在 *Palo Alto Networks* 實作零信任的最佳做法

9.1

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

December 18, 2019

Table of Contents

零信任的最佳做法

本文件說明什麼是「零信任」策略，以及如何使用分為五個步驟的方法，藉由最佳做法引導您將該策略實作至您的網路；包括識別您的重要保護面、對應您的重要交易流程、建構您的零信任網路、建立零信任政策，以及維護部署。章節內容含有從 Palo Alto Networks 取得詳細資訊的連結，包括如何設定新世代防火牆 (實體及虛擬) 和出自 Palo Alto Networks 的安全功能，避免資料外洩。

> 什麼是零信任？我為何需要它？
> 零信任的觀點
> 五步驟方法
> 零信任的資源

什麼是零信任？我為何需要它？

零信任是業務主導的策略性方法，根據保護面中特定業務的重要項目，除了保護您最重要的資料、應用程式、資產和服務 (DAAS) 之外，也包括您的使用者在內。零信任策略不分基礎結構，可套用至所有實體和虛擬位置，例如網路、公共雲端、私人雲端和端點。零信任背後的概念相當簡單：信任即弱點。數位環境中的一切皆不可信任，包括封包、身份、裝置或服務，因此全部予以驗證。一概沒有預設信任。

實作此策略並非只做一次就能在網路之間如法炮製，因為每個環境與保護面各不相同，隨著業務逐漸改變，目標與 DAAS 元素也會改變。策略依業務而特定，安全性策略也依照保護對您的特定業務而言重要的事物而有所特定。

零信任策略的目標是去除網路中的信任。去除信任有助於預防資料外洩成功、透過自動化和縮減規則庫以簡化操作，加上因為零信任環境正是針對合規與便於稽核所設計，所以能簡化合規與稽核。

零信任的觀點

待您了解零信任，就能看出信任的真面目；那是攻擊者入侵所利用的弱點。攻擊者能盜取認證、偽造封包標頭中的資訊，甚至假冒「受信任」的員工或合作夥伴。Edward Snowden 是受信任的使用者，其工作站上有適當的防毒軟體和正確的修補程式層級。他也使用多因素驗證。但因為身為受信任的使用者，無人在意他從哪裡登上網路或是產生了哪些封包，於是他就能探索網路，找尋並且洩漏敏感資料。從這個例子學得的教訓就是，數位信任的後果等於數位背叛；切勿信任身分、應用程式或資料。只要採取零信任的觀點，您就能：

- 讓安全性符合業務職能，因為業務職能決定您所需保護的項目。
- 當這些職能存取資源時，可檢查並記錄第七層的所有封包。
- 不計位置，以安全的方式存取所有資源。
- 對所有位置套用一致的安全性政策。
- 集中管理安全性和區隔政策。
- 隨著您的業務變化採行變更。

信任是您藉由實作零信任策略而規避的失敗點。

- 零信任高階最佳做法
- 如何開始我的零信任實作？

零信任高階最佳做法

實施下列最佳做法可做好準備，並協助您將網路移轉至零信任架構：

- 建構零信任環境之前，定義想要的業務成果。零信任模型可支援並促成安全的業務功能。
- 由內而外設計而非由外往內，可優先保護對您的業務最寶貴的部分。您最寶貴的資產更有可能在資料中心，而非位於周邊。
- 使用能減少總擁有成本、整合式的集中管理平台，避免共同運作效果不強的單點產品集合。Palo Alto Networks 能在平台元素之間共用資訊，使用 Panorama、GlobalProtect 及 Prisma Access 達成中央管理，簡化操作，遍及所有位置提供一致的政策、防範及保護。
- 以 Palo Alto Networks 新世代防火牆作為區隔閘道，將安全性的技術合併至一個平台，使用 App-ID、User-ID 及 Content-ID 於第七層原生性質地對所有位置套用一致的安全性政策。區隔閘道能基於應用程式、使用者和資料將網路加以分段與控制，因為跨越微周邊，取得對保護面的存取權，所以應當提供精細存取控制，保護所有流量。

