Palo Alto Networks 新世代防火牆概覽

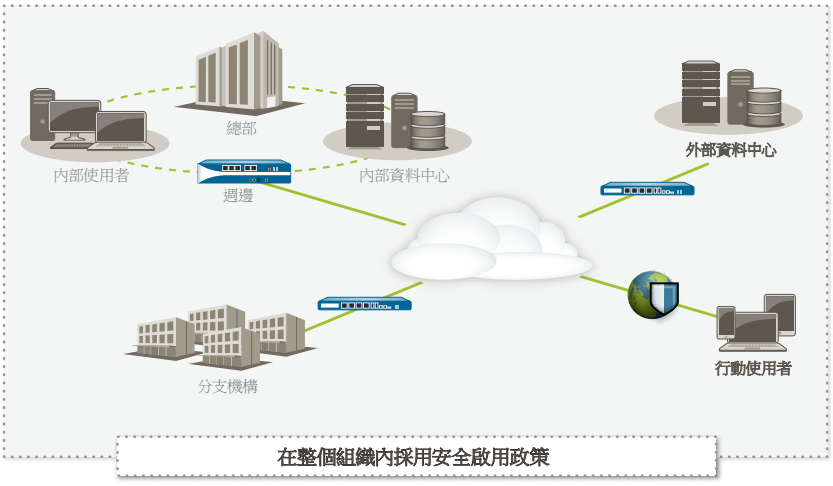
應用程式與威脅概況、使用者行為和網路基礎設施方面的根本轉變不斷削弱傳統連接埠防火牆所提供的安全性。您的使用者使用一系列類型的裝置存取各種類型的應用程式，這通常需要存取多次才能完成工作。同時，資料中心擴展、虛擬化、行動性以及基於雲的舉措正在迫使您重新思考如何才能夠既存取應用程式又保護您的網路。

傳統的對應包括試圖透過防火牆以外所提供繁多的單點技術鎖定全部應用程式的流量（這樣做可能會阻礙您的業務），或者允許全部應用程式（由於業務和安全風險的增加，這種做法同樣不可接受）。您所面對的挑戰是，傳統的連接埠防火牆即便帶有附加的應用程式阻止功能，也不能取代這兩種做法中的任一種。為了在允許全部和拒絕全部之間取得平衡，您需要透過使用與業務相關的元件（例如應用程式標識、誰正在使用應用程式和內容類型）作為防火牆安全性政策標準、安全地啟用應用程式。

