊者收到來自這個不合法來源 IP 封包後做出的回應封包就會依循正確的路由指向一路繞送到上圖1的偵測環境被抓到，但此時抓到的封包來源 IP 本身是受害者，他並非惡意的真正來源，我們不能把這個遠方來源 IP 舉報為惡意者，也不該對他全網封鎖，因為它可能是個正常公開的服務伺服器。這種情況，我們必須先用這個被遠方回應連線的「未使用 IP」到骨幹 Netflow 資料中查詢是否有對外傳送封包的紀錄，如果有，表示真正的惡意者出在本網，需要更進一步的追索。如果查無對外連線紀錄，那麼遠方 IP 或是真的惡意者，也可能是下一個狀況二的類型，可以再輔以幾個判斷，例如遠方 IP 反查 FQDN、遠方 IP 的來源傳輸埠等等，這些比較細緻的推測我們在後面章節再說明。

狀況二，他網有惡意使用者冒用本網未使用網段 IP 傳送封包到受害者那邊，受害者的回應封包遵循正確路由繞送到本網來，這種狀況因為始發的惡意封包並未經過本網骨幹，Netflow 當然查詢不到，也只能輔用狀況一提的一些細緻推測，但終究無法百分百確認是否惡意。

狀況三，遠方 IP 是無惡意的調查機構，有些機構會進行廣泛的網路調查來蒐集數據，其行為其實跟惡意者沒太大差別，最多是頻率壓力會比較低，作為未被告知就莫名被調查的標的，其實把他們當作惡意者來處理也是情理之中。

基於上述三種狀況的考量，是否要做自動阻斷保護，需要進一步搭配更細緻的傳輸特徵輔助推測，將在本文後面章節做進一步說明。然而不管做不做自動阻斷保護，都不會改變它是異常流

量的結果，只是表示那個外界 IP 未必是惡意者，不過這種栽贓行為對連線單位學校來說並不會時常遇到，所以大部分時候可以不必考慮，除非是被壞人記恨上了。

圖 1的環境所抓到的封包，可以轉化為 netflow 資料進行保存，也可以只留下 Header 資訊做保存，這些資訊都可以餵給 AIOps 學習何為異常。

1.2 利用已配發網段的未使用 IP 識別異常流量

接下來我們針對已配發網段中的未使用 IP 來識別異常流量，方法蠻多種的，我們先從簡單到難的順序來說明幾種方式。

首先，依然是從 Netflow 開始，我們以週期性工作(例如五分鐘或一小時)，用已使用的網段 IP 範圍做來源 IP 查詢出 Netflow 並彙整出來源 IP 陣列 Ain(網段內 IP)以及目的 IP 陣列 Aout(外界 IP)不論這些傳輸是主動發起或被動回應，都表示當下這些網段內 IP 是使用中的。

再來，以該網段 IP 範圍做目的 IP 為查詢條件在相同時區間內取得 Netflow 並彙整出來源 IP 陣列 Bout(外界 IP)及目的 IP 陣列 Bin(網段內 IP)。

再來比對這四個陣列，我們就能獲得下列狀況資訊：

狀況一，Ain 陣列應該是 Bin 陣列的子集合，Ain 代表當時有使用的 IP，因此存在於 Bin 卻不在 Ain 中的 IP 就是對外無回應，或是當時未使用的 IP，究竟是哪種情況，可輔以 Gateway Router 的 ARP 資訊來判斷，我們後面章節再說明，但不論是哪種情況，都表示該 IP 並沒有對外界連線，因此外界主動來連線就屬於異常的行為，所以在這個時區間內連線這些 IP 的外界來源 IP 就可以識別為異常行為者，其流量也屬於異常流量。

狀況二，將狀況一識別出來的外界異常 IP 拿去跟 Aout 比對，若有符合，代表有內部 IP 回應給異常行為者，網管人員就應該追查該內部 IP 為何會回應，是否正常，這一檢查，往往可以抓出許多使用者沒做好的資安問題，尤其是現在很多單位都有防火牆之類的資安設備防護，實務上外界對單位的惡意掃描，理應被防火牆擋下，不應該產生內部 IP 對外傳輸的 Netflow，如果防火牆設定沒問題，確實有阻擋，那表示這些連線是內部 IP 主動對外發起的，那麼會主動連線已被識別惡意行為者的內部 IP，是否已被感染呢？網管或資安人員就可以進一步清查。