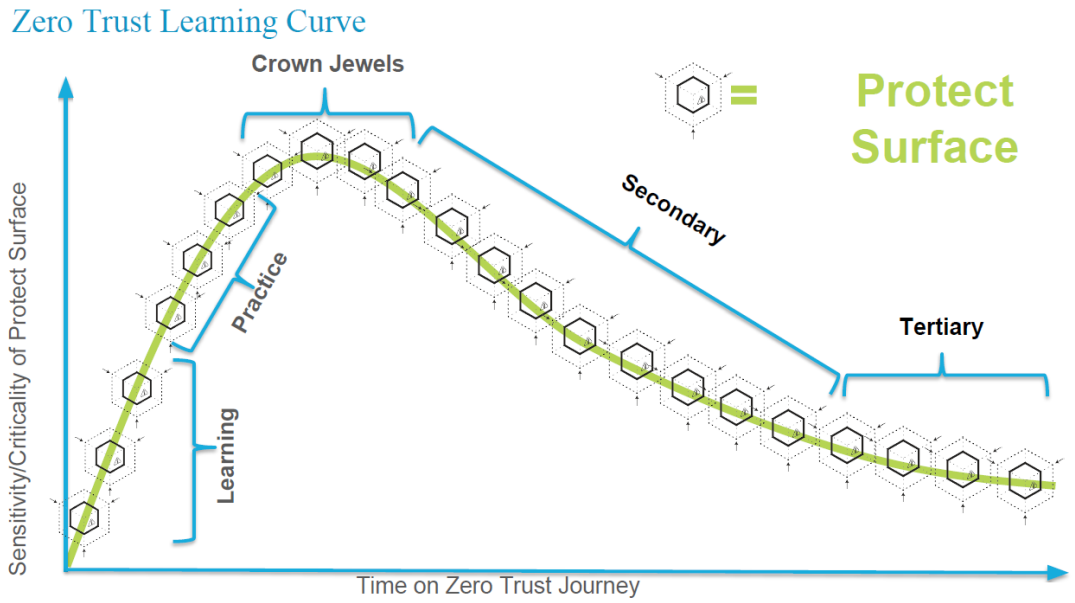
  您不需要為了建立微周邊而變更基礎結構，因為是在第七層政策中建立微周邊，僅允許授權使用者存取為了業務目的所需存取的保護面。
- 基於對業務而言寶貴的項目將網路分段，防止未授權的橫向移動。
- 對您的保護面套用最低權限存取原則。判定誰需要存取哪些資源、需要如何存取，及何時需要存取。僅允許各使用者和裝置所需的確切存取層級、判斷身分 (包括適當授權)，接著將第七層政策對應到身分。
- 將法規、合規和業務作法允許您檢查的每個封包透過第七層加以解密、檢查及記錄。您必須檢查並記錄第七層流量。記住，每個攻擊者都知道如何繞過第三層和第四層的安全性控制。
- 為標記工作負載到群組物件和動態性地註冊標籤建立策略，以利安全性政策的自動化。
- 開發程序以隨著您開發策略、設計網路，操作、維護及持續更新防範控制。將程序做成正式記錄、教育並訓練人員，設立基準線，對照基準線度量進度。
- 一次一個分段地逐漸移轉至零信任環境，並且從一或多個非關鍵分段開始，以從中學習，累積經驗。零信任分段與傳統分段共存，您可使用安全、反覆的方式，不必採取去除後換新的冒險方式。

因為應用程式的重要性降低，您在於保護可降低激進性。例如，不需要對聊天應用程式套用與業務關鍵應用程式相同的保護。與業務領導人協同作業有助於判定哪些應用程式是保護的最關鍵對象。

