網路安全買家指南

製作可獲得成果的安全 RFP 權威指南

目錄

風暴正在形成

安全專家對很多事務的看法可能不盡相同，不過幾乎沒有人不同意威脅形勢正變得愈來愈嚴峻且複雜。考量 Unit 42 最近的預測，我們的內部團隊提供網路安全業界的威脅研究和前瞻性分析：[1]

- 在入侵發生之前修補弱點的時間持續縮短，從數天縮短到數小時。
- 發動攻擊所需的技能程度比以往還低，因為在暗網上取得預先建立的惡意軟體所需的成本低廉，而且容易取得。
- 經濟困難時期可能會導致更多內部人員願意探索與外部威脅行動者進行的潛在交易。
- 出於政治動機的事件，無論是所謂的駭客行動主義還是國家資助的攻擊，都可能導致以損害品牌而不是尋求經濟利益為目標的事件增加。

很顯然，為了降低風險並且為敏感資訊提供額外保護，加強網路安全措施的壓力愈來愈大。

網路安全趨勢

網路已經問世四十年，對於快速發展的網路安全性而言，四十年的時間顯得異常漫長，防火牆在這段時間發揮極大的作用。美國市場之前由於 COVID-19 而不景氣，但現在對防火牆的需求正以同比 23.5% 的速度成長，到了 2027 年市值將達到 160 億美元以上。[2]

這個數據其實不足為奇。新世代防火牆 (NGFW) 作為目前最先進的技術，仍然是網路安全性的基石。其中一項關鍵原因是新世代防火牆的多功能性：其實，現在的新世代防火牆是可以提供全方位安全服務的安全平台，這些服務已經不像以往一樣需要個別的設備，例如入侵防禦、URL Filtering、行動安全性和 DNS Security。此外，新世代防火牆現在有多種形式，包括硬體和軟體，因此，採用防火牆技術建立安全解決方案比以往更加的容易。

有鑑於新世代防火牆對網路安全性而言相當重要，採購防火牆的責任相當重大。本指南能夠協助您制定提案徵求書 (RFP) 以確保採購成功並實現較高的投資報酬率。本指南的主體按照安全類別 (例如存取控制、雲端安全性和加密) 的字母順序排列。對於各個主題，本指南會解釋挑戰以及因應這些挑戰的一般方法。此外，您會找到各個類別的範例問題，以便您可以根據您的採購進行調整。

在了解類別內容之前，讓我們概略了解影響網路安全性和新世代防火牆的重要網路安全趨勢。

軟體防火牆成為注目焦點

現代數據中心極度虛擬化，防火牆也呈現這種趨勢。相較於實體防火牆，軟體防火牆 (例如虛擬防火牆和容器防火牆) 具有相當大的優勢。例如，軟體防火牆在現有伺服器上執行，因此不會造成數據中心的額外負擔。軟體防火牆容易安裝和升級，可以從集中位置進行管理。彈性是另一個關鍵原因，因為軟體防火牆可以部署在任何需要的地方，不像實體防火牆必須駐留在網路中的關鍵流量點。

硬體防火牆會過時嗎？完全不會。實體新世代防火牆設備仍然是網路安全性的主力，因為硬體設備的容量比虛擬設備還高。全面的企業安全性需要硬體和軟體防火牆在不影響效能的情況下儘可能提供保護。

此外，一種新型的軟體防火牆正在興起，也就是容器防火牆。容器防火牆由 Palo Alto Networks 推出，能夠與 Kubernetes 環境原生整合，解決雲端原生容器應用程式開發和保護的一些安全挑戰。請持續注意新世代防火牆的這種全新趨勢。進一步了解。

1. *2022 Unit 42 Incident Response Report*，Palo Alto Networks，2022 年 7 月 26 日，https://start.paloaltonetworks.com/2022-unit42-incident-response-report。
2. *Network Security Firewall Market Research Report by Component (Services and Solution), Type, Deployment, End-User, Region - Cumulative Impact of COVID-19, Russia Ukraine Conflict, and High Inflation - Global Forecast 2023-2030, Research and Markets*，2023 年 1 月，https://www.researchandmarkets.com/reports/5470743/network-security-firewall-market-research-report。

零信任正在流行

最近的三個趨勢 – 移轉到雲端、混合工作模式的興起以及進階威脅的成長 – 對安全業界滿足客戶需求的能力提出挑戰。業界的反應是推出更多工具 – 在某些情況下，針對每種威脅推出一種工具。這種方法完全不可能正確 – 迫切需要更有組織而且永續的網路安全方法。

採用零信任，這是顛覆傳統安全性的架構理念。零信任的關鍵是用持續驗證取代隱性信任。在零信任架構中，信任是透過在數位互動的各個階段持續驗證來實現。另一種看待零信任的方式是無狀態安全性，這表示過去的驗證不影響未來的安全測試 – 永不信任，持續檢驗。除了提供更嚴格的安全性之外，零信任也具有簡單性的額外優勢。無論情況如何，您基本上都在執行相同的安全措施 (見圖 1)。深入了解零信任。