1.3 利用 Gateway 的 ARP 資訊輔助識別

在 LAN 領域內要識別內部 IP 是否有使用，最主要的資訊就是 Gateway Router 上的 ARP 資訊，因為內部 IP 若主動對外傳輸，封包一定要經過 Gateway，封包內的來源 MAC 位址會被 Gateway 記入 ARP 表格，若是外部先傳送封包要給內部網路，Gateway 也會先在 ARP 表格內查詢是否有目的 IP 的 MAC 位址，如果沒有就會發出 ARP 請求封包(ARP Request)，若接到回應(ARP Reply)就會把目的 IP 的 MAC 記入 APR 表格，因此查詢 Gateway Router 上的 ARP 表格，週期性獲取 Gateway Router 的適當方法是透過 SNMP (Simple Network Management Protocol，簡單網路管理協定) 去取得，如下**圖 1**。

```
$ snmpwalk TWAREN-XX-ASR9912-01 ipNetToMediaPhysAddress
IP-MIB::ipNetToMediaPhysAddress.485.211.79.XX.26 = STRING: 8:4f:a9:c9:d3:2b
IP-MIB::ipNetToMediaPhysAddress.485.211.79.XX.27 = STRING: 70:e4:22:19:86:f9
IP-MIB::ipNetToMediaPhysAddress.485.211.79.XX.29 = STRING: 0:0:0:0:0:0
IP-MIB::ipNetToMediaPhysAddress.485.211.79.XX.30 = STRING: b4:c:25:ef:40:4c
IP-MIB::ipNetToMediaPhysAddress.523.211.73.XX.1 = STRING: 0:0:0:0:0:0
IP-MIB::ipNetToMediaPhysAddress.523.211.73.XX.2 = STRING: 0:0:0:0:0:0
IP-MIB::ipNetToMediaPhysAddress.523.211.73.XX.3 = STRING: 0:0:0:0:0:0
IP-MIB::ipNetToMediaPhysAddress.523.211.73.XX.4 = STRING: 0:0:0:0:0:0

$ snmpwalk TWAREN-XX-ASR9912-01 ipNetToMediaType
IP-MIB::ipNetToMediaType.485.211.79.XX.26 = INTEGER: static(4)
IP-MIB::ipNetToMediaType.485.211.79.XX.27 = INTEGER: dynamic(3)
IP-MIB::ipNetToMediaType.485.211.79.XX.29 = INTEGER: invalid(2)
IP-MIB::ipNetToMediaType.485.211.79.XX.30 = INTEGER: dynamic(3)
IP-MIB::ipNetToMediaType.523.211.73.XX.1 = INTEGER: invalid(2)
IP-MIB::ipNetToMediaType.523.211.73.XX.2 = INTEGER: invalid(2)
IP-MIB::ipNetToMediaType.523.211.73.XX.3 = INTEGER: invalid(2)
IP-MIB::ipNetToMediaType.523.211.73.XX.4 = INTEGER: invalid(2)
```

圖 2 利用 SNMP 取得 Gateway ARP 資訊

不過 SNMP 的請求跟回應適合程式做處理，卻不太適合人類解讀，所以本文以 SSH 等 CLI 的指令回應做例子來說明，如下**圖 1**。

```
Via SSH: show arp

Address         Age        Hardware Addr   State      Type  Interface
211.79.XX.26    -          084f.a9c9.d32b  Interface  ARPA  TenGigE0/5/0/3
211.79.XX.27    02:49:04   70e4.2219.86f9  Dynamic    ARPA  TenGigE0/5/0/3
211.79.XX.29    00:00:04   0000.0000.0000  Incomplete ARPA  TenGigE0/5/0/3
211.79.XX.30    00:00:19   b40c.25ef.404c  Dynamic    ARPA  TenGigE0/5/0/3
211.73.XX.1     00:00:02   0000.0000.0000  Incomplete ARPA  Bundle-Ether60
211.73.XX.2     -          0000.0000.0000  Deleted    ARPA  Bundle-Ether60
211.73.XX.3     -          0000.0000.0000  Deleted    ARPA  Bundle-Ether60
211.73.XX.4     -          0000.0000.0000  Deleted    ARPA  Bundle-Ether60
211.73.XX.5     00:00:03   0000.0000.0000  Incomplete ARPA  Bundle-Ether60
211.73.XX.6     -          0000.0000.0000  Deleted    ARPA  Bundle-Ether60
211.73.XX.7     00:00:01   0000.0000.0000  Incomplete ARPA  Bundle-Ether60
211.73.XX.8     00:00:01   0000.0000.0000  Incomplete ARPA  Bundle-Ether60
211.73.XX.9     00:00:00   0000.0000.0000  Incomplete ARPA  Bundle-Ether60
211.73.XX.11    -          0000.0000.0000  Deleted    ARPA  Bundle-Ether60
211.73.XX.12    00:00:02   0000.0000.0000  Incomplete ARPA  Bundle-Ether60

Default expire: 4 hours
```