如何開始我的零信任實作？

教育和協同作業開啓走向零信任安全性這段旅程。您與識別哪些事項對您的業務特別有價值、以及如何加以保護的其他利害關係人，需要瞭解零信任的概念、原則和目標。

1. 建立追求卓越的零信任中心。這是業務領導人 (業務和技術決策者)、IT、資訊安全性、基礎結構、應用程式開發人員及其他利害關係人組成的跨職能團隊。此團隊定義並識別各個保護面與組成各保護面的資料、應用程式、資產及服務 (DAAS 元素)。他們為您的業務訂定最具價值保護面的優先順序，以及規劃和實作零信任策略。此團隊隨著業務變化，始終參與部署的維護。業務領導人可以談想要的業務結果、合規要求和業務資產的價值。
2. 參加零信任研討會，讓大家做好準備，並且一致向前。請聯絡您的 Palo Alto Networks 銷售代表，取得更多資訊並且排定研討會時程。
3. 依照 五步驟方法 對應您所想建置的分段網路。
4. 從一或多個小型、非常瞭解的低風險 (對業務運作非關鍵性) 區段開始移轉，以從經驗中學習。勿從重要資產開始。接著，對一或多個練習區段測試您的學習成果。當您覺得準備好時，將業務上最關鍵的保護面 (組成保護面的 DAAS 元素) 置入零信任微周邊，每個保護面一個微周邊。之後，將其次一組最寶貴的保護面轉換為零信任，依此類推。



五步驟方法

這套實作零信任策略的五步驟方法呈現具有邏輯性的清晰路徑，能保護您的環境、資料、應用程式、資產、服務和使用者。您套用方法的方式取決於您所保護的項目和業務需求 (屬您業務的關鍵)，不過您所朝向的目標是一致的：

- 高效且有效率地區隔網路，防止橫向移動。
- 保護業務關鍵資料和系統，避開未經授權的應用程式與使用者。
- 保護業務關鍵應用程式，避免未經授權之下遭到存取與使用。
- 橫跨網路、雲端和端點無縫強制實施政策，以簡化管理，並且遍及所有位置套用一致的政策。

這套五步驟方法無論是要將零信任政策實作到雲端、私人網路或是端點上，不分基礎結構皆能適用。

步驟 1：定義您的保護面

保護面是對您的業務而言相當寶貴的項目：您為了確保業務正常運作，所需要保護的資料、應用程式、資產和服務 (DAAS)。定義您的保護面可讓您專注在保護對業務真正重要的項目，而非嘗試識別並保護整個攻擊面，或僅專注於周邊。保護面也比攻擊面或周邊小了許多，因此更容易保護。

請基於對業務最重要的 DAAS 元素來定義保護面：

- 資料。需要保護的是什麼資料？您可考慮智慧財產，例如專屬程式碼或程序、可識別個人的資訊 (PII)、支付卡資訊 (PCI) 及個人健康資訊 (PHI)，例如健康保險便利和責任法案 (HIPAA) 的資訊。
- 應用程式。哪些應用程式會使用敏感資訊？哪些應用程式是您業務職能的關鍵？
- 資產。哪些資產最敏感？取決於您的業務，可能是 SCADA 控制、POS 終端、醫療設備、製造設備及關鍵伺服器群組。
- 服務。攻擊者能入侵哪些服務以擾亂 IT 作業並對業務有負面影響，例如 DNS、DHCP 及 Active Directory？

各關鍵 DAAS 元素皆為保護面的部分 (或部分情況下為一保護面)。例如，若您的業務提供健康照護，則個人健康資訊 (PHI) 是您的業務關鍵。資料是患者資訊。應用程式是存取 PHI 資料所用的應用程式—例如 EPIC。資產是儲存資料的伺服器和產生 PHI 的設備，例如醫療掃描器或醫師的工作站。服務是存取資料所用的服務，例如單一登入和 Active Directory。

隨著您依照五步驟方法，會將各保護面放在其本身的微周邊 (以 Palo Alto Networks 實體或虛擬的新世代防火牆作為區隔閘道加以區隔)，因此您可控制具體由誰存取元素、如何存取以及何時存取。以對該保護面適當的方法保護各個保護面。微周邊的管理與防護，比環繞存取要求不同的使用者所需與之通訊的 DAAS 元素所形成的寬廣周邊更為容易。也能將保護措施移為更接近關鍵資料。