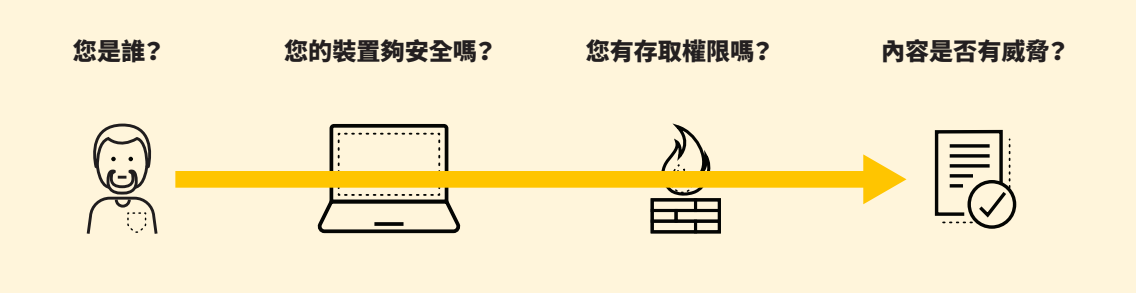


圖 1：零信任實際應用的簡化描述

機器學習重新定義新世代防火牆

正如您一定會打開引擎蓋 (或通風孔蓋，如果您住在英國) 檢視之後才買車一樣，了解驅動新世代防火牆的關鍵技術很重要。對於 Palo Alto Networks 的新世代防火牆，您會感到驚喜 – 機器學習 (ML) 是我們所有防火牆的核心。機器學習是人工智慧 (AI) 的一種應用，其中的機器會分析大量數據，在數據中發現有意義的模式，並且根據這些模式建立演算法，最後隨著時間持續穩定運作。

透過識別已知威脅和模式的變體、預測攻擊的後續步驟，並且在整個企業內幾乎即時自動建立和採用防護措施，Palo Alto Networks 的新世代防火牆使用機器學習來保持對攻擊者的領先優勢。Palo Alto Networks 的機器學習式新世代防火牆使用內嵌機器學習模型來協助防止先前未知的攻擊，這種攻擊很容易規避特徵碼型的安全措施。「內嵌」部分很重要，因為這可以確保在不影響輸送量的情況下快速地回應零時差威脅。機器學習是重要的差異化因素，Palo Alto Networks 推出的防火牆正因為這一點而與同類型產品截然不同。深入了解機器學習。

雲端交付安全服務支援快速回應

網路安全性是一場競賽，防禦者與積極且具才能的攻擊者進行較量。攻擊者擁有先發優勢，他們可以任意地選擇時間和地點發動攻擊，而且攻擊呈現多型態，能夠修改已進行的入侵而改變本身的特徵碼，已知威脅因此變成未知威脅。請記住，只需要一次得逞的入侵就足以危害您的網路。

在克服零時差威脅的競賽中，我們的新世代防火牆完全可以因應挑戰。他們使用特徵碼型的防護來阻止所有已知威脅，也使用雲端交付安全服務 (CDSS) 這種獨特的程序來偵測未知威脅。結合從多個來源收集而得的威脅情報，Palo Alto Networks 方法提供業界最快速的保護。深入了解雲端交付安全服務。

圖 2：Palo Alto Networks 新世代防火牆的典型回應時間

AIOps 簡化網路安全營運

隨著企業的擴張和威脅形勢的演變，公司也開始投資新型且昂貴的網路安全設備和工具來支援他們日益增長的基礎結構並防禦威脅，以維護一個安全的工作場所。不過，僅憑這些投資並不能保證效率或帶來可觀的投資報酬率 (ROI) – 網路營運也發揮應有的作用。許多安全團隊並不知道設定各種功能的最佳實務為何，因此無法有效地最大化其安全功能，也缺乏關於錯誤設定的見解。這將導致安全狀況出現落差並且造成極大的洩露風險。

IT 營運人工智慧 (AIOps) 可以提供協助。AIOps 結合大數據和機器學習來自動化 IT 營運程序，其中包括事件關聯、異常偵測和因果關係判斷。Palo Alto Networks 推出業界首創以網域為中心的新世代防火牆 AIOps，能夠在業務遭受衝擊之前預測、判讀及解決問題，重新定義防火牆運作體驗。

新世代防火牆 AIOps 讓安全團隊可以根據最佳實務和設定建議來最佳化動態環境的設定，進而持續改善安全狀況。其還可提供透過機器學習式異常偵測，並且針對整個部署的健全狀況和效能提供可採取行動的見解，讓網路安全營運團隊變得更具有主動性。新世代防火牆 AIOps 會主動解決目前最主要的營運挑戰，包括錯誤設定、人為錯誤、最佳實務的合規性、資源使用、硬體和軟體故障等等。深入了解 AIOps。

依據新世代防火牆類別的要求

本節按照安全類別的字母順序排列。各個部分將介紹該類別中的挑戰和一般解決方案要求。此外，您也會發現各個類別的典型 RFP 問題，您可以在防火牆採購中提出、調整和因應這些問題。

存取控制

挑戰：識別使用者並提供適當存取權限

問題

員工、客戶和合作夥伴 (也就是您的網路使用者) 連線到網際網路以及您網路中的不同資訊儲存庫。為了保護這些裝置，您必須能夠識別使用者並評估使用者裝置 (受支援和不受支援) 的風險。

網路使用者會持續存取不同實體位置的資訊，並且使用多個裝置、作業系統和應用程式版本。由於 IP 位址的性質，安全政策不會自動地跟隨使用者，因此會出現弱點。

目錄型的存取策略完全按照個人的角色來確定權限。不過，準確的風險評估必須包括行為特徵，例如風險或惡意活動。因此，目錄型的系統無法有效因應或降低風險。

解決方案要求

只有整合來自多個來源的資訊並根據角色以外的因素將風險指派給使用者的新世代防火牆才能因應這種挑戰。典型的資訊來源包括虛擬私人網路 (VPN)、無線區域網路 (WLAN) 存取控制器、目錄伺服器、電子郵件伺服器和網頁驗證入口網站，藉以確定哪些人在使用各個應用程式以及他們是否在散佈威脅。

此外，新世代防火牆必須使用基於使用者或使用者群組 (傳出或傳入) 授予存取權限的政策嚴格管理存取權限，例如僅允許 IT 部門使用 SSH、Telnet 和 FTP 等工具。無論使用者身在何處 (總部、分公司或家中)，而且無論使用何種裝置，新世代防火牆也必須確保政策都會跟隨使用者。最後，新世代防火牆必須根據新的入侵指標 (IOC) 等資訊動態變更使用者存取政策，或者需要對一組使用者授予臨時的存取權限。

