網管網路的安全存取與系統紀錄監控

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

摘要

本文將說明以軟體方式打造安全的異地多機房網管網路與遠端接入網管網路的安全方式，使用雙重身份驗證之後仍需監控登入與組態設定的變更以期快速察覺入侵與異常，最後提出一些 syslog 的保護與儲存方法。

關鍵詞：網管網路, 登入管理, 組態變更管理, syslog

I. 前言

TWAREN 骨幹網路原本就有很高的資安要求，近幾年更被定為國家重大基礎設施，接受更多的資安稽核，NOC 維運團隊花費更多精力強化網管安全，眾所周知的資訊安全三大面向 CIA：機密性、安全性、可用性，就是強化資安實作非常好的指引。

這些年資安議題越來越重要，相信許多學校的網管同仁也都被要求強化資安管理，因此我們也將一些可以公開的，簡單又容易達成的想法在本文分享，首先最重要的，自然是先打造比較安全的管理環境，尤其是遠端管理環境，畢竟這年頭誰也無法預料明天是否會突然確診或居家自主管理，為了自己可以遠端管理替自己所開的專用門，要如何防護才能降低被有心人士竊取利用的風險，這就是本文第一個重點。

這幾年，雙重身份驗證(Two Factor Authentication, 2FA)也是正當風頭，這是必然要做的措施，但是並非做了就高枕無憂，無論多好的資安手段，執行者只要是人類就會有疏失，總有一天會出錯，因此我們依然要思考被入侵之後能快速察覺的機制，這也是本文第二個重要議題。

由於第二議題主要以 syslog 作為資料來源，本文也會針對資訊安全管理系統(Information Security Management System, ISMS)非常關心的 syslog 安全管理方面提出一些心得分享。

II. 安全的網管環境與遠端安全存取

網路設備與伺服器的管理總是要靠人來操作的，幾乎都是透過網路連線，然而管理員或操作者也不可能總是待在組織辦公室走內網連線，總會有身在外地或家中需要遠端管理設備的需求。

網路設備與伺服器的管理連線方式不外乎 SSH、HTTP/HTTPS、TELNET 幾種方法，若對外直接開放 TCP 連線，被駭客發現後有可能面臨猜密碼的攻擊或被 Denial-of-Service (DoS)攻擊癱瘓，若利用防火牆或 Access-Control List (ACL)限制外部連線來源 IP，卻不夠彈性，臨時出差或是家用網路對外 IP 會變化的就會很困擾。

本文建議的方法是建立一個 Private Network，在單位內是一個獨立的 VLAN，使用 Private IP 網段，所有納管的設備或伺服器只在接入此 VLAN 的網路介面上開啟管理服務埠，其他外界可接觸到的網路介面(亦即對外服務的網路介面)都不開啟管理服務埠，這個 VLAN 可以不設 Gateway，如果設備管理模組有下載更新與網路校時的需求，可在此 VLAN 內設一個 NAT(Network Address Translation)服務來處理，以 NAT 做 Gateway 的好處是外界無法主動送封包進入 VLAN。

接下來就是要談管理員該如何以安全的方式從外界接入此 VLAN 中以登入設備了。

A. 保護網管資料與命令傳輸

接續前文，市面上有很多 SSL-VPN 設備都能達成需求，不過一般單位很少會為了設備管理員配備專屬的 SSL-VPN 設備，若與單位一般人共用 SSL-VPN 設備風險又比較高，因此本文以開源軟體 OpenVPN[1]來舉例如何搭建安全的管理員傳輸通道，同時也說明如果管理員管控的設備放置於多處異地機房又該如何延伸 Private 的網管網路。

