FORTINET

白皮書

面對當今攻擊面的不斷擴大，傳統網路的分割 (Segmentation) 技術已經失效！

這就是為什麼營運首長跟網路工程師需要關注的原因

摘要

由行動化和多雲應用導致的攻擊面不斷擴大和零碎化，正在削弱網路工程師和營運首長維護企業網路效能、安全性、可靠性和可用性的能力。

不管是傳統的 VLAN 和 VXLAN 的網路分割技術或較新的 VMware NSX 和 Cisco ACI 的微分割技術，這些網路分割技術都是不够的，受網路架構的限制，它們比較像是戰術性問題，而非戰略性問題。它們通常也是靜態的，只允許曾經受信任的使用者、設備和應用程式來控制其允許的部分，而且它們缺乏對整個網路及高階第 7 層加密流層的全面可見性及安全防護，這往往是對於有效的風險管理是非常重要。

如果需要進行微分割的網路不執行內容檢查和執行，那麼它將會有安全問題的疑慮，如不防範，可能因此遭遇到橫向傳播的攻擊。[2]

網路分割是管理不同網路的解方嗎？

如果微分割的網路而不執行內容檢查，它可能會阻礙安全檢查，不利防堵橫向擴散攻擊。

典型的企業網路，使用者在地理上的距離越來越分散，連接到企業 IT 資源的設備與應用程式也是如此。當企業網路包含行動和物聯網 (IoT)，並在多個公共雲中採用了如 SaaS 應用，即使擁有強大的前端安全，也變得越來越難以保護。

這些不斷擴大、碎片化的攻擊面帶來的一個挑戰是，它們創造了一系列新的路徑，網路駭客可以透過這些路徑尋找攻擊目標。另一個問題是，威脅變的越來越複雜，它們會自動尋找和利用任何漏洞，使情況進一步複雜化的是，企業間的併購和收購活動可能導致在基礎架構的多樣化，讓不同部分之間的協調性與可視性變的有限。

在許多企業中，資安已成為一種被動的工作，因為 IT 部門無法檢測到遍佈網路設備與應用程式之間橫向移動的入侵，而更無法防止這樣的攻擊。

多年來，網路工程師們和營運首長透過分割他們的網路來因應這些挑戰。傳統 IP 地址和 vlan 的分割方式已經透過 VMware NSX 等微分割技術得到了補強，而利用思科設備的網路則是依賴實體交換機和 vxlan 的 Cisco ACI 分割。這些微分割技術允許由工作負載、應用程式或體系結構屬性 (如應用程式、數據和操作系統所在的虛擬機) 來定義存取的控制策略。為了滿足更細緻的分割，其他技術利用如端口、程序或運用主機的分割也在我們的討論中找到了方法。

這些傳統的分割方法，包括微分割，只使用防火牆功能來控制，而不執行深層的封包檢查來識別好壞流量。這將禁止未被授權的流量在區段之間移動。因此，當攻擊破壞了一個區段的網路安全時，這種方法不能阻止擴散到其他網路的橫向攻擊。

不幸的是，微分割並不是萬靈藥，不過這樣的想法仍是有意義的：將一個複雜的企業網路劃分成大量的小區段可以增加分割的可視性。但是，如果進行微分割的網路不執行內容檢查和安全執行，那麼實際上可能已妨礙安全維護，並允許攻擊的橫向傳播了。[1]

目前網路分割風險增加的3個原因

目前的網路分割技術有三個主要問題：

- **缺乏綜合的能見度**
  應用程式包括檢測未經許可的影子 IT、應用程式、系統設備，以及無法檢查加密流量以檢測隱藏的網路攻擊。
- **無法實現自適應信任 (Adaptive trust)**
  內部網路區段的存取控制從架構起來，這方法無法輕易適應不斷變化的網路需求，存取策略所依存的信任評估往往是靜態的，並且很快就會過時。
- **缺乏高階安全保護**
  由於缺乏從數據中心到網路前端的高階 (第 7 層) 安全保護，存取控制的有效管理無法實施，而且無法有效查看和控制這些組件。這些問題往往源自於網路工程師和運營人員在規劃分割網路的架構時對高階安全部份沒有給予足夠的重視。