請基於執行業務的關鍵為何，決定優先保護的項目。您最寶貴的資產往往位於資料中心或在雲端。您對一或多個非關鍵保護面實作零信任以獲得經驗之後，請防護最關鍵的保護面。您在開始時可能不知道資料中心內的所有應用程式，但知道最關鍵的應用程式。之後，請繼續進行優先順序清單中的下一組保護面，並持續到達成安全性的目標為止。

您可使用下列工具獲取對網路流量的可視性，協助識別組成最關鍵保護面的 DAAS 元素：

- 團隊的業務知識。例如，業務領導人可談論應用程式的策略價值。
- 將一或多個新世代防火牆以虛擬介接 (vwire) 模式透明地置入您的網路，該模式屬於通過模式，因為 vwire 介面沒有 IP 或 MAC 位址，所以無需變更拓樸即可對流量獲取可視性。查看流量日誌以檢視並分析網路流量。若您的網路中已有受管理的防火牆，請使用 Panorama 記錄。

- 在 Cortex 資料湖中檢視記錄，並使用 Palo Alto Networks 的整合合作夥伴出品、適用於 Cortex 的協力廠商資產探索工具。
- 使用 Prisma SaaS 探索 SaaS 應用程式的使用者、資產和資料，並獲取對這些應用程式的可視性。
- 若您在新世代防火牆或管理防火牆的 Panorama 上執行 PAN-OS 9.0 或更新版本，請使用政策最佳化工具協助識別現有安全性政策規則的主要應用程式。(政策最佳化工具甚至能為您顯示基於連接埠的規則的所有應用程式 。) 若您無法使用政策最佳化工具，請使用 Expedition 獲取對應用程式的可視性。
- 應用程式相依性對應工具能自動探索應用程式的相依性 (應用程式使用的資源，例如資料庫、負載平衡器、伺服器等)。

步驟 2：對應保護面的交易流程

對應關鍵 DAAS 元素與使用者之間的交易流程 (互動)，以瞭解其相互依存性，亦即誰有業務理由應可存取各元素、以何種方式，以及在何時機。您可對應交易流程，以便瞭解並建構網路。對應可協助您瞭解如何建立安全性政策，僅允許授權使用者使用指定應用程式存取特定資料和資產 (最低權限存取原則)。

有許多方式可對應交易流程，部分定義保護面的技巧也能適用於對應其交易流程：

- 如果現有流程圖，可以利用 (合規與稽核有時會要求企業建立流程圖)。
- 與應用程式、網路、企業架構師和業務代表合作，瞭解應用程式的宗旨以及架構師和業務代表構思的交易流程。
- 以虛擬介接 (vwire) 模式對網路透明地置入一或多個新世代防火牆，以取得對流量的可視性。查看流量日誌以檢視並分析流量。
- 使用 Palo Alto Networks 整合合作夥伴的協力廠商工具。
- 使用 Cortex Data Lake 的日誌資訊取得對交易流程的可視性，並加以對應。Cortex Data Lake 可從新世代防火牆、VM-Series 防火牆、Prisma Access 和 Traps 彙總日誌。
- 對於應用程式，請對應工作流程，包括全網路的應用程式資料流程、各應用程式所需的運算物件，以及各應用程式由誰使用。
- 對於資料，請找出使用資料的是誰；您收集、儲存、使用及傳輸資料的位置，以及資料用後是如何儲存、加密、封存或銷毀。
- 對於資產，請找出資產的位置、使用資產的是誰、何時使用資產，及資產於何處納入工作流程。
- 對於服務，請對應全環境的服務工作流程。

除了能夠得知誰、何處與何時使用哪些應用程式之外，對應交易流程可提供精細的可視性，有助於嚴重損壞修復規劃和合規。也能給您機會優化工作流程，檢視誰有合理業務理由可存取各保護面的 DAAS 元素。

當您瞭解經由網路的交易流程，就能知道如何將網路分段，以及在何處插入控制項，因為您能瞭解各保護面由誰使用、如何使用、位在何處，以及哪些元素互動以促成各關鍵應用程式運作。