圖 3 利用 CLI 取得 Gateway ARP 資訊

首先我們先看上**圖 3**中最下面的「Default expire: 4 hours」，亦即此 ARP 內的每筆紀錄預設可存活四小時之久，網管們或許會奇怪，Switch 之類的 MAC table 的預設 Age 似乎都只有幾分鐘，為何此範例 Router 的會長達四小時之久，因為在 Switch 的角度來看，IP 有可能會經常變換上線的連接埠，例如跑 DHCP 的電腦教室，或是無線網路，因此 Switch 的 MAC 或 ARP table 的 Age 通常較短，而對 Gateway Router 來說，只要一台機器還在這個 LAN 裡面，他的實體連線位置無關緊要，只要 IP 對應網卡 MAC 不變就好，不管無線網路或是 DHCP 環境，IP 與網卡 MAC 對應的 ARP 資訊在正常情況下不會時常變化，因此，我們只要以每小時或半小時為周期從 Gateway 收集 ARP 資訊，原則上就足以。

接下來我們說明幾種對我們有輔助作用的資訊：

狀況一，如上**圖 3**中 211.79.xx.27 這個例子，其 Age 已經02:49:04，已存活兩小時多，且有 MAC 位址資訊，State 為 Dynamic 表示是透過 ARP Reply 學到或該 IP 主動送來封包時記下的，這是正常的例子。

狀況二，上**圖 3**中 211.79.xx.29 的 State 是 Incomplete 且 Age 已經00:00:04，也就是記入 ARP Table 中已經過了4秒鐘，其意思就是外界有封包打算送給 LAN 裡的 211.79.xx.29，所以 Gateway 發出 ARP request，等了4秒鐘還沒等到回應，在一個 LAN 中等4秒還沒回，通常是沒人會回了，所以這應該是目前沒被使用的 IP。

狀況三，上**圖 3**中 211.73.xx.2 的 Age 是個「-」符號，State 是「Deleted」表示已標註要刪除，而 MAC 資訊欠缺表示根本沒取得過，所以這也是一個未使用過的 IP，也就是狀況二等待到逾時之後的情況。

至於為何標註 Deleted 卻還在 ARP 中，那是因為 ARP Table 是 Router 共用表格，需考慮多工維護的各種規矩，例如共用鎖定等等，頻繁增刪紀錄很傷效能，標註為 Deleted 表示此位可覆蓋即可。

所以，根據上**圖 1**的例子，我們可以推測，當下正有外部的惡意行為在掃描探測 211.73.xx.0 這個 Class C 網段，導致 Gateway 被迫發 ARP Request 去詢問 MAC，卻沒一個有回答的，因此我們可確認這些沒獲得 MAC 的 IP 都是當下未使用，而企圖連線他們的外界來源 IP 就是妥妥的異常行為者，而這些外界 IP 可以透過同時區間的 Netflow 資料取得並且識別其 Netflow 或封包為異常流量，送給 AIOps 學習。

1.4 低頻率微小異常的識別

前文所提的方法主要用在即時或是短時間內就希望察覺的異常，但是前面所提到的那些資訊收集方法，如果能利用大資料平台儲存起來，是否能用來查找低頻率或微小的異常呢？這是有可能的，當我們針對某個連線單位用整天的 Netflow 以內部 IP 為基底做聯外 IP、傳輸協定、傳輸埠、封包數、Bytes Count 等資訊做統計分析，反向排名，就會發現一些有趣的事情，確實存在一些內部 IP，整天下來只會跟寥寥幾個外部 IP 進行連線，而且傳輸甚少，而那些外部 IP 也並非 Well Known 的服務。

在這些例子中，每個個例分開看，沒有明顯異常，但綜合起來仔細看，會發現某些外部 IP 重複了，而連線的來源與目的傳輸埠，傳輸的封包與量，有類似性，這些都有與 C&C 連線的可能性。

連線的協定、雙方傳輸埠、封包數、傳輸量這些綜合來看，也能展現一些訊息，舉個例子，假設某個內部 IP，大部分時間閒置，但會週期性以高位傳輸埠(大於32768)與外界 IP 發生傳輸，使用高位傳輸埠通常是 Client 端，若是 TCP 協定，只用一筆 Netflow 就傳過多個封包與 Byte 量，Netflow 的 TCP Flag 帶有 SYNC 旗標，輸出遠大於下載，基本上就是很明確的機械化扔資料包去給遠方，對於這種行為，網管其實已經可以去詢問該 IP 使用者這是否計畫中的自動化工作做確認了。

針對這些，未來我們將會嘗試送給 AIOps 進行分類，分類好再用經驗與知識來推測是否異常。

此外，活動太少了，其實也可能是異常，更何況基於資安的意識，非人類使用的機器其自動化的工作與連線應該被列管或掌握，閒置的機器應該離線或關閉，否則風險很高。不過因為目前研究人力有限，我們雖然意識到「量少」也是一塊相當有趣的研究方向，但是現階段也只能先送進大資料平台累積，當作未來研究資料，目前 NOC 仍會先以有助於骨幹維運的任務為首要。

參考文獻

[1] TWAREN，TaiWan Advanced Research and Education Network，台灣高品質學術研究網路，http://www.twaren.net/

[2] NETFLOW，https://zh.wikipedia.org/zh-tw/NetFlow

[3] David C. Plummer. RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware. Internet Engineering Task Force, Network Working Group. November 1982 [2017-09-14].