參見“圖1”，假設管理員需要管理三個異地機房的設備，可以建構如“圖1”內的環境。

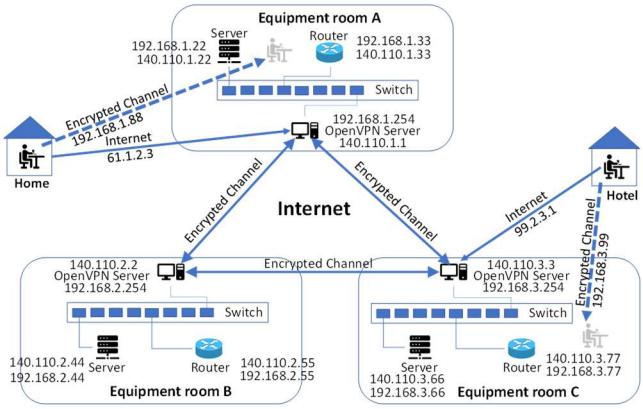

圖1. 多個異地機房網管網路示意圖

OpenVPN 可建構兩種模式的加密通道，如“圖1”內三地機房的三台 OpenVPN Server 之間使用的是點對點路由模式，作用類似於路由器，三地設備網管網段彼此間的傳輸可以透過本地OpenVPN Server路由到另外兩地，跨過網際網路的傳輸是加密的。這種模式的加密通道，VLAN 內的 ARP 等廣播封包不會走上加密通道，不會浪費頻寬在廣播封包上。如果需要管理的異地機房有很多個，建立 Fully-Mesh 的加密通道太過複雜，也可以採用雙核心或三核心的分群架構來減少加密通道數量。

身在外地的管理員電腦想連接三地的 OpenVPN Server 所建立的通道模式就是另外一種模式，類似 VLAN 的第二層傳輸模式，OpenVPN Server 會配置一個內部網管網段的 IP 給管理員端的虛擬網卡，因此管理員的電腦就彷彿移入單位內的網管網路中，只是這條虛擬通道是加密的，而且管理員可以連上任一地就能操控三地所有設備。

OpenVPN 的傳輸效能相當好，一般個人電腦或是VM(Virtual Machine)就足夠運行 Server 端，像 TWAREN NOC 使用的 OpenVPN Server 就只是運行在一個 VM 上就能服務十幾位管理員。既然是軟體，當然非對稱金鑰長度、資料傳輸用的對稱金鑰長度等都是可以自行設定長一點的，目前我們使用非對稱金鑰2048位元跟對稱金鑰256位元都能順暢使用。

B. 加強驗證安全度

一般 SSL-VPN 設備使用帳號+通行碼驗證，OpenVPN 以每個人獨立一組非對稱金鑰為基礎，私鑰可用通行碼加密保護，每次讀取都需要輸入通行碼以解密私鑰，以上措施似乎已經相當安全，然而，資訊安全最大的漏洞始終在於「人」而不是設備，管理員也是人，除非管理員能堅持只使用特定電腦去連線網管網路並且該電腦決不做其他事情(例如瀏覽外界網頁等等)，否則電腦總難免有感染木馬(例如看郵件就有風險)或被蠕蟲入侵(有接上網際網路)的風險，因此強烈建議利用2FA 來降低管理者電腦被入侵後造成的傷害，例如最常見的2FA 就是基於時間的一次性密碼(Time-based One-Time Password, TOTP)，既然我們無法保證管理員電腦的絕對安全，那只好利用2FA 並且強制管理員絕不能把 TOTP 的金鑰置放在電腦上，這樣萬一駭客已入侵電腦並且利用側錄畫面與鍵盤輸入的方法竊取到管理員所敲過的帳號密碼，自己去也會卡在隨時變化的 TOTP 而難以私下進入設備，請注意，在此僅說是「難以」進入而不是「無法」進入，那是因為對於真正有心的駭客而言，他可以在側錄到管理員敲下 TOTP 時立刻在同一個 Time-Window 內另行登入，這手段確實可行，很難預防與阻絕，但可以設法事後發現，本文後面章節會再說明，在此也提醒各位網管同仁，TOTP 的 Time-Window 千萬別設定太久，越久風險越高。