進一步了解。

RFQ 問題

您的新世代防火牆能否：

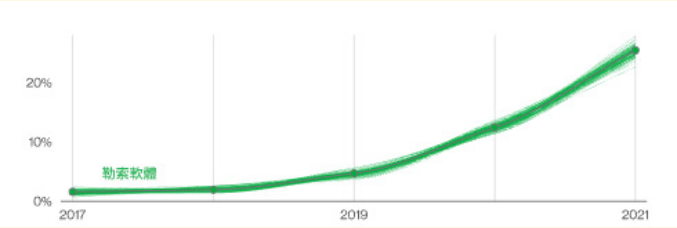
- 從多個來源收集風險相關資訊？
- 支援使用者型 (而不是位置型) 的政策？
- 即時變更政策以回應新資訊？

進階威脅防禦

挑戰：阻止進階威脅，防禦網路攻擊得逞

問題

勒索軟體攻擊正在加速 – 2021 年勒索軟體攻擊增加將近 13%，增幅是過去五年的總和。[3]



來源：Verizon

大多數現代惡意軟體，包括勒索軟體變體，都使用先進的技術來規避偵測。攻擊者採用掃描有效使用者活動、系統設定和特定虛擬化技術指標的技術。例如，惡意承載可以嵌入到合法檔案中，藉以透過網路安全裝置和工具發動攻擊或入侵。

結果就變成一場貓捉老鼠的遊戲，造成安全系統過度負荷。

這還不是最糟的情況。入門技術門檻不斷降低。幾乎任何人都買得到隨插即用威脅技術，藉以規避基於惡意軟體分析的安全措施。

解決方案要求

正確的新世代防火牆必須具備機器學習式內嵌分析和防禦方法來偵測未知威脅。藉由這些工具，新世代防火牆可以使用行為分析識別網路攻擊生命週期內所有階段的威脅，並且根據傳出通訊模式分析來探索命令與控制 (C2) 活動。

此外，新世代防火牆必須能夠阻止對惡意 URL 的存取，以免您的網路遭到入侵，並且必須能夠使用雲端交付的安全執行來進行快速擴展。

為了因應持續變化的開發方法，現代防火牆必須能夠支援 DevOps 和 Kubernetes 環境，並且運用這些技術提供的機會。自動化對於減輕忙碌的安全人員所承受的負擔極為重要。

進一步了解。

RFQ 問題

您的新世代防火牆能否：

- 提供機器學習式防禦來阻擋未知的惡意軟體檔案和變體，包括利用 PowerShell 等指令碼的可執行檔和無檔案攻擊？
- 提供內嵌機器學習式防禦來阻擋惡意網站攻擊，包括 JavaScript 和憑證網路釣魚攻擊？
- 阻止來自未知應用程式和 URL 的可執行檔和其他有風險的檔案類型？
- 以自動和動態的方式將所有已知的 IOC (也就是 IP、網域和 URL) 匯入封鎖清單？
- 對於 URL 篩選數據庫的惡意軟體類別中與勒索軟體有關的惡意 URL，與威脅情報整合以支援動態更新？

您的雲端式惡意軟體分析系統是否：

- 使用自訂程式碼的超級管理器有效防範可感知沙箱的惡意軟體？
- 建立威脅防禦特徵碼，例如 1) 內容型的防毒特徵碼，用於防禦惡意軟體的已知和未知變體，以及 2) 模式型的反間諜軟體特徵碼，用於偵測與已知和未知 C2 基礎結構的通訊？
- 支援 Windows、Android、Linux 和 macOS 作業系統的惡意軟體分析？

您的雲端式惡意軟體分析系統能否在做出裁定之後即時發佈特徵碼？

3. *2022 Data Breach Investigations Report*，Verizon，Verizon，2022 年 5 月 24 日，https://www.verizon.com/business/resources/reports/dbir/2022/summary-of-findings/。

應用程式啟用

挑戰：安全地啟用所有應用程式和控制功能

問題

應用程式 (例如即時傳訊應用程式、對等檔案共用和網路電話) 通常在非標準連接埠上執行。此外，使用者也可以從許多裝置和位置存取各種類型的應用程式，包括軟體即服務 (SaaS) 應用程式。一些使用者愈來愈精明，想要透過 RDP 和 SSH 等通訊協定強制應用程式在非標準連接埠上執行。

新應用程式為使用者提供豐富的功能集，有助於確保使用者忠誠度，但可能代表高風險狀況。例如，Webex 是一個非常有用的業務工具，但是使用 WebEx Desktop Sharing 從外部來源控制員工的桌面可能會違反內部規則或規定。Gmail 和 Google Drive 是很好的範例。使用者登入 Gmail (可能政策允許使用) 之後，他們可以輕鬆切換到 YouTube 或 Google Photos (可能政策不允許使用)。

安全管理員需要完全控制這些應用程式的使用，並設定政策來允許或控制某些類型的應用程式和應用程式功能，同時拒絕其他類型。

解決方案要求

新世代防火牆預設必須始終按照所有連接埠上的應用程式將流量分類，而且不會導致員工研究每個應用程式使用的通用連接埠而造成負擔。防火牆必須提供應用程式使用的完整可視性以及了解和控制應用程式使用情況的功能。例如，應該了解應用程式功能 (例如音訊串流、遠端存取和發佈文件) 的使用情況，並且能夠對這些使用實施精細控制，例如上傳與下載權限、聊天和檔案傳輸。

流量分類必須是連續的程序，因為這些常用的應用程式會共用工作階段並且支援多項功能。如果工作階段中引入不同的功能或特性，防火牆必須再次執行政策檢查。透過持續的狀態追蹤來了解每個應用程式可能支援的功能以及相關風險，是新世代防火牆必須具備的功能。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 防禦使用非標準連接埠、連接埠跳躍或錯誤設定來規避偵測的應用程式？
- 使用 UltraSurf 或加密 P2P 等機制來偵測故意規避的應用程式？還有其他機制嗎？
- 優先使用應用程式 ID 而非網路連接埠或網路目標作為分類基礎？
- 追蹤應用程式狀態，確保以一致的方式控制應用程式和關聯的功能？
- 自動更新應用程式數據庫？這是動態更新還是系統重新啟動升級？
- 允許系統管理員直接在設備上作業，並視需要變更設定，完全不需要登入中央管理員？
- 解密 SSL 和 SSH 流量？