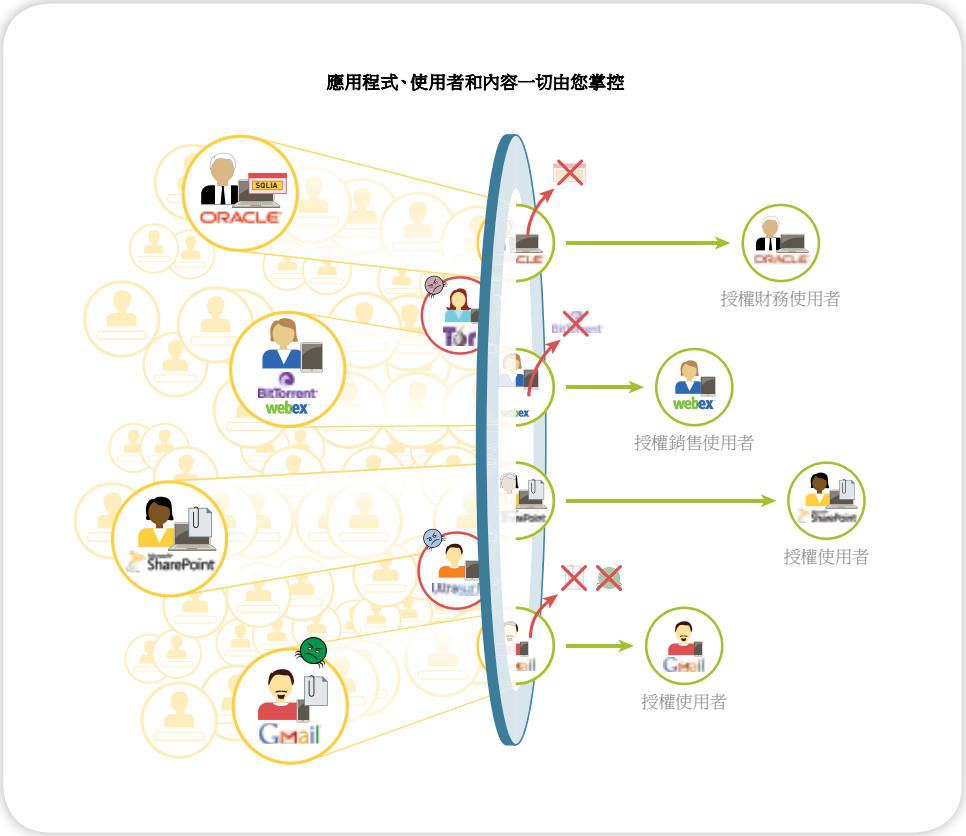
關鍵安全啟用要求：

- **識別應用程式，而非連接埠。**流量一進到防火牆就對其進行分類，從而確定應用程式標識，而不考慮協定、加密或規避政策，然後將該標識用作全部安全性政策的基礎。
- **無論任何位置或裝置，均將應用程式與使用者身份（而非 IP 位址）互相關聯。**無論任何地點和裝置，使用從企業目錄和其他使用者存儲區獲得的使用者與群組資訊均對您的全部使用者部署一致的啟用政策。
- **防止已知和未知的各種威脅。**防止已知漏洞入侵、惡意軟體、間諜軟體和惡意 URL，同時對具有高針對性和以前未知的惡意軟體進行流量分析並自動提供保護。
- **簡化政策管理。**透過易於使用的圖形化工具、統一的政策編輯器、範本和裝置群組，可以安全地啟用應用程式並減少管理工作。

安全應用程式啟用政策有助於在所有部署地點改善您的安全性狀態。在週邊，透過阻止各種不需要的應用程式並針對已知和未知威脅檢查所允許的應用程式，可以減少您的威脅足跡。在傳統或虛擬化資料中心，應用程式啟用轉換為確保授權使用者只使用資料中心應用程式，從而防止內容受到各種威脅，並應對虛擬基礎設施的動態特性所導致的安全性挑戰。可以透過在總部地點部署的同一組啟用政策對您的企業分支機構和遠端使用者進行保護，從而確保政策的一致性。



paloalto NETWORKS
the network security company™



使應用程式能夠增強業務實力

Palo Alto Networks 新世代防火牆的安全啟用應用程式有助於應對與迅速增加的大量穿越您網路的應用程式相關的業務和安全性風險。透過本機、行動和遠端啟用使用者或使用者群組的應用程式，並防止該流量免受已知和未知威脅，您可以改善安全性狀態，同時拓展業務。