SSH 可以使用2FA，HTTP/HTTPS 沒有標準做法，只能各顯神通，OpenVPN 也能支援2FA，例如開源免費的 Google-Authenticator 函式庫[2]，並且可以做到每個人使用獨立的 TOTP 金鑰。

此外，因為要允許管理員不論身在何地皆可連線回來，SSL-VPN 的傾聽埠(UDP Listen-Port)勢必要開放全世界可連線，就有可能被猜測帳密或 DoS 攻擊，OpenVPN 針對這一點，設計可產生一把金鑰事先交給使用者，當 Client 端像 Server 發起連線申請時第一個封包就用這把金鑰加密，Server 端也直接用此金鑰解密，如果金鑰不對，Server 端解出來的「明文」當然是錯亂的看不懂，就不會回應而直接拋棄，並且不會等待下一動，這方式可以降低猜密碼風險，同時也降低被 DoS 時的效能傷害，這把金鑰同樣可以各個使用者獨立一把不必共用。

III. 監控管理

《孫子兵法》有云：「勿恃敵之不來，恃吾有以待之」，前面章節雖然提出建構安全網管網路與通道，並利用2FA 加強驗證，但終究不可能達成百分百不被入侵，畢竟資安最大的漏洞就是「人」，人不可能永不出錯，電腦系統也不可能永不出事，因此我們需要建置快速察覺異常的方法，才能快速矯正，本大章將舉例說明一些可用的機制。

A. 登入與組態設定變更的監控

由於 syslog 是事發當下就會即時發出的，所以就算駭客成功登入取得權限也無法消除已經發出去的 syslog，因此適合作為快速察覺登入與異變的訊息來源。現今網路設備通常有將 syslog 外送的能力，伺服器作業系統必然可外送 syslog，ISMS 就要求 syslog 必須進行異機儲存、保護與異地備份，一般來說，會將所有設備與伺服器的 syslog 統一送到一或兩台集中做後續處理，以 TWAREN NOC 為例，我們所有 syslog 都即時傳送給分發器進行一式多份複製後繼續派送(因為很多網路設備

僅能設定一個外送目標)，然後同時派送給第一階儲存、大資料平台、即時異常偵測系統，以及本小節要說明的登入與組態設定變更監控系統，下“圖2”是本系統的架構圖。

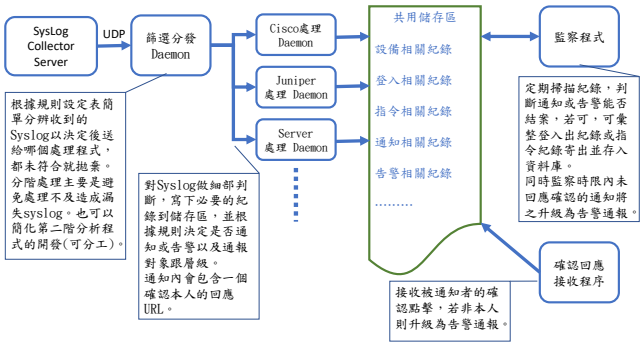

圖2. 登入與組態設定變更監控架構圖

系統本身並沒有什麼複雜的架構，第一個難點在於各款設備的 syslog 格式各不相同，即使我們只聚焦於「登入」跟「組態設定變更」兩個重點就要花費不少功夫來撰寫字串分析規則，好在分析規則是可以慢慢補完的，一款款設備逐步寫下去，總有完成的時候。

系統的第二個難點就是如何避免過度騷擾，如果一察覺登入或是變更就立刻告警通報，程式是最好寫的，但後果就是騷擾過度，導致被通知者煩到進行屏蔽或忽略，那麼系統就形同虛設，因此必須能自動區分嚴重等級，彙整同質的事件不連續告警，舉例來說，管理員一旦登入網路設備，通常因為發生事件，此時可能會多次登入一個或多個設備，因此在一個時段內的多次登入可以只通報第一次。此外，為防駭客側錄 TOTP 同步仿冒，在同一個 TOTP time-window 時間內同一管理員登入超過一次也需要通報此情況以策安全。以上說來簡單，但是事件的儲存方式就需要講究，畢竟每一筆 syslog 到達都得往前查找分析有無上述情況，處理時間大大增加，因此“圖2”的架構才會將原本一個階段就能做完的分析程序拆分成兩三個階段，就是擔心處理太久導致後來的 syslog 因為 UDP queue 滿溢而被拋棄。