防火牆如何準確識別應用程式？

如何在新世代防火牆中實施 SSL/SSH 解密？

自動化

挑戰：減少進行手動任務的的時間

問題

網路安全專家的需求量很大，不過人才供應出現斷層。在最近針對網路安全領導者的研究中，三分之二 (60%) 的參與者報告說，網路安全人員短缺導致本身的企業面臨更大的風險。[4]

更嚴重的是網路安全人員一天中的大部分時間都在執行手動任務，例如調查誤判和管理補救。這種浪費時間的情況延緩了緩解措施、增加錯誤發生的機會，而且難以擴展。

安全團隊可能接獲大量的警示，而忽略可行動的關鍵警示。雖然大數據分析可揭露隱藏的模式、相關性和其他見解，可為安全團隊提供可化為行動的情報，不過您仍然需要正確的數據。這些數據必須來自各處 (網路、端點、SaaS 應用程式、公用雲端、私人雲端、數據中心等等)，並且需要隨時準備好進行分析。

解決方案要求

分析驅動的自動化可以減少花在日常任務上的時間，而且安全人員能夠專注處理業務優先事項，例如加速應用程式執行、改進程序和尋找威脅。自動化可以在三個方面提供協助：

- **工作流程自動化**：防火牆必須公開標準 API，以便可以使用其他工具和指令碼進行程式設計。這必須與 Ansible 和 Terraform 等工具整合，而且能夠使用這些工具的 API 在安全生態系統中的其他裝置上啟動工作流程，完全不需要人為介入。這種自動化應該擴展到開放原始碼格式的規則和威脅資訊運作化，例如 Snort 或 Suricata。
- **政策自動化**：防火牆必須能夠使得政策適應環境中的任何變更，例如跨越虛擬機器移動應用程式。還必須能夠從第三方來源取得威脅情報並自動採取行動。
- **安全自動化**：您的環境必須能夠發現未知威脅並向防火牆提供保護，以便自動阻止新威脅。

一些威脅仍然隱藏在數據中。透過深入探索不同位置和部署類型的數據，您可以發現潛在的威脅。透過自動化，您可以準確地識別威脅、進行快速防禦、提高效率，更有效運用專業人員的智慧，改善企業的安全狀況。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 關聯、識別和隔離網路中受感染的主機，以限制這些主機在網路中進行的存取？
- 觸發 MFA 以防止憑證濫用並保護關鍵應用程式？
- 運用從全球威脅情報獲得的資訊關聯在網路中發現的威脅？
- 對於攻擊生命週期自動產生防禦特徵碼的功能？

4. *A Resilient Cybersecurity Profession Charts the Path Forward, (ISC)² Cybersecurity Workforce Study, 2021*，(ISC)²，2021 年 10 月 26 日，https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx。

憑證安全性

挑戰：防止公司憑證遭到竊取和濫用

問題

使用者及其憑證是企業的安全基礎結構中最脆弱的環節之一。人為因素仍然是 82% 入侵的主因，其中以網路釣魚和假冒攻擊最嚴重。完成社交攻擊後，行動者可以利用遭竊的憑證進行第二步，這強調了擁有強大安全意識計劃的重要性。[5]

使用竊取的憑證時，攻擊者成功入侵的機會就會增加，遭到察覺的風險也會降低。為了防止憑證遭竊，大多數企業依賴員工教育，這種教育本質上容易出現人為錯誤。技術產品通常依賴於識別已知的網路釣魚網站和過濾電子郵件。

不過，有時可以規避這些方法。攻擊者可以透過網路釣魚、惡意軟體、社交工程或暴力破解輕鬆竊取憑證，甚至可以在暗網上購買。在 13% 的 Unit 42 研究案例中，企業並未採取任何緩解措施來確保鎖定帳戶以避免暴力破解憑證攻擊。[6] 攻擊者使用這些憑證存取網路、橫向移動並升級其權限，以便對應用程式和數據進行未經授權的存取。

解決方案要求

企業應該尋找採用機器學習分析的防火牆，以識別竊取憑證的網站。分析識別出惡意站點時，應該更新防火牆政策。您的新世代防火牆也必須允許您阻止向未知網站提交公司憑證。

防火牆也必須允許您透過強制執行 MFA 來保護敏感數據和應用程式，以防止攻擊者濫用遭竊憑證。Unit 42 的研究發現，網路攻擊者所針對的企業中有 50% 在關鍵面向網際網路的系統上缺乏 MFA，例如企業網路郵件、虛擬私人網路 (VPN) 解決方案和其他遠端存取方法。[7] 透過與常見的 MFA 廠商整合，您的防火牆可以保護包含敏感數據的應用程式，包括舊有應用程式。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 避免在未知的網站使用公司憑證？
- 阻止使用者在未於防火牆儲存一份雜湊時提交公司憑證？
- 快速分析以前未知的網路釣魚網站並更新其防護措施？
- 記錄使用者嘗試在 HTTP Post 中提交憑證的情況？

根據存取的資源本身的敏感度在存取控制政策中支援 MFA？

如果您支援 MFA，您的防火牆是否：

- 提供多種 MFA 技術選擇？
- 支援與 MFA 合作夥伴的 API 整合？
- 對於任何類型的應用程式，包括網路、用戶端伺服器和終端機應用程式，支援 MFA 政策？
- 支援任何通訊協定的 MFA 功能，而不受限於特定通訊協定？