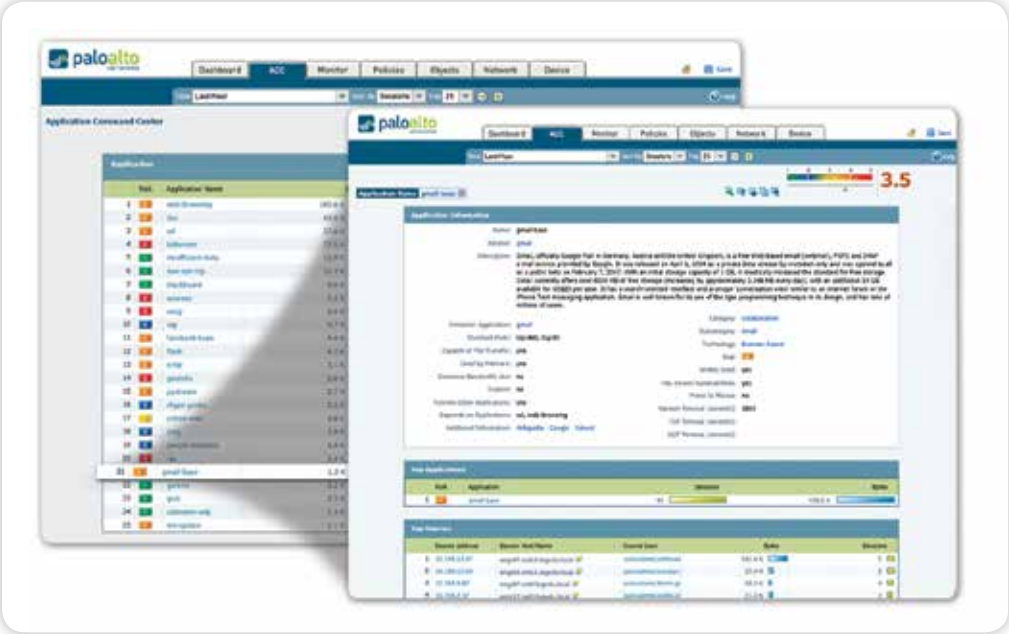
- **每時每刻在各連接埠對全部應用程式進行分類。**將流量精確分類是所有防火牆最重要的工作，而其成果正是安全性政策的基礎。但是現今的應用程式可以輕易繞過連接埠防火牆；在連接埠間轉換、使用 SSL 和 SSH、暗中跨過連接埠 80 或使用非標準連接埠。App-ID 透過對流量串流應用多種分類機制來應對困擾傳統防火牆的流量分類視覺化限制，從而在防火牆發現之後立即確定穿越您的網路的應用程式的確切身份，而不考慮連接埠、採用的加密（SSL 或 SSH）或規避技術。瞭解穿越您的網路的確切應用程式（不僅僅是連接埠和協定）成為您所有安全性決策的基礎。可為不明身份應用程式（通常為流量比例小卻擁有高潛在風險）進行自動分類，從而實現系統化管理，而這種管理可能包含政策控制與檢查、威脅鑑識、建立自訂 App-ID 或 Palo Alto Networks App-ID 開發的封包擷取。

- **將使用者和裝置（而不僅僅只是 IP 位址）整合到政策中。**無論任何地點和裝置，均可根據應用程式與使用者身份建立和管理安全性政策，這種方法比單純依靠連接埠和 IP 位址來保護網絡更加有效。與各種企業使用者存儲庫進行整合可提供存取應用程式的 Microsoft Windows、Mac OS X、Linux、Android 或 iOS 使用者的身份。透過在本機或企業網路上使用相同的一致性政策，可對差旅或遠端工作的使用者進行無縫保護。在使用者應用程式活動上結合了可見度和控制，這意味著無論使用者正在何處或如何存取 Oracle、BitTorrent、Gmail 或穿越您的網路的任何其他應用程式，您均可安全地進行啟用。

- **防止已知和未知的各種威脅。**要保護當今的現代網路，必須應對漏洞、惡意軟體和間諜軟體的混合體，以及完全未知的與有針對性的威脅。這種流程透過隱含的「拒絕其他全部」政策或明確的政策允許特定應用程式，從而縮小網路攻擊面。然後，可以將協調後的威脅防禦應用到所允許的全部流量，阻止已知的惡意網站、漏洞入侵、病毒、間諜軟體和同一個通道中的惡意 DNS 查詢。透過在虛擬化沙箱環境中執行未知檔並直接觀察 100 多項惡意行為，可積極分析和識別自訂或未知惡意軟體。發現新的惡意軟體時，會自動生成並向您發送感染檔的特徵碼和相關惡意軟體的流量。全部威脅防禦分析均使用應用程式和協定的完整範圍，如此一來，即便這些威脅試圖躲避通道中、壓縮內容中或非標準連接埠上的安全性政策，也始終都會被捕獲到。