系統的第三個難點就是事件通報後的追蹤與如何結案，為了避免過度騷擾，第一次通報原則上只通知該名管理員，接到通知的管理員應該判斷是否本人所為，若是，則僅記錄不告警，如果不是，就要立刻啟動資安事件通報流程。但是如果被通知者漏接、不回、甚至通知半路就遺失了，系統總不能等到海枯石爛，一個可行的方式就是在通知內含一個 URL 要求被通知者在時限內點擊該 URL 上網進行回報確認，超過時限則系統會將通知轉告警，提升通報層級(備援管理員或上級主管)，同樣也需要規劃好追蹤的儲存方式，回應確認的防偽機制等等。

此外，登入與組態設定變更顯然嚴重程度差很多，所以本系統在這兩種情況的處理等級必然有所差別，例如登入事件可以給予被通報的管理員比較久的確認等待時間，組態設定變更就不能等那麼久了。若事件發生在半夜，那肯定需要立即通報與確認，因為太過可疑。

最後，就是系統定期檢視所有未結案事件是否可以結案，如果某管理員已經一段時間沒動作，則將這段時間管理員的命令紀錄收集彙整 EMAIL 給管理員審查有無異常，既防備駭客混水摸魚同時也能糾錯，管理員查看後須轉寄給上級主管查核，作為最後一關保險，若有需要，也能內含一個主管專用的URL由主管點擊後進行確認以記錄到系統中完全結案，同時也能達成 ISMS 的多項要求(歷程證據、查核與監督)，一舉多得。

B. 週期排程作業的多重監督

網路與系統管理常常需要不少週期排程的任務工作，在 Unix 稱為 Cron-Job，在微軟 Windows 就稱為排程工作，一般管理員在安排 Cron-Job 之時，通常也會設計檢查程式運行的結果是否有錯、是否符合預期，但這樣的檢查一般就是在當台伺服器內自行檢查，有問題才通報。然而我們的經驗卻教訓我們「這樣是不夠的」，實務上總是出現各種意外導致系統的 Cron Daemon 本身就出現問題，而發生排程工作沒執行，自然也就沒檢查，更不會通報錯誤。

Cron 意外已遇過幾種，例如系統做了某些更新後導致 Cron 的執行環境出問題、還有 Cron-Job 執行帳號因通行碼過期而被系統拒絕執行 Cron-Job、以及因記憶體耗盡使 Cron Daemon 產生子程序的系統請求失敗等等，或許還有某些尚未遇過的事因在未來等著我們，但我們不能坐以待斃，即使預防不到，也要有快速察覺異常的機制。

我們的做法其實很簡單，既然本機自行監督可能出事，那就增加別機加入監督，將重要的 Cron-Job 執行程式改成 Shell Script 型態，如下所示：

```
*/5 * * * * update-database > update-database.log 2>&1
更改如下
*/5 * * * * update-database.sh > update-database.log 2>&1
```

而 Shell Script 內容則舉例如下：

```
#!/bin/bash
update-database > cron.log 2>&1
cat cron.log > /dev/udp/192.168.1.100/7777
cat cron.log
exit 0
```

如上 Shell Script 第三行的執行就會將 cron.log 內容以 UDP message 方式送到192.168.1.100的 Port 7777，因此192.168.1.100收到後可存成檔案，例如以發送者 IP 為檔名，而192.168.1.100則定期檢查各機送來的檔案內容與

