paloalto NETWORKS

STRATA™
BY PALO ALTO NETWORKS

GlobalProtect

GlobalProtect 將 Palo Alto Networks 新世代防火牆的保護範圍擴大到在任何地點的行動工作者成員。

因為使用者和應用程式移轉到傳統網路邊界外的地點，所以您需要保護的範圍會持續擴大。安全團隊在維持網路流量的可視性和實施安全政策來阻止威脅時面臨著諸多挑戰。保護行動端點所使用的傳統技術 (例如主機端點防毒軟體和遠端存取虛擬私人網路 (VPN)) 無法阻止現今攻擊者所運用的縝密先進技術。

GlobalProtect™ 端點網路安全能夠將 Palo Alto Networks 新世代防火牆延伸到任何地點的所有使用者，從而讓您保護行動工作者的安全。它能夠運用平台的功能來瞭解應用程式使用情況、將流量與使用者和裝置關聯，並運用新一代技術來實施安全政策，藉以達到保護流量安全的效果。

關鍵使用場景與優點

遠端存取 VPN

- 提供對內部及雲端商業應用程式的安全存取。

進階威脅防禦

- 保護網際網路流量的安全。
- 阻止威脅進入端點。
- 防範網路釣魚和憑證竊取。
- 運用固定不變的特徵隔離遭到入侵的裝置。

URL Filtering

- 實施可接受的使用政策。
- 篩選對於惡意網域和成人內容進行的存取。
- 防止使用規避和迴避工具。
- 保護對於 SaaS 應用程式存取的安全。
- 控制存取，並實施 SaaS 應用程式的政策，同時封鎖未批准的應用程式。

自備裝置政策

- 支援應用程式層級 VPN，為使用者保護隱私。
- 為合作夥伴、同事以及承包商提供安全的無用戶端存取。
- 支援非受控裝置的自動識別。
- 支援受控和非受控裝置的自訂驗證機制。

零信任實作

- 提供可靠的使用者辨識。
- 提供快速並準確的主機資訊，以便讓您獲得可視性並執行政策。
- 針對存取敏感性資源，執行更高層級的多因素驗證。

向外延伸平台防護

GlobalProtect 使用新世代防火牆 (在周邊、非軍事區 (DMZ) 或雲端部署為網際網路閘道) 檢查所有流量，從而保護行動工作者。安裝 GlobalProtect 應用程式的筆記型電腦、智慧型手機和平板電腦會使用最佳閘道，自動建立與新世代防火牆的安全 IPsec/SSL VPN 連線，因此能夠掌握所有網路流量、應用程式、連接埠和通訊協定的完整可視性。組織能夠消除行動工作者流量的盲點，持續監控應用程式。

在您的網路中實作零信任

並非所有使用者都需要存取公司網路內的所有資產。安全團隊採用零信任原則區隔其網路，並準確控管對於內部資源的存取。GlobalProtect 為新世代安全平台提供最快速、最權威的使用者辨識，讓您能夠按照業務的需求來擬定準確的政策，以允許或限制用戶的存取。此外，GlobalProtect 提供建立與安全政策相關裝置合規性準則的主機資訊。這些措施可讓您採取預防步驟來保護內部網路的安全、採用零信任網路控制，並降低攻擊風險。

以此方式部署 GlobalProtect 時，可設定內部網路閘道搭配或不搭配 VPN 通道使用。

此外，GlobalProtect 可讓您運用端點的固定不變的特徵來隔離遭到入侵的裝置。這讓管理員能夠限制網路存取，並防止遭到入侵的端點感染其他使用者和裝置。無論受感染的裝置是在外部網路還是內部網路中，都可以套用隔離限制。

流量的檢查和安全政策的實施

GlobalProtect 能夠協助安全團隊制定對於內部或遠端使用者一致的政策。安全團隊可以利用平台的所有功能來阻止網路攻擊得逞：

- **App-ID™** 技術會識別任何連接埠號碼的應用程式流量，並且讓組織按照使用者和裝置來制定政策，管理應用程式使用。
- **User-ID™** 技術會識別使用者和群組成員以取得可視性，並實施以角色為基礎的網路安全政策。
- **SSL 解密**會檢查和控管以 SSL/TLS/SSH 流量加密的應用程式，並阻止加密流量中存在的威脅。
- **WildFire® 惡意軟體防禦服務**會自動進行內容分析，按照行為來識別新的、先前未知的和高針對性的惡意軟體並產生威脅情報，以近乎即時的速度阻止惡意軟體。