步驟 3：建構零信任網路

在擁有對保護面和交易流程的瞭解之下，您可基於對業務別具價值的事物，開始建構零信任網路。由內而外，建構您在 步驟 1：定義您的保護面 中識別的業務關鍵保護面。隨著您開發架構，請牢記在輕鬆操作與維護和彈性之下，順應保護面與業務的變化。執行最佳做法評估工具以設立最佳做法設定的基準線，並且度量朝向零信任目標的進度。

架構的基石在於區隔閘道，亦即以實體或虛擬 Palo Alto Networks 新世代防火牆連接您的網路區段，並且強制實施第七層政策。經由區隔閘道運作所有流量、讓區隔閘道盡可能靠近所保護的資源，並搭配其他 Palo Alto Networks 功能使用，能達到最大自動化。新世代防火牆：

- 環繞各個保護面，在第七層政策中建立微周邊。如此可防範橫向移動，因為微周邊能提供精細的政策控制，包括誰 (User-ID) 以什麼方式 (Content-ID) 在什麼時間經由區隔閘道存取哪些應用程式 (App-ID) 和資源。您可基於交易如何流經網路，以及使用者和應用程式如何存取資料與服務來進行區隔。
- 將安全性功能彙總成為單一控制點，囊括進出保護面的所有流量。區隔閘道應當強制實施政策、將加密的流量解密，並且套用保護，例如：

    - DNS 安全性 (使用 DNS 安全性 服務，其提供多方即時威脅情報來源、對 DNS 請求的無限可調整即時分析，和進階 DNS 特徵碼)。
    - 入侵防禦 (弱點保護、反間諜軟體及防毒設定檔)。
    - 封鎖有潛在危險性的檔案類型。
    - 防範未知和 Day 1 威脅 (WildFire)。
    - URL 篩選。
    - 資料遺失防護 (DLP)。
- 即時解密並檢查第七層的流量。
- 記錄第二層至第七層的每一個封包。針對受管防火牆從 Panorama、從個別防火牆 (未受 Panorama 管理的防火牆)、從 Prisma Access (原為 GlobalProtect™ 雲端服務) 和從 Traps 傳送日誌到 Cortex Data Lake，針對實體和 VM-Series 防火牆集中並彙總您內部和虛擬 (私人和公共雲端) 的日誌儲存區。
- 使用 API，以與合作夥伴出品的協力廠商防禦工具密切整合。
- 將偵測事件並將回應自動化的回饋迴圈自動化。
    - 標記工作負載並以標籤作為篩選準則，藉以判斷安全性政策中的動態位址群組成員。如此可讓您基於到 HTTP(S) 伺服器的日誌轉送事件將動作自動化。日誌轉送事件觸發動作的方式是即時動態性地新增或移除安全性政策中使用的動態位址群組成員。由安全性政策判定動態位址群組的成員獲得允許或遭到拒絕存取，並由防火牆強制執行動作。例如，在反間諜軟體安全性設定檔中設定 DNS Sinkhole 以自動隔離企圖存取 Sinkhole 的潛在受危害系統。使用標記和日誌轉送動態性地從附加到政策規則的動態位址群組新增及移除這類系統，其中政策規則可封鎖並記錄通往 Sinkhole 位址的所有流量。於是您便能應日誌警示的通知，調查潛在受危害系統。
    - 使用 Cortex XDR 自動分析您的網路、探索指出潛在入侵跡象的異常行為，並就該行為提供警示，以便您能調查並修復問題。Cortex XDR 可提供對網路流量的可視性、將日誌交互關聯而簡化對威脅的調查，讓您能識別警示的根本原因，立即回應。使用 Cortext XDR API 以與 Demisto 整合，並使用依您的業務工作流程量身訂做的 Desmisto 回應劇本自動回應，將回應時間從數日縮短為數分鐘。
    - 使用 WildFire 自動探索新的惡意軟體。WildFire 探索出世界上的任何位置有惡意軟體時，至多花五分鐘，WildFire 就能更新您的安全性設定檔，為您防範新的惡意軟體。
- 使用 Panorama 中的範本和範本堆疊以將政策部署自動化。
- 使用工具，例如 Ansible、Terraform 和 Python 以自動化、協調及加速對於 Prisma 雲端部署的保護。