檔案時間，若有超過週期仍未更新者，就告警通報該伺服器管理員，以上方法免費又簡單，不過 MS-Windows 就沒這麼簡單的傳訊方法了，或許需要自己寫個傳訊的小程式給排程工作傳訊用，當然，在192.168.1.100上面的稽查程式肯定是需要自行開發了，基本能力便是檢查檔案最後變更時間是否逾越週期，進階一些就是檢查特定的檔案內容複查 Cron-Job 的執行結果。

當然192.168.1.100這台負責稽查別人的機器也需要被稽查，方法也簡單，執行稽查排程的帳號也每日排程對192.168.1.100的管理員送一封 EMAIL 說早安，以表明自己的 Cron Daemon 正常運行即可。

C. Syslog 的保護、儲存與查詢

前文提過我們會將 syslog 集中送到分發器，我們使用 Samplicator[3]這個免費開源軟體來做複製分發器，此軟體除了可將收到的 syslog 複製多份轉發給多個 IP/Port 接收之外，最重要的是它可用參數「-S」要求將 UDP 封包的原始發送者 IP 複製成轉發封包的來源 IP，而不是執行 Samplicator 的伺服器自己的 IP，因此後續收到複製封包的各個處理程式都能從來源 IP 得知是哪個設備發出的 syslog，這功能非常重要，因為很多設備(例如 Cisco)外送的 syslog 訊息中並不包含自己的名稱與 IP，Linux 作業系統如果管理員沒設定好 syslog 程式的 configuration 也只會在訊息中自稱「localhost」，所以一旦失去 UDP 封包來源 IP 就再也無法判斷發送者是哪個設備。

ISMS 非常重視 syslog，必須實作 syslog 的完整性保護，不可被竄改且不可遺失，預防竄改的主要手段就是在 syslog 一產生就立刻送出且複製，不可遺失同樣也是依靠複製及異地儲存，為了可以保存得長長久久，我們需要高效率的壓縮以節省成本，我們使用7zip 來處理，使用它的主要原因是7zip 支援的壓縮演算法中有一個稱為 PPMd 的算法對於每一行都有類似格式且包含大量重複字詞的純文字檔具備極為高超的壓縮比與壓縮速度，很適合壓縮 syslog，舉例用法如下：

```
7z a -t7z -mx=9 -m0=PPMd:mem=1024m:o=32 -pXXXX asr.7z *
```

加密時設下密碼算是聊勝於無的保護，未來壓縮檔若被移到保護較差或是多單位共用的大型儲存空間時就能避免被其他人窺看或是竄改，因為想竄改就得先破解密碼解壓回原文才能改，也算是達成 ISMS 長期儲存的完整性保護。

IV. 結論與未來工作

前文說明了我們對於 TWAREN 的網管安全所進行的一些措施，基於資安的原因，我們僅挑能說的來說，很多細節不能說得太明，否則我們就有風險了。我們盡量以免費開源軟體或 Shell Script 來舉例，很多事情沒有經費也是能做的，至少能讓管理員減少小事變大事的風險，希望本文能對各校網管同仁提供一些幫助。

雖然說預防永遠勝於治療，然而誰也無法保證永遠不會疏忽，也許就被趁虛而入了。資安攻防除了是技術戰，更是心理戰，有心的駭客，一旦成功入侵有價值的目標，一定會盡力掩飾被他利用成功的弱點，或是粉飾太平避免被管理員察覺，或是放煙幕彈凸顯某些棄子弱點或棄子木馬給管理員抓到以掩飾更重要的弱點以及真正的木馬，因此我們與駭客之間的技術戰與心理戰仍要繼續下去，沒有人可以千日防賊，所以我們仍須繼續努力開發自動程式來協助我們防賊，例如，繼續加強入侵與異常的快速察覺項目的開發，盡力補完判斷規則，對於 ISMS 要求的「預防」與「矯正」兩個方向仍會繼續努力。

參考文獻

[1] OpenVPN, https://openvpn.net/community-downloads/

[2] Google Authenticator PAM module, https://github.com/google/google-authenticator-libpam

[3] UDP Samplicator, https://github.com/sleinen/samplicator/