- 用於 IPS 和防毒軟體的 **Threat Prevention** 會阻擋鎖定有漏洞的應用程式和作業系統的網路型入侵、拒絕服務 (DoS) 攻擊和連接埠掃描。防毒設定檔使用串流式引擎阻止惡意軟體和間諜軟體進入端點。
- **使用 PAN-DB 的 URL 篩選**會根據 URL 的網域、檔案和頁面的層級的內容將 URL 分類，並獲得 WildFire 的更新，以便網路內容變更時，分類也隨之變更。
- **檔案封鎖**會運用 WildFire 阻止傳輸不需要和危險的檔案，同時進一步審視允許的檔案。
- **數據篩選**能夠讓管理員制定政策從而來阻止未經授權的數據移動 (例如傳輸客戶資訊或其他機密內容)。

安全存取控制

使用者驗證

GlobalProtect 支援所有現有的 PAN-OS® 驗證方法，包括 Kerberos、RADIUS、LDAP、SAML 2.0、用戶端證書、生物特徵登入，以及本機使用者數據庫。GlobalProtect 驗證使用者後，會立即為新世代防火牆提供 User-ID 所用的使用者與 IP 位址的對應關係。

強型驗證選項

GlobalProtect 透過 RADIUS 和 SAML 整合支援多種第三方多因素驗證 (MFA) 方法，包括一次性密碼權杖、證書和智慧卡。

這些選項有助於組織強化存取內部數據中心或軟體即服務 (SaaS) 應用程式所用的身分證明。

GlobalProtect 提供的選項使得強型驗證更容易使用和部署：

- **Cookie 型驗證：**進行驗證後，您可以選擇對於入口網站或閘道的後續存取在該 Cookie 生命週期內使用加密的 Cookie。
- **簡化的證書註冊通訊協定支援：**GlobalProtect 可以自動與企業公開金鑰基礎結構 (PKI) 進行互動，以便管理、發出和分配 GlobalProtect 用戶端的證書。
- **MFA：**在使用者可以存取應用程式之前，可能要求他 (她) 提供其他形式的身分驗證。

主機資訊設定檔

GlobalProtect 會檢查端點來清查端點的設定，並建立與新世代防火牆共用的主機資訊設定檔 (HIP)。新世代防火牆會使用 HIP 來實施應用程式政策，僅允許在端點得到妥善設定和保護時進行存取。這些原則有助於強制遵循規範特定使用者對於特定裝置可進行之存取次數的政策。

HIP 政策能夠以許多屬性為依據，包括：

- 受管理/非受管理裝置識別
- 存在於裝置上的電腦證書
- 從行動裝置管理員收到的裝置資訊
- 作業系統和應用程式修補程式等級
- 主機防惡意軟體版本和狀態
- 主機防火牆版本和狀態
- 磁碟加密設定
- 數據備份產品設定
- 自訂主機狀態 (例如，登錄項目、執行中的軟體)

應用程式和數據的存取控管

安全團隊能夠以應用程式、使用者、內容和主機資訊為基礎而建立政策，以便對於向特定應用程式進行的存取維持精密的控管機制。這些政策可能與目錄中定義的特定使用者或群組相關聯，以確保組織按照業務需求提供正確的存取層級。安全團隊能夠進一步制訂更高層級的 MFA 政策，以便在存取特定的敏感性資源與應用程式之前，提供額外的身分證明。

提升疑難排解能力和可視性

GlobalProtect 應用程式控管中心 (ACC) Widget、報告，以及新的 GlobalProtect 日誌會對您部署中的 GlobalProtect 使用情況，提供完整可視性。分階段詳細記錄連線工作流程可大大簡化使用者連線問題的疑難排解過程。當特定使用者有問題時，此記錄可讓系統管理員輕鬆地識別連線程序中的階段/事件。

安全啟用 BYOD

自備裝置 (BYOD) 政策的影響正在改變許多安全團隊需要支援的使用情境之數量。必須為使用更多種行動裝置，類型更多樣的員工與承包商提供應用程式存取權。

整合 AirWatch® 與 MobileIron® 等行動裝置管理產品能夠協助您部署 GlobalProtect，並且透過交換情報與主機設定，提供額外的安全措施。若與 GlobalProtect 結合使用，貴組織便能夠以個別應用程式為基礎，維持可視性和安全政策的執行，同時將數據與個人活動分離，以滿足使用者在 BYOD 情境中所需要的隱私。

GlobalProtect 支援無用戶端 SSL VPN，以便從未管理的裝置安全存取數據中心以及雲端內的應用程式。這種方法允許客戶透過 Web 介面存取特定的應用程式，而無需使用者安裝用戶端，也無需設定 VPN 通道，就可以使從 BYOD 裝置連線的第三方使用者和員工能夠進行安全存取。

架構的重要性

彈性的 GlobalProtect 架構提供許多功能，有助於您解決多種安全性挑戰。基本上，您能夠使用 GlobalProtect 取代傳統的 VPN 閘道，因此不需要進行繁雜的獨立式第三方 VPN 閘道管理。