Palo Alto Networks 可供您建構零信任環境，遍及所有位置套用一致的安全性：

- Panroma 集中控制多重新世代防火牆的管理政策，與個別管理防火牆相較之下操作效率更高。
- 企業網路與資料中心：使用新世代防火牆，將網路區隔成為您的保護面的微周邊。
- 公共雲端：使用 Prisma Access，其使用內部或 VM-Series 新世代防火牆，以及 Prisma Cloud (API 型雲端基礎結構安全性解決方案) 實作雲端環境的零信任政策。虛擬私人雲端 (VPC) 定義保護界限，以區隔工作負載。
- 私人雲端：使用 VM-Series 防火牆實作零信任政策。
- 分公司與行動使用者：使用 Prisma Access 提供雲端型安全性，避免與企業網路資源之間的來回行程。設定使用者適用的 Prisma Access 和網路適用的 Prisma Access 以保護分公司的安全。

  或者，使用內部的新世代防火牆搭配 GlobalProtect 訂用服務以將安全性政策與強制作業延伸至遠端使用者和分公司。
- 端點：針對區隔與第一層保護使用新世代防火牆分層保護，第二層保護則使用 Traps。使用 GlobalProtect (內部安裝) 或 Prisma Access (使用 Panorama 所安裝，並代您於雲端管理) VPN 強制實施一致的政策，將政策延伸至遠端端點，讓政策隨使用者移動。Prisma Access 要求行動使用者端點上有 GlobalProtect 應用程式。無論何種情形，請將 GlobalProtect 應用程式安裝在受管 端點，至於未受管端點 (無法、或不想設置代理程式的端點，例如合作夥伴的系統或個人的裝置) 則使用 GlobalProtect Clientless VPN。請視保護高價值資產所需，適當地套用多因素驗證。
- SaaS 應用程式：使用 Prisma SaaS 掃描、分析、分類及協助保護 SaaS 應用程式。對於未受管理的裝置，請經由新世代防火牆將 SaaS 應用程式的流量重新導向 (受管理的裝置的流量通過 Prisma Access、GlobalProtect 或新世代防火牆)。

步驟 4：建立零信任政策

零信任政策由白名單規則所組成—亦即僅允許獲得授權的使用者在正確的時間於適當位置使用指定的應用程式存取特定資源的規則。如果流量不符合規則，防火牆會自動封鎖該流量。這之所以重要的原因如下：

- 知道您為了支持業務所想允許的應用程式，要比承擔識別及封鎖一切不想允許的應用程式這種無窮無盡的任務，來得簡單許多。
- 所有外洩和惡意活動都發生在允許規則上。請將安全性專注在您允許的流量，並僅允許業務所需的流量。

零信任政策是基於 Kipling 法。回答 Rudyard Kipling 的 6 元組問題「誰、什麼、何時、何地、為何及如何」，您可以知道如何決定允許、還是封鎖流量，以及如何建立能夠防衛各保護面的安全性政策。Palo Alto Networks 以安全性政策提供實作 Kipling 法的功能：