5. *Verizon Data Breach Investigations*，2022 年。
6. *Unit 42 Incident Response Report*，2022 年。
7. 同上。

DNS Security

挑戰：阻止使用 DNS 滲透防禦的攻擊

問題

DNS 是龐大的網際網路通訊協定，承載大量數據，對於任何企業的運作來說都是極為重要，不過大多數企業未能妥善保護這個通訊協定。大多數企業都有適當的解決方案來保護網路和電子郵件，不過他們並未採取任何措施來保護他們的 DNS 流量，因此，攻擊者可以利用這種情況進行惡意活動，例如數據外洩、C2、勒索軟體和網路釣魚。由於 85% 的現代惡意軟體濫用 DNS 進行惡意活動，因此公司必須監控和分析 DNS 流量。[8]

解決方案要求

一些企業嘗試使用已知惡意網域的封鎖清單來防範 DNS 攻擊，這只能解決部分的問題。需要設法預測高度動態的惡意網域。阻止 DNS 型攻擊需要配備同級最佳安全服務的新世代防火牆，這些服務可以使用預測分析和機器學習式偵測來即時識別和阻止已知和未知的 DNS 層威脅。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 使用機器學習式預測分析和偵測來識別未知的惡意網域？
- 整合威脅情報以提高偵測能力？
- 自動將惡意網域新增到封鎖清單？
- 識別並阻止新註冊的網域名稱來降低網域搶註或網路釣魚攻擊的風險？

加密

挑戰：安全加密的流量

問題

大多數企業 Web 流量現在已經過加密，而攻擊者會利用這種情況來隱藏威脅以便規避安全監控。即使企業擁有成熟且全面的安全措施，如果不監控加密的流量，也可能會遭到入侵。此外，使用 TLS/SSL 加密的情況相當普遍，最終使用者可以輕鬆地進行設定，以隱藏與工作無關的活動。

解決方案要求

解密 TLS/SSL 加密流量的能力是基本的安全功能。我們所要尋找的關鍵元素包括任何連接埠上的識別和解密 (傳入或傳出)；對解密採取的政策控制，以及在不影響效能的情況下，跨數萬個能同時執行 SSL 連線並進行解密所需的硬體和軟體元素。

您的新世代防火牆必須具有足夠的靈活性，才能透過政策將某些類型的加密流量 (例如來自未分類網站的 HTTPS) 輕鬆地解密，而其他類型 (例如來自已知金融服務企業的 Web 流量) 則必須遵守隱私權標準。新世代防火牆應該將安全性和負載平衡應用於跨越多個安全裝置堆疊的解密流量，以進行額外的執行。這種方法不需要專用的 SSL 卸載裝置，因此降低網路複雜度，並讓解密操作更簡單。這種方法也必須支援目前獲得廣泛採用的現代通訊協定解密，例如 TLS 1.3 和 HTTP/2。

RFQ 問題

您的新世代防火牆是否：

- 包括政策控制以選擇解密、檢查和控制基於 SSL 的應用程式？
- 支援雙向 SSL 識別、解密和檢查？
- 加入 SSL 解密作為標準功能？
- 自動識別由於憑證關聯等 MITM 緩解技術而無法解密的應用程式？
- 支援 SSH 控制作為存取遠端裝置的一種方式？若支援，控制的深度為何？

在所有連接埠 (包括非標準連接埠) 上識別加密應用程式的流程為何？

哪些機制用來識別迴避應用程式 (例如 UltraSurf 和 Tor)？

8. Unit 42 威脅研究，Palo Alto Networks，2022 年。

混合雲端和多雲端安全性

挑戰：保護混合雲端和多雲端環境

問題

數據和應用程式越來越多地駐留在雲端中。在最近的研究中，將近半數 (48%) 的受訪者表示他們計劃在來年將 50% 或更多的應用程式移轉到雲端中，其中 20% 計劃移轉所有應用程式。[9]

企業現在必須保護網路和各種雲端環境 (包括 SaaS) 中的敏感數據。此外，為靜態網路設計的傳統安全工具和技術不適用於雲端原生工具或功能。此外，來自雲端供應商本身的原生安全服務通常僅提供第 4 層保護，而且只有這個雲端供應商提供，結果導致威脅攔截效率欠佳。

解決方案要求

企業需要雲端安全措施以一致的方式將政策從網路擴展到雲端，阻止惡意軟體在雲端中進行存取和橫向 (東西向) 移動、簡化管理，並在雲端工作負載發生變化時儘可能減少安全政策延遲。理想的防火牆必須運用實體網路中已經建立的相同安全狀況，保護常駐的應用程式和數據。

為了確保您能夠保護多雲端部署，防火牆必須支援各種雲端和虛擬化環境：

- **公用雲端服務供應商**：Amazon Web Services、Microsoft Azure、Google Cloud Platform、Oracle Cloud、AliCloud 和 IBM Cloud
- **軟體定義網路 (SDN) 整合**：Nutanix Flow、VMware NSX 和 Cisco ACI
- **超級管理器**：VMware ESXi、Microsoft Hyper-V、Linux KVM 和 Nutanix AHV 超級管理器
- **Kubernetes 容器**：VMware Tanzu、Rancher、Amazon EKS、Azure Kubernetes Services (AKS)、Google Kubernetes Engine 和 OpenShift

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 為私人雲端和公用雲端中的動態工作負載建立安全政策？
- 即使 IP 位址或位置發生變化，也可以確保工作負載的安全政策保持一致？
- 追蹤虛擬機器和容器的移動、新增和變更？

為新建立的虛擬機器或應用程式容器建立安全政策的程序如何進行？

哪些功能可用於與自動化和協調系統整合？

在虛擬化環境中，如何在整個虛擬機器和 Kubernetes 容器之間為流量分類 (東西向、南北向)？

什麼是虛擬化/雲端環境中的整合點？

您的新世代防火牆如何根據工作負載的虛擬機器或容器屬性建立安全政策？

9. Mike Loukides，「The Cloud in 2021: Adoption Continues」，O'Reilly，2021 年 12 月 7 日，https://www.oreilly.com/radar/the-cloud-in-2021-adoption-continues/。