手動連線和閘道選取的選項能夠讓您自訂設定來支援所需的業務需求。

為了保護流量安全而進行更全面的部署，GlobalProtect 可以搭配有全通道而且持續不中斷的 VPN 連線進行部署，確保能夠持續防護，而且完全不干擾的使用者體驗。您可以針對注重延遲的流量，依應用程式、網域名稱和路由或視訊流量來定義例外。

雲端匣道

工作者在不同地點之間移動，流量負載也會隨之變動。考量公司發展的情境時，無論是暫時 (例如，自然災害後) 還是永久 (例如，進入新市場時)，情況都是如此。

Palo Alto Networks 所推出 Prisma™ Access 能夠使用您的安全政策，為組織所需位置的部署提供共同管理選項。該服務能夠跟您現有的防火牆結合運用，讓您的基礎架構能夠針對條件的變動進行調整。

Prisma Access 支援自動調整，能夠根據特定區域的負載和需求，動態配置新的防火牆。

結論

Palo Alto Networks 新世代防火牆對於防範入侵而言相當重要。GlobalProtect 可用來將平台的保護擴大到在任何地點的使用者。使用 GlobalProtect 後，您就可以一致地實施安全政策，因此，即便使用者離開工作地點，防範網路攻擊的措施仍然持續有效。

表 1：GlobalProtect 功能

類別	規格
VPN 連線	IPsec
	SSL
	無用戶端 VPN
	Android、iOS 上個別應用程式的 VPN
閘道選取	自動選取
	手動選取
	選取優先使用的閘道
	根據來源位置進行外部閘道選取
	根據來源 IP 進行內部閘道選取
連線方式	使用者登入 (始終開啟)
	按需要
	預先登入 (始終開啟)
	預先登入後按需要
	使用者啟動的預先登入
連線模式	內部模式
	外部模式
第 3 層通訊協定	IPv4
	IPv6
單一登入	SSO (Windows 憑證提供者)
	Kerberos SSO
	適用於 macOS 的 SSO
分割通道	包括路由、網域、應用程式
	排除路由、網域、應用程式

表 1：GlobalProtect 功能 (續)	
驗證方法	SAML 2.0
	LDAP
	用戶端證書
	Kerberos
	RADIUS
	雙因素驗證
	根據作業系統或裝置擁有權，選擇驗證方法
HIP 報告、政策執行和通知	修補程式管理
	主機防間諜軟體
	主機防惡意軟體
	主機防火牆
	磁碟加密
	磁碟備份
	數據遺失防護
	自訂 HIP 狀態 (例如，登錄項目、執行中的軟體)
受控裝置識別	依電腦證書
	依硬體序號
MFA	在連線時和資源存取時
其他功能	User-ID
	IPsec 到 SSL VPN 的遞補
	對網路存取執行 GlobalProtect 連線
	根據使用者位置設定通道
	HIP 報告重新分配
	HIP 中的證書檢查
	SCEP 式自動使用者證書管理
	在執行階段前後執行的指令碼動作
	動態的 GlobalProtect 應用程式自訂
	根據使用者、群組與/或作業系統設定應用程式
	自動內部/外部偵測
	手動/自動升級 GlobalProtect 應用程式
	OID 的證書選擇
	封鎖遺失、遭竊與未知裝置的存取
	連線/中斷連線的智慧卡支援
	針對 SSL 解密，透明地分配受信任的根憑證授權單位
	停用對本機網路的直接存取
	自訂歡迎與幫助頁面
	至遠端用戶端的 RDP 連線
	作業系統原生通知
	使用者登出限制
	Proxy 支援
	執行 GlobalProtect 排除
	僅透過 SSL 連線
	RSA 軟體語彙基元整合
	裝置隔離

表 1：GlobalProtect 功能 (續)	
MDM/EMM 整合	AirWatch
	MobileIron
	Microsoft Intune
管理工具和 API	Palo Alto Networks 新世代防火牆，包括實體和虛擬設備
	Prisma Access
	Panorama 網路安全管理
支援 GlobalProtect 應用程式的平台	Microsoft Windows 與 Windows UWP
	Apple macOS
	Apple iOS 和 iPadOS
	Google Chrome OS
	Android OS
	Linux OS (Red Hat、CentOS、Ubuntu)
	物聯網裝置
IPsec XAuth	Apple iOS IPsec 用戶端
	Android 作業系統 IPsec 用戶端
	第三方 VPNC 和 StrongSwan 用戶端
GlobalProtect 應用程式本地化	中文、英文、法文、德文、日文、西班牙文

paloalto NETWORKS

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 號台北南山廣場 34 樓

strata-globalprotect-ds-060120