- 誰應當存取資源？
  - User-ID 可識別使用者，讓您能以政策控制誰能存取資源。透過最低權限存取 (誰需要知道？) 的透鏡，僅將存取權允許給予具合理的業務理由，得存取資源的個人、群組和裝置。
  - 建立驗證政策，以於使用者嘗試存取資源時確認其身分。驗證政策也決定是否需要多因素驗證 (MFA)。
  - 使用 MFA 以保護敏感的服務和應用程式，作法是除了在被控制的入口網站中輸入密碼之外，另要求滿足至少一項驗證因素，例如傳送至手機或或電子郵件的一次性代碼，之後防火牆才會允許存取敏感的服務、應用程式和資源。如為遠端使用者，請設定 GlobalProtect 以實施 MFA 通知 (您也必須在防火牆上設定 MFA)。
  - 如為使用 GlobalProtect 的裝置，請設定主機資訊設定檔 (HIP) 以定義主機的存取政策、強制對這些主機實施政策，並防止未符合安全性和維護標準的裝置存取資源。例如，您可使用 HIP 以確保端點啟用加密、主機的防毒特徵碼為最新版本。如果主機未符合 HIP 的要求，安全性政策會封鎖存取。
- 用什麼應用程式存取資源？
  - 建立基於應用程式的第七層政策時會使用 App-ID，其不分連接埠、通訊協定或規避戰術皆能識別應用程式，讓您僅允許網路上存在適當的應用程式。基於第三層和第四層的政策倚賴 IP 位址，攻擊者能偽造並使連接埠保持對規避應用程式開放。
  - 將服務設定為依應用程式預設以安全地在預設連接埠上啟用應用程式，防止規避的應用程式從非標準連接埠存取您的網路。
  - 如果防火牆執行 PAN-OS 9.0 或更新版本、或執行 PAN-OS 9.0 或更新版本的 Panorama 設備管理執行 PAN-OS 8.1 或更新版本的防火牆，請用政策最佳化工具檢查現有政策規則 (應用程式為主規則和傳統式連接埠為主規則)、識別未使用的規則，及識別有未使用應用程式的規則。如為執行早期版本 PAN-OS 的防火牆，請使用 Expedition 檢查政策規則。(如您需要將傳統設定移轉至 PAN-OS 裝置，請依照移轉至基於應用程式的政策的最佳做法。
- 使用者何時存取資源？

  如為使用者僅於某些時段存取的應用程式，請套用排程 (Panorama 設備和防火牆上的 **Objects**（物件）> **Schedules**（排程）) 至政策規則，防止不用的時段發生可疑的存取。攻擊者經常在正常上班時段外攻擊和企圖洩漏資料，以減少被發現的機會。
- 資源位於何處？

  請加入政策之目的地資源位置。適當時，也請限制流量的來源 (區域和 IP 位址)。
- 為何資料被存取—資料遺失的代價 (毒性) 為何？

  將資料分類以瞭解其毒性—為何該資料值得保護？如果攻擊者洩漏該資料，您是否必須揭露遺失？設定資料篩選以防敏感資訊離開您的網路，並使用資料分類工具提供關於資料的中繼資料。瞭解資料的毒性有助於您瞭解如何保護資料、資料使用後如何處理，及如何在政策中標記其的使用。
- 您應當如何允許存取資源？

  套用 Content-ID 和最佳做法以防禦應用程式流量中的威脅：
  - 將最低權限存取的理念運用到安全性政策。僅允許具有合理業務理由的使用者，於適當時間以妥善的方式存取為了業務用途之所需存取應用程式。

- 記錄透過第七層的所有內部與外部流量。防火牆政策規則預設為啟用記錄。請轉送日誌至 Cortex 資料湖 (或至 Panorama 或日誌收集器) 以合併日誌，享有更簡易也更徹底的分析。
- 橫跨所有位置 (網路、雲端、端點) 一致地為所有本機和遠端的使用者套用政策和威脅防護，以便政策適用於所有應用程式和所有資源，跟隨使用者至任何位置。政策不一致會增加弱點、難以瞭解及維護，恐怕對合規要求和稽核有負面影響。請使用實體新世代防火牆與虛擬 VM-Series 防火牆作為區隔閘道，在網路和雲端套用一致的零信任、第七層、Kipling 法政策。使用 Prisma Access (雲端) 和 GlobalProtect (內部安裝與使用 Prisma Access) 將一致的零信任政策延伸至端點。如為未受管的端點 (您不想、或無法放置代理程式的端點)，請使用 GlobalProtect Clientless VPN 套用一致的政策。請建立並重複使用 Panorama 範本和堆疊以遍及類似的位置 (例如資料中心或周邊) 套用一致的政策。
- 設定安全性設定檔 (IPS 的弱點保護設定檔、防毒和 WildFire 設定檔以防禦惡意軟體，包括當日惡意軟體；反間諜軟體設定檔以防範命令和控制威脅、檔案封鎖設定檔以封鎖或警示有風險的檔案類型，及 URL 篩選以控制網站存取、協助防範網路釣魚攻擊，及對搜尋引擎強制安全搜尋) 並套用至所有允許的流量。請遵循資料中心防火牆和周邊防火牆安全性設定檔的最佳做法。
- 使用 WildFire 最佳做法偵測及防範零時差惡意軟體。
- 使用解密最佳做法將法規與業務要求讓您解密的流量盡皆解密，以便盡可能檢查多的流量。您無法保護您的網路遠離看不見的威脅。
- 使用 DNS 安全性服務對於 DNS 特徵碼、DNS 要求的即時分析和使用機器學習與預測性分析產生的進階 DNS 特徵碼，提供無限可調的即時存取權。
- 「如何」也包括判定敏感資料使用後續應如何處理—例如使用加密加以抽象化、權杖化，或遮罩，或以封存或刪除方式處置。封存陳舊資料 (大多數系統上約有 80% 的資料未經存取達二年以上)。
- 使用 Cortex XDR 提升並改善政策。