了解每一個問題以及它們的綜合影響，可以引導出更明智的風險網路分割方法。

在很多情況下，網路的設計沒有考慮資安的設計與操作。IT 團隊未能將資安藍圖作為網路藍圖的一部分，結果就變成這兩者在 IT 螺旋中變成領導者和追隨者，而不是成為合作夥伴的角色，這種落差將在高度細分與越來越複雜的網路環境中加倍的增加，而實際上，這兩者有著重要且密不可分的關係的。[3]

能見度低導致巨大的盲點

客戶聲稱他們 72% 的網路流量是加密的，不過沒有完整的檢查就會造成一個巨大的盲點，模糊了能見度，並造成只檢查 28% 的部份。一個自然要問的問題是，如果沒有檢測可能隱藏在網路中的威脅，那如何建構一個有效的資安防護呢？

一個從下向上的存取控制設計

企業網路的設計大概是從企業發展過程中的需求所決定。管理誰和什麼內容可以存取哪些資源由業務策略、產業標準和政府法規來確定，再根據這些規則，網路團隊來進行配置路由器和交換機中的存取控制設置，允許用戶、設備或應用程式可以存取哪些特定的網路資源。

網路工程師和營運首長將立即認識到這種方法的兩個缺點，首先，企業的業務流程、合規需求和網路存取需求比其網路結構複雜得多，因此，很難使用網路架構為網路資源定義所謂的安全區段，讓所有被授權的用戶和應用程式同時來存取，而對其他用戶不開放存取。在實務中，因為在架構網路時，沒有預想到一些存取情境，會有一些不良的參與者利用這些安全漏洞進行攻擊，而隨著更進階、複雜的惡意軟體出現，這些漏洞早已出現在網路上了。

第二，隨著時間的推行，任何規定或企業組織都可能產生變化。因此，即使擁有了最新的資安系統，也必須面臨需要修改。而隨時這些變化，也產生許多安全漏洞的機會，更不用提很少有網路團隊能夠負擔得起重新佈置的時間和成本，更何況用網路架構來規劃安全分段的工作是非常困難的。

以物聯網現象為例，物聯網現象導致自動販賣機、電燈泡、咖啡機等智慧設備得到廣泛採用，因而豐富了我們的生活，不過您如何可以靈活地知道在這些多種多樣的設備中，如果有天被人拔掉一個設備並連上一台筆記型電腦，能確保沒有惡意行為的發生呢？

信任評估往往是靜態形式

為了有效地管理風險，網路工程師和營運首長需要掌握關於使用者、應用程式和網路資產的可信賴性的最新準確的資訊。它們的內部防火牆 (如果有的話) 或其他啟用或禁止網路區段之間流量的存取必須使用最新的信任數據。如果信任評估過時，分割技術在防止透過網路橫向移動的潛在威脅方面就會變得無作用。

由於網路資源的實際可信性會發生意想不到的變化，信任數據的品質是網路分割安全中迫切需要解決的問題。事實上 許多企業都對來自其信任的員工和承包商的攻擊感到吃驚。有超過三分之一的入侵跟內部使用者用關，29% 涉及使用者資訊被盜。[4]

一些企業對這些危險的應對方式是：鎖定他們的網路，不相信任何使用者或應用程式，並在允許存取之前建立驗證層。不過網路工程師和營運首長必須保護敏感資產，但不能給那些合法要求存取這些資產的人造成不必要的負擔。

如果沒有強制執行， 存取控制就變的沒有意義

如果網路缺少有效的安全基礎架構的關鍵元素，存取控制就不能像預期的那樣工作。傳統分割方法假設所有必要的網路安全組件都已就緒，可以執行 IT 團隊定義的存取控制策略。然而，這一假設可能並不成立，原因如下。