部署和管理靈活性

在專屬硬體平台或虛擬化形式因素中均可使用安全應用程式啟用功能。如果您在硬體或虛擬形式因素中部署了多個 Palo Alto Networks 防火牆，您可以選擇使用集中管理系統 Panorama，這個系統可洞察流量模式和部署政策，並從一個中央地點提供內容更新。



應用程式可見度：以清楚、容易閱讀的格式檢視應用程式活動。新增和刪除篩選器，從而瞭解應用程式及其功能和使用者的詳細資訊。

安全應用程式啟用：全面方法

安全應用程式需要一種從深入瞭解您網路上的應用程式著手來保護網路和拓展業務的全面方法，而不論平台或地點、使用者是誰、應用程式承載的內容是什麼。透過更全面地瞭解網路活動，您可以根據應用程式各元件以及與您的業務相關的使用者和內容建立更有意義的安全性政策。使用者地點及其平台、部署策略的地方——（週邊、傳統或虛擬化資料中心）、分支機構或遠端使用者——對如何建立政策而言區別不大或毫無區別。現在，您可以安全地啟用任何應用程式、使用者和內容。

全面瞭解意味著更加嚴格的安全性政策

安全性最佳作法指出，更全面地瞭解網路上的具體情況有利於實施更嚴格的安全性政策。例如，確切地知道哪些應用程式正在穿越您的網路（而不是一組基於連接埠的粗略流量）可使您的管理員能夠特別允許使企業正常營運的應用程式，同時阻止有害的應用程式。知道使用者是誰（而不僅只是 IP 位址）可增加一條能夠讓您在政策分配方面更加具體的政策標準。透過使用一套功能強大的圖形化視覺工具，您的管理員可以更完整地瞭解應用程式活動和潛在的安全性影響，並做出更明智的決策。會對應用程式持續進行分類，並隨其狀態變化對圖形化摘要進行動態更新，然後在易於使用的 Web 介面中顯示資訊。

- 使用單鍵作業即可顯示應用程式的說明，讓管理員能夠調查新的或不熟悉的應用程式及其重要功能、行為特性和誰正在使用。
- URL 類別、威脅和資料模式方面的額外可見度則能提供一份完整且全面的網路活動紀錄。
- 可對未知應用程式（通常為每個網絡上比例小卻擁有高潛在風險的）進行分類，以便分析並決定其是否為內部應用程式、尚未識別的商業應用程式或威脅。
- 您的客戶經常存取其所需的任何應用程式，並且通常需要多次存取才能完成工作，進而使應用程式、使用者和相關內容與您的業務比以往任何時候都更加相關。透過更完整地瞭解網路上的情況，您的管理員可以將該資訊轉換成應用程式啟用政策，從而降低風險。

啟用應用程式和降低風險

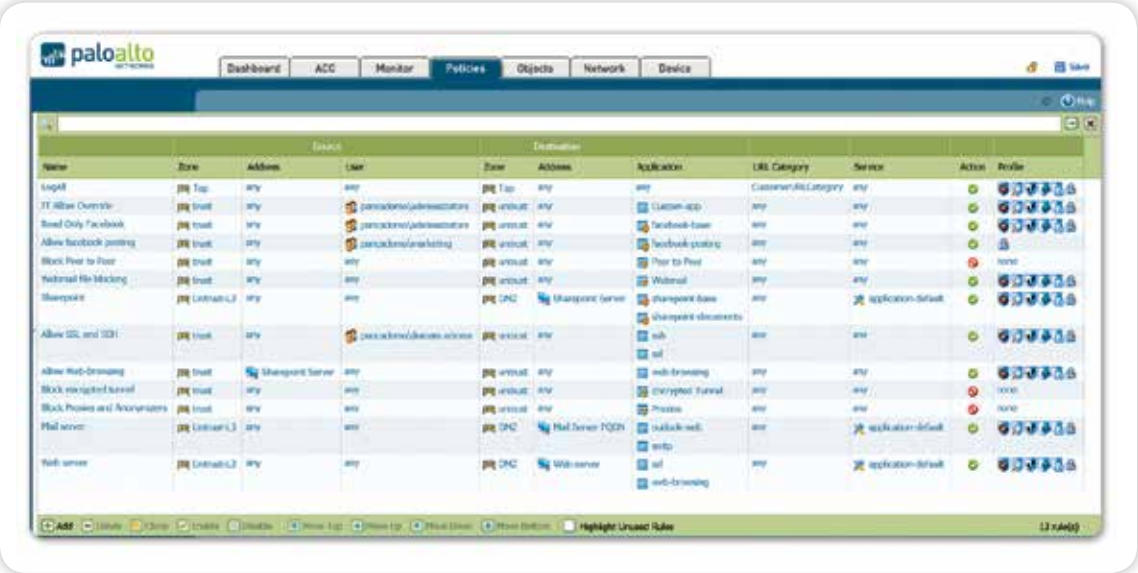
安全應用程式啟用將各種決策標準用作在拒絕全部應用程式的業務限制和允許全部應用程式的高風險選擇之間取得平衡的一種手段，這些標準包括應用程式/應用程式功能、使用者與群組以及內容。