IoT 安全性

挑戰：減少 IoT 安全暴露的風險

問題

雖然 IoT 裝置可以協助企業提高生產力、效率和營收，不過這些裝置對於攻擊者來說也是網路中最薄弱的環節。在 2021 年的研究中，78% 的資訊技術決策者發現 IoT 安全事件的數量比前一年增加。[10]

由於各種原因，現有的安全策略無法保護易受攻擊的 IoT 裝置。最重要的是缺乏明確的所有權。IT 安全團隊可能不完全了解 IoT 部署的範圍和性質，因此不會將這些元件包含在 SOC 工作流程中。許多現有的資產和端點管理工具都無法滿足 IoT 安全性的需求。此外，IoT 安全產品通常採用特徵碼型的靜態方法來識別裝置。這種方法無法擴展以因應每天大量增加的全新裝置或裝置變體。其他方法僅提供可視性，缺乏實際保護這些裝置所需的原生內建政策執行功能。

解決方案要求

在評估您的新世代防火牆時，請考慮可以識別和分類網路上所有 IoT 裝置的解決方案 (包括前所未見的裝置)。您的防火牆解決方案應該有助於安全團隊憑藉每個裝置的完整脈絡來快速擬定決策，進而判斷裝置身分、風險層級，以及任何行為上的異常。然後，防火牆應該根據原生自動執行的風險評估提供區隔和其他政策建議。防火牆也應該能夠阻止對 IoT 裝置的已知和未知威脅。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 識別和分類網路上的所有 IoT 裝置，包括前所未見的裝置？
- 評估 IoT 特有的風險和威脅？
- 根據風險評估提供和執行政策建議？
- 與資產管理、SIEM、EPP、XDR 和 NAC 等其他 IT 和安全技術共享 IoT 裝置脈絡？

行動安全性

挑戰：保護行動工作者

問題

隨著行動裝置的使用，行動工作人員不斷增加，他們通常透過公用網路和對進階威脅毫無防備的裝置連接到業務應用程式。此程序會增加使用者在外部所面臨的風險，因為沒有網路防火牆可以阻止攻擊，而且在考慮雲端和自備裝置 (BYOD) 做法的影響時，問題變得更加複雜。此外，遠端位置和小型分公司通常缺乏一致的安全性，因為在操作防火牆或向總部回傳流量的運作效率偏低，而且成本相當高。

解決方案要求

行動工作人員和遠端位置需要從遠離網路的位置存取應用程式。這些人員和位置也需要防範針對性網路攻擊、惡意應用程式和網站、網路釣魚、C2 流量和其他未知威脅。

您的新世代防火牆必須一致啟用所需層級的可視性、威脅防禦和安全政策實施，以便透過從雲端提供新世代防火牆功能來保護您的分散式使用者和位置，藉以在不需要部署實體硬體的情況下保護這些使用者和位置。

進一步了解。

RFQ 問題

您的新世代防火牆是否：

- 保持使用者持續連線，無論使用者位於外部網路還是內部無線網路，確保一致的政策執行？
- 安全地啟用企業和 BYOD 筆記型電腦、手機和平板電腦？

有哪些選項可用來保護遠端使用者 (包括所有必要元件) 的安全？

是否包括用戶端元件，它是如何進行部署？

可以同時支援多少個使用者？

遠端使用者安全功能組對用戶端是否透通？

對遠端使用者實作政策控制 (在防火牆政策中，在單獨的政策/裝置中等等)？

遠端功能 (例如 SSL、應用程式控制和 IPS) 提供哪些功能和保護？

10. *The Connected Enterprise: IoT Security Report 2021*，Palo Alto Networks，2021 年 10 月 20 日，https://www.paloaltonetworks.com/resources/research/connected-enterprise-iot-security-report-2021。

政策一致性

挑戰：在混合雲端環境中保持一致的政策

問題

安全管理的複雜度不斷提高，公司領導階層對此不太滿意。最近的研究發現，將近半數 (46%) 的企業正在整合或計劃整合有業務往來的廠商數量，藉以降低安全系統的複雜度。[11]

這種複雜度通常是舊有決策造成的結果。對於內部部署和/或在雲端環境託管的應用程式，企業已經採用各式各樣的單點產品來滿足不同的網路和安全性要求。但是，每個產品都有個別的管理政策和介面，進而造成額外的成本、複雜度和安全漏洞。此外，這些產品未經過整合，無法共享對網路存取、應用程式存取或政策違規的見解，也無法提供整合的日誌。

企業還發現，大規模上線新的防火牆設備、維護一致的安全政策以及對數千個防火牆部署政策變更相當有挑戰性。這種方法會造成安全性和網路效能方面的差距，從而導致人員和成本短缺。

解決方案要求

若要成功，防火牆解決方案必須以各種形式 (硬體、軟體和容器化) 提供安全功能，藉以將安全保護整合到環境的最佳部分。您必須能夠透過集中管理、整合核心安全任務和簡化功能，跨越內部部署和雲端部署 (包括遠端位置、行動使用者和 SaaS 應用程式) 的數萬個防火牆部署一致的集中式安全政策。

例如，您應該能夠使用單一主控台查看所有 Web 流量、管理設定、推送全域政策，以及產生流量模式或安全事件的報告。您的報告功能必須讓您的安全人員深入了解網路、應用程式和使用者行為，藉以掌握做出明智決定所需的脈絡。

從雲端提供這些功能後，您的團隊可以在針對所有位置的流量、應用程式和使用者而設計的架構中，獲得所需的網路和安全性。在現今不斷變化的威脅形勢中，運用單一安全廠商來滿足您的大量安全和業務需求可能不切實際。在這種情況下，整合和運用第三方見解和創新的能力極為重要。