整體擁有成本 (TCO) 是企業可能沒有辦法投入防護的主要原因，例如，將一些較小攻擊面的網路區段不放在第 7 層安全的保護。由於預算原因或者部署需要太多資源，網路工程師和運營團隊可能對在所有需要的地方，如內部、正在運作的雲端、各端點與 IOT 等等設備部署防火牆或其他進階的威脅保護解決方案產生猶豫，也就會讓已經部署的安全設備可能無法完全發揮功能。一些網路管理團隊可能擔心成本會大幅增加，又想要優化網路效能，會故意關閉防火牆中的傳輸層安全 (TLS) / 安全共享層 (SSL) 的檢查。

以這種方式限制安全檢查，雖然可以幫助合法流量更快在各網段之間移動，但同時也為非法流量打開了大門。 以現在 72% 的網路流量都是經過加密的，[6] 網路駭客卻利用它來滲透網路並外洩資料，這是一個嚴重的問題。

如果沒有緊密地整合，安全組件的整體有效性就會降低，例如：您如何得知自己所管理的網路是否有人將 USB 插入到筆電中？缺乏一體化設計，這是無法知道的。

首先，當防火牆檢測到可疑流量時，可能需要幾個小時或更長時間，直到安全管理團隊收集到訊息並將其傳播到網路的其他部分。

其次，不同的安全解決方案無法共同工作，不能輕易共享威脅情報，無論是獲取的已知和最新出現的威脅情報，還是能發現新威脅的零日威脅情報。這可能是識別入侵威脅的平均時間仍然需要很高的時間的原因 (197 天) 之一。[7]

第三，企業不能有效反應減輕被檢測到的破壞的影響。如果在終端設備上沒有智能檢測機制、沒有分析使用者行為、沒有檢測未知攻擊 (即零日攻擊)，等到安全團隊著手處理時，可能已發生更大規模的破壞。

在這種情況下，認為分割網路得到良好保護的網路工程師和營運首長可能在錯誤的安全認知下工作。正在進行的端點到端點安全評估將告訴他們安全平臺的運行情況，以及他們的存取控制方法是否正確的實現了他們的想要的樣子。不幸的是，如果沒有端點到端點的全面可視性，還有檢測、主動威脅情報共享以及自動化的強制措施，就不可能進行可靠的評估，從而使許多網路工程師和營運首長無法準確報告企業的安全狀態。

結論

網路分割有其必要，但還是不夠。如果企業沒有將動態信任評估合併到各區段之間的存取控制中，那麼使用者和相關資產就容易受到牽連攻擊。同時，如果安全需求如果被效能考量取代，則網路分割可能會讓威脅減輕變的被動與無效。

為了實現一個強大的安全環境，網路需要足夠的可視性，能檢測到認可和非認可的應用程式，和擁有高階的第 7 層安全機制，以利執行和防止橫向的擴散攻擊。

這取決於網路工程師和營運首長，以便在這個攻擊面不斷擴展和碎片化的時代中，確保內部各區段的網路存取策略是足夠的。只有仔細注意分割設計，企業才能有信心挫敗企圖在網路中橫向移動的攻擊者。

未施行與注重相關的安全問題可能會產生可怕的後果，影響所及除了企業組織的營運外，對品牌的聲譽和財務安全也將造成長期的損害。

[1] Keith Townsend, "Get a Quick Primer on How Microsegmentation Can Improve Network Security," BizTech, May 26, 2017.

[2] Ibid.

[3] "Friction in the IT Helix: How to Create Harmony between Network Design and Security," Masergy, 2019.

[4] "2019 Data Breach Investigations Report," Verizon, accessed July 8, 2019.

[5] Omar Yaacoubi, "The hidden threat in GDPR's encryption push," PrivSec Report, January 8, 2019.

[6] John Maddison, "More Encrypted Traffic Than Ever," Fortinet, December 10, 2018.

[7] "2018 Cost of a Data Breach Study," IBM and Ponemon Institute, October 2018.

FORTINET

www.fortinet.com/tw

October 14, 2020 2:28 PM

744558-0-0-TW

wp-FA-traditional-segmentation-fails-842020