在包括分支機構、行動和遠端使用者在內的週邊，啟用政策集中在識別全部流量，根據使用者身份有選擇地允許流量，然後掃描流量是否存在威脅。政策範例可能包括：

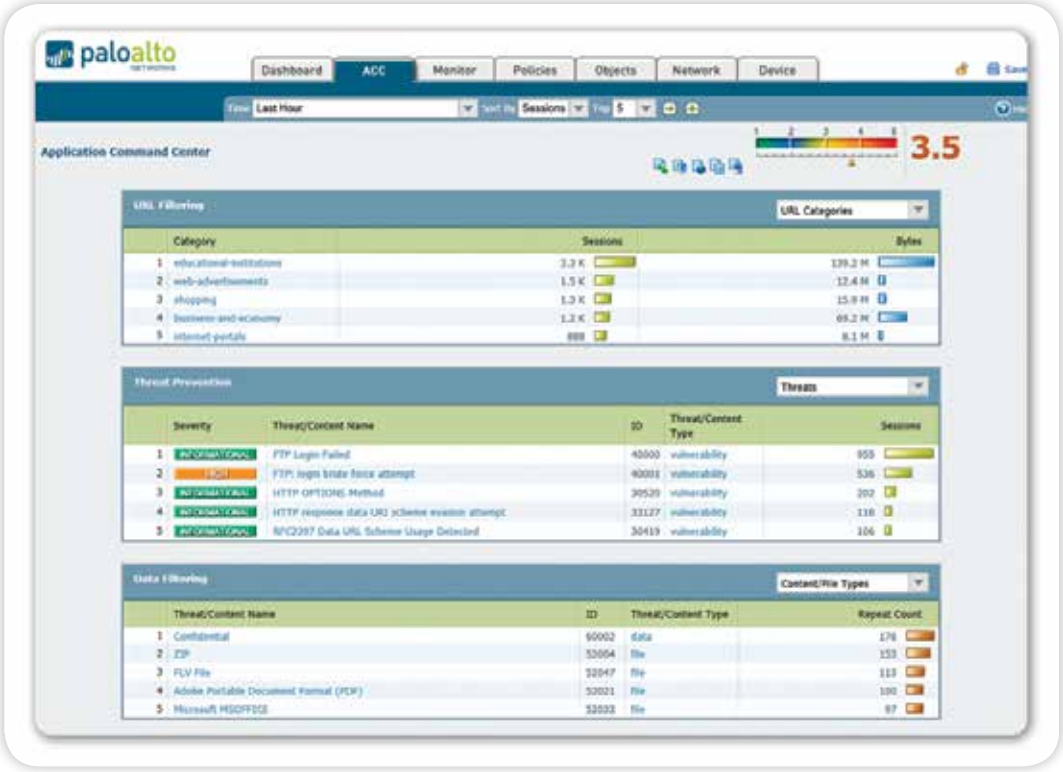
- 對選定的一些變數限制使用 Webmail 和即時通訊；對使用 SSL 的連線進行解密，檢查流量是否試圖入侵，並將未知檔上傳到 WildFire 進行分析和特徵碼開發。
- 允許串流媒體應用程式和網站但套用 QoS 和惡意軟體防禦，以便限制對 VoIP 應用程式的影響並保護網路。
- 透過允許您的全部使用者「瀏覽」、阻止全部 Facebook 遊戲和社交外掛程式、允許 Facebook 發佈僅用於市場行銷的內容，對 Facebook 進行控制。掃描 Facebook 的全部流量，從而檢查是否存在惡意軟體和入侵。
- 透過允許和掃描業務相關網站的流量並同時阻止存取明顯與工作無關的網站，對網路瀏覽進行控制，並透過自訂阻止網頁「引導」存取可疑網站。
- 透過使用 GlobalProtect 將相同政策透明地部署到本機、行動或遠端的全部使用者，強制執行一致安全性。
- 使用隱含的「拒絕其他全部」政策或明確阻止不需要的應用程式（例如 P2P 和 Circumventor 或來自特定國家的流量），從而減少引入業務和安全性風險的應用程式流量。