在評估安全廠商時，務必評估能夠提供的彈性、可擴展性和可程式性。閱讀本電子書，了解為使用雲端的企業提供保護以及為企業網路和安全性提供速度和敏捷性的新方法。

RFQ 問題

您的新世代防火牆能否：

- 對於內部部署以及在虛擬化和容器環境中執行的應用程式提供一致的網路安全性和威脅防禦？
- 在 Kubernetes 環境中原生部署？
- 提供持續整合/持續開發 (CI/CD) 程序？
- 整合至軟體定義網路 (SDN) 解決方案以將安全防護延伸至遠端位置，藉以進行分公司區隔並達到 PCI 合規性？
- 使用 API 針對各個功能自動進行設定變更？

您的新世代防火牆是否允許中央管理員：

- 直接在設備上作業，並視需要變更設定，完全不需要登入中央管理員？
- 監控和查看本機管理員所做的變更？
- 迅速地回復特定使用者的變更並還原工作設定？

您的中央防火牆管理員可以：

- 將日誌管理與核心設定管理分開？
- 針對高達 50,000 LPS 的輸送量取得日誌？
- 充當單一管理平台以實現統一可視性？

11. Jon Oltsik，*Technology Perspectives from Cybersecurity Professionals*，ESG，2022 年 7 月，https://www.issa.org/wp-content/uploads/2022/07/ESG-ISSA-Research-Report-Security-Process-and-Technology-Trends-Jul-2022.pdf。

政策漏洞管理

挑戰：弭平危險的政策差距

問題

傳統防火牆依據連接埠和 IP 位址允許和阻止流量。這種方法並不合適，因為依據連接埠的規則會允許透過防火牆傳輸的善意和惡意應用程式。應用程式可以透過跳躍連接埠，使用 SSL 和 SSH，或使用眾所周知的開放連接埠 (例如 80 和 443) 輕鬆地透過連接埠型防火牆傳輸。

隨著時間的推移，客戶在其防火牆上累積數千個依據連接埠的規則，而且經常會將這些規則按原狀遷移到新世代防火牆。這些規則會留下危險的政策差距。客戶意識到必須遷移到依據應用程式的規則來建立有效的安全性，但這需要大量的手動操作，而且由於網路安全技能的不足，大多數企業都沒有這些資源。這成為可能導致業務中斷的高安全性風險。

解決方案要求

在評估新世代防火牆時，請尋找可以降低規則和政策管理複雜度的防火牆。一種方法是探索在您的網路上運作的應用程式，將這些應用程式對應到舊有規則，並且協助替換舊有規則。您的新世代防火牆應該協助您的安全團隊使用依據應用程式的直覺式政策輕鬆替換舊有規則。由於依據應用程式識別的規則易於在業務需求發展時建立、了解和修改，因此可以儘可能減少容易遭受數據外洩攻擊的設定錯誤。這些政策可以加強安全性，並且大幅縮短管理時間。最後，您的新世代防火牆應該彙總遙測資訊並套用機器學習來自動識別所需的政策和設定變更。這些功能可以改進安全政策最佳化，藉以消除由於設定錯誤所造成的漏洞。

RFQ 問題

您的新世代防火牆能否：

- 在識別應用程式之前對流量分類執行狀態檢查？
- 允許對應用程式數據庫中的所有應用程式實施以連接埠為基礎的控制？
- 允許管理員依據政策執行應用程式和連接埠關係？例如，確保 IT 人員是唯一獲准使用 SSH 和 RDP 的人？
- 為機器學習式安全政策最佳化收集遙測數據，藉以消除由於設定錯誤造成的漏洞？
- 提供可用於自訂或非標準識別基礎結構整合的 API？

識別應用程式後，如何監控、追蹤應用程式狀態變更並將其用於政策？

應用程式數據庫階層如何在父應用程式中公開功能以獲得更精細的啟用政策？

您可以對個別應用程式及其各自的功能施加哪些層級的控制？

以使用者為基礎的控制支援哪些企業識別儲存庫？

使用者和群組如何針對終端機服務環境實作政策式控制？

硬體和虛擬化執行個體的應用程式啟用選項有什麼區別？

保護分公司連線的安全

挑戰：將分公司安全地連線到總部

問題

隨著企業持續將應用程式遷移到雲端，IT 團隊面臨著快速、可靠並安全地將公司位置和分公司連線到關鍵業務資源的挑戰。軟體定義的廣域網路 (SD-WAN) 承諾增加頻寬，同時改善連線能力和效能，企業對此表示關注。

但是，儘管 SD-WAN 擁有諸多優勢，但它也帶來許多挑戰，例如，安全性下降或束手無策、無法預見架構和部署複雜，以及效能難以預測。

解決方案要求

您的新世代防火牆應該將始終一致的安全性擴展到分公司，以保護數據中心和雲端環境。企業可以透過實作與其原生整合的防火牆，以安全地採用 SD-WAN，藉以整合其連線能力和安全性。這也有助於維持從網路核心到分公司的安全政策的一致性。利用 SD-WAN 設定和監控功能，以及可透過單一管理平台提供的防火牆使用者和應用程式政策工作流程，企業就可以避免安全狀況方面的漏洞，並從改善的安全性、簡便性和效率中受益。閱讀本電子書，了解如何運用 SD-WAN 實現一致的安全性。

進一步了解。

RFQ 問題

您的新世代防火牆能否：

- 與您的 SD-WAN 原生整合？
- 維持從網路核心到分公司的安全政策的一致性？
- 透過單一管理平台整合可用的 SD-WAN 設定和監控以及防火牆使用者和應用程式政策工作流程？

安全協調

挑戰：利用其他安全工具，協調偵測與分析

問題

進階攻擊者不會將自己局限於架構的一部分。他們的目標是從端點橫向移動到您的網路、雲端和其他數據結構，以存取並洩漏有價值的數據。Unit 42 進行的研究發現，客戶往往會低估特定威脅肆虐的時間長度。在某些案例中，我們發現威脅行動者會在六個多月的期間內顯得特別活躍或不停在環境中橫向移動。[12]

考慮到這一點，孤立的安全方法只能看到並了解基礎結構的一部分，從而產生次佳的結果。這些方法會限制分析的應用，並迫使安全分析師在介面之間不停地轉換，以嘗試手動整合攻擊，此過程既耗時又容易出錯。

解決方案要求

隨著所需安全功能數量的增加，可以提供有意義安全功能整合的平台/裝置的潛在價值也隨之增加。如果您的防火牆可以充當更全面的機器學習導向分析平台 (例如擴展的偵測與回應 (XDR) 解決方案) 的感測器和執行點，您的安全團隊將在發現、補救及防止複雜攻擊方面獲得效能和效率。

您的新世代防火牆應該與 XDR 整合，讓您的網路和安全團隊都能了解攻擊的完整範圍、分享威脅脈絡和情報，並在防火牆與其他執行點之間推動自動化回應以及執行。

RFQ 問題

您的新世代防火牆能否：

- 根據在防火牆上發現的惡意事件，在變更管理系統上建立票證？
- 在無線網路上，對受感染的主機觸發隔離動作？
- 透過 API 進行完全編程？
- 透過 API，從無線控制器收集與連線到無線網路的主機有關的 User-ID 資訊？
- 將第三方或自訂的威脅情報摘要動態地整合到防火牆而不需要政策認可？
- 在將指標推送到防火牆之前，支援威脅摘要彙總、整合和刪除重複數據？
- 與您的新世代防火牆整合，讓過期的威脅指標自動逾時，以避免使用過時的威脅情報？
- 允許您鎖定最近 APT 活動的威脅指標，並且在您的新世代防火牆中主動整合威脅摘要？
- 允許您根據信任度評分，使用情報強化雲端威脅情報和 IOC，以減少處理誤判造成的營運開支？

12. *Unit 42 Incident Response Report*，2022 年。

零信任

挑戰：採用零信任安全策略

問題

傳統的安全模型都依賴一種早已過時的假設，亦即假設企業網路內的所有內容都可以信任。這些模型旨在保護週邊。同時，進入網路的威脅卻完全未受到注意，因此到處破壞有價值的敏感業務數據。在數位世界中，信任極為脆弱。

考慮由內部威脅引起的風險。雖然內部威脅不是入侵的主要原因 (Unit 42 研究僅在 5.4% 的研究事件中引用內部威脅[13])，不過蓄意的內部攻擊可能造成災難性後果，因為這些惡意行動者確切知道在哪裡尋找敏感資訊。報告的內部威脅案例中有 75% 是由心懷不滿的前員工而造成，他們在離職後挾帶公司數據離開、銷毀公司數據或存取公司網路。[14]

解決方案要求

零信任是一種網路安全策略，可以消除信任的概念。在零信任世界中，沒有可信任的裝置、系統或人員。您可以識別對企業最關鍵的數據、資產、應用程式和服務，根據工作職能決定誰或甚麼有存取權，並且透過網路區隔、精細的第七層安全政策、使用者存取控制以及威脅防禦，強制執行最低權限的存取模型。

在評估新世代防火牆時，尋求可作為區隔閘道的防火牆來啟用零信任架構。您的新世代防火牆應該直接與「零信任」保持一致，包括為各地的所有使用者提供安全存取、檢查所有流量、執行最低權限存取控制的政策，並偵測和預防進階威脅。零信任可大幅減少企業內外部攻擊者存取關鍵資產的途徑。

進一步了解。

RFQ 問題

您的新世代防火牆是否可讓您撰寫以脈絡為依據的政策，以確定誰或什麼可以存取您的保護範圍？

新世代防火牆如何運用網路區隔、防止橫向擴散、提供第七層威脅防禦，以及簡化精細的使用者存取控制？

新世代防火牆是否會檢查所有流量中是否有惡意的內容、未經授權的活動和數據洩露，以及是否會透過第七層查看網路和公用雲端或私人雲端環境中的內部和外部日誌？

13. *Unit 42 Incident Response Report*，2022 年。
14. 同上。

選擇 Palo Alto Networks 的六大理由

同級最佳產品組合

我們領先業界的解決方案以智慧化方式協同運作，藉以加強安全性、簡化操作並提高投資報酬率。進一步了解。

對零信任的承諾

Palo Alto Networks 是唯一一家在使用者、應用程式和基礎結構的整個數位生態系統中實現全面零信任並持續驗證每次互動的公司。進一步了解。

絕佳的安全存取

我們透過業界最完整的 SASE 解決方案和 ZTNA 2.0 增強和保護全球混合工作者。進一步了解。

多雲端保護

Palo Alto Networks 提供唯一全面的雲端原生應用程式保護平台 (CNAPP)，可以跨越所有雲端提供完整生命週期、完整堆疊保護。進一步了解。

驅動自發性 SOC

藉由運用現今最先進的人工智慧和自動化所展現的優勢，Palo Alto Networks 有助於安全團隊為下一步做好準備。進一步了解。

世界級威脅情報和事件回應

我們的 Unit 42 威脅情報增強我們一切作為的成效。我們的團隊是 70 多家網路保險公司指名的入侵回應公司。進一步了解。

您的下一步

本指南應該有助於您制定全面的 RFP，藉以瀏覽數十家可能的廠商並且找到適合貴企業的廠商。Palo Alto Networks 相信我們的解決方案可以提供業界最佳價值 – 我們可以證明這一點。立即註冊產品體驗營！

諮詢熱線：0800666326
網址：www.paloaltonetworks.tw
郵箱：contact_salesAPAC@paloaltonetworks.com

Palo Alto Networks 台灣代表處
11073 台北市信義區松仁路 100 號 6F-1