在傳統、虛擬或二者組合的資料中心內，啟用範例集中在確認應用程式、尋找流氓應用程式和保護資料方面。

- 在自身的安全性區域內隔離基於 Oracle 的信用卡號碼儲存庫；控制對金融集團的存取，從而迫使流量經過其標準連接埠，並檢查應用程式漏洞的流量。
- 使 IT 群組只能使用其標準連接埠上固定的一組遠端管理應用程式（例如 SSH、RDP、Telnet）存取資料中心。
- 只允許管理團隊使用 Microsoft SharePoint Administration，並允許所有其他使用者存取 Microsoft SharePoint 文檔。



統合政策編輯器：熟悉的外觀與操作，可讓您快速建立和部署控制應用程式、使用者和內容的政策。



內容與威脅的可見度：以清楚、容易閱讀的格式檢視 URL、威脅與檔案/資料傳輸活動。新增和刪除篩選器，以進一步了解個別元素。

保護已啟用的應用程式

安全應用程式啟用意味著允許存取某些應用程式，然後套用具體政策，以便阻止已知入侵、已知或未知的惡意軟體和間諜軟體；還意味著控制檔案或資料傳輸以及網路瀏覽活動。透過使用 App-ID 中解碼器生成的應用程式和協定範圍執行威脅防禦政策，可應對跳連接埠和通道效應等常見威脅規避策略。相反，UTM 解決方案對威脅防禦採用一種基於 Silo 的方法，其中每個功能、防火牆、IPS、AV、URL 篩選、全部掃描流量均不共用任何內容，使其更易受到規避行為的影響。

- **阻止已知威脅：IPS 與 Network Antivirus/Anti-spyware。**統一的特徵碼格式和基於串流的掃描引擎讓您能夠保護您的網路免受各種威脅。入侵防禦系統 (IPS) 具有阻止網路和應用程式層漏洞入侵、緩衝區溢位、DoS 攻擊和連接埠掃描功能。Antivirus/Anti-spyware 保護可阻止數以百萬計的惡意軟體變種，以及任何惡意軟體生成的命令與控制流量、PDF 病毒和隱藏在壓縮檔案或網站流量（壓縮的 HTTP/HTTPS）中的惡意軟體。跨越全部連接埠上所有應用程式的政策式 SSL 解密可保護您免受在 SSL 加密的應用程式中移動的惡意軟體侵害。

- **阻止未知的和有針對性的惡意軟體：Wildfire™。**WildFire 可識別和分析未知的或有針對性的惡意軟體。WildFire 在基於雲端的虛擬化沙箱環境中直接執行和觀察未知檔案。WildFire 可監視 100 多項惡意行為，並以警報形式將結果立即發送給管理員。WildFire 可選訂閱以提供增強的保護、記錄和報告。訂閱之後，在世界上任何地方發現新的惡意軟體之後一個小時內，您就可以受到保護，這樣可以有效地在新的惡意軟體對您造成影響之前就停止其散播。訂閱之後，您還可以存取整合的 WildFire 記錄與報告以及 API，以便向 WildFire 提交範本進行分析。

- **識別感染殭屍病毒的主機。**App-ID 對所有連接埠上的全部應用程式進行分類，其中包括在您的網路中經常暴露出異常或威脅的任何未知流量。殭屍網路的行為報告與未知流量、可疑的 DNS 與 URL 查詢以及揭示裝置可能已感染惡意軟體的各種異常網路行為相關聯。其結果會以可能受感染之主機的清單格式顯示，而這些主機就可以當作殭屍網路可能的成員來加以調查。
- **限制未經授權的檔案和資料傳輸。**資料篩選功能讓您的管理員能夠執行可減少與未經授權的文檔和資料傳輸相關之風險的政策。可以透過查看檔案內容（而不僅只是檢查副檔名）來控制文檔傳輸，從而確定是否允許傳輸作業。可以阻止通常位於偷渡式下載中的可執行檔，從而保護網路免受隱形惡意軟體傳播侵害。資料篩選功能可以偵測和控制機密資料模式（信用卡號、社會保險號碼以及自訂模式）的傳輸。
- **控制網路瀏覽。**完全整合的自訂 URL 篩選引擎可讓您的管理員應用細微網路瀏覽政策，以此補充應用程式可見度和控制政策，並保護企業免受法律、法規和生產效率方面的風險。此外，可將 URL 類別應用在政策中，從而對 SSL 解密、QoS 或其他規則基礎提供更加精確的控制。

持續的管理與分析

安全性最佳做法指出，管理員應在主動地管理防火牆（無論是一個還是數百個裝置）和被動地對安全性事故進行調查、分析與報告之間取得平衡。

- **管理：**可以透過命令列介面 (CLI) 或全功能瀏覽器式介面對每個 Palo Alto Networks 平台進行單獨管理。針對大規模部署，可許可 Panorama 並將其作為集中管理解決方案進行部署，讓您能夠使用範本和共用政策等功能在整體的集中控制和本機政策靈活性需求之間取得平衡。對 SNMP 和基於 REST 的 API 等標準式工具的額外支援讓您能夠與第三方管理工具進行整合。無論是使用裝置的 Web 介面還是 Panorama 介面，介面的外觀和感覺是一樣的，這樣可以確保從一個介面轉移到另一個介面時不存在學習曲線。您的管理員可以使用所提供的任何介面隨時進行變更，而無需擔心同步問題。全部管理介質均支援基於角色的管理，這讓您能夠將特性和功能分配給具體的個人。
- **報告：**預先定義的報告可以依原樣使用，或者群組為單一報告以符合特定要求。所有報告均可匯出成 CSV 或 PDF 格式，而且可以按照排程執行以及用電子郵件寄出。
- **記錄：**即時記錄檔篩選有助於對穿越您的網路的每一個工作階段進行快速鑑識調查。記錄篩選結果可以匯出至 CSV 檔案，或傳送至 syslog 伺服器，以供離線封存或其他分析。

專屬硬體或虛擬化平台

從設計用於企業遠端辦公的 PA-200 到設計用於高速資料中心的 PA-5060，Palo Alto Networks 提供全系列專屬硬體平台。平台結構以單一通道軟體引擎為基礎，對連網、安全性、威脅防禦和管理採用功能特定的處理，從而提供可預測的性能。VM 系列虛擬防火牆也擁有在硬體平台中提供的相同防火牆功能，讓您能夠使用與應用到您的週邊或遠端辦公防火牆相同的政策，從而保護您基於雲端的虛擬化運算環境。

paloalto NETWORKS
the network security company™

3300 Olcott Street
Santa Clara, CA 95054

Accueil : +1.408.573.4000
Ventes : +1.866.320.4788
Assistance : +1.866.898.9087

www.paloaltonetworks.com