Kipling 法因為能使您瞭解誰應該有存取權、其應如何存取、何時應存取，以及套用的保護措施，所以可讓您建立能妥善防禦各保護面的安全性政策。您開發政策規則的做法是基於 Kipling 法開發業務聲明。例如：

	誰	什麼	何時	何處	為何	如何
方法	使用者-ID	App-ID	時間限制	系統物件	分類	內容 ID
內部	Epic 使用者	Epic	任何	Epic 伺服器	有毒 (資料具高價值)	解密、檢查 (安全性設定檔)、記錄流量
雲端	銷售	Salesforce	工作時段	美國	有毒 (資料具高價值)	解密、檢查 (安全性設定檔)、記錄流量

這兩個案例中，防火牆僅允許滿足 Kipling 元組中所有的條件並通過檢查的流量通過。防火牆會自動拒絕有一條允許規則未符合的所有流量。

除了安全性、驗證和解密政策之外，也請使用 DoS 和區域保護最佳做法保護重要伺服器，免於拒絕服務 (DoS) 攻擊。

如為您尚未設定的防火牆，請使用 IronSkillet Day 1 設定範本實作 *Day 1* 最佳做法政策，再依照最適合您的保護面的方式調整政策。

步驟 5：監控並維護網路

安全性是反覆的程序，因為記錄和監控能透露應作出的改善，也因為您的業務和網路會逐漸改變。請依照您在建構網路時開發的操作程序，以維護並持續更新預防控制措施。

- 解密、檢查並記錄所有流量 (內部及外部) 直至第七層。

- 針對受管防火牆從 Panorama、從個別防火牆 (未受 Panorama 管理的防火牆)、從 Prisma Access 和從 Traps 轉送日誌到 Cortex Data Lake，集中並彙總您內部和虛擬 (私人和公共雲端) 的日誌儲存區。如此可對您的網路流量和保護面提供可視性。
- 更新政策，亦可能基於 Cortex XDR 提供的智慧新增保護面，其使用 Cortex Data Lake 的資料和機器學習以根據您網路的正常行為自動分析網路，並識別異常行為，可能表示有入侵或其他威脅。以不在保護面的 DAAS 元素為目標的威脅活動，可凸顯您最初定義保護面時未考慮的保護面。
- 使用 Cortex XDR 獲取對網路流量的可視性、將日誌交互關聯而簡化對威脅的調查，讓您能識別警示的根本原因，立即回應。
- 使用 Cortext XDR API 以與 Demisto 整合，並使用依您的業務工作流程量身訂做的 Desmisto 回應劇本自動回應，將回應時間從數日縮短為數分鐘。
- 使用 Prisma Cloud 進行彙整，並提供對於設定資料、使用者活動資訊和網路流量資訊的可視性。Prisma Cloud 能分析資料，傳遞簡明又可行動的洞見。
- 依照應用程式與威脅內容更新的最佳做法取得新的及修訂的 App-ID，同時讓威脅特徵碼保持為最新。
- 使用最佳做法評估工具度量朝向最佳做法設定的進展，也協助您移轉至最佳做法的安全性狀態。
- 監控網路活動，使用預先定義的報告，並產生自訂報告以對您的環境取得可視性。
- 保持跨職能團隊的聯繫，隨著網路和業務演進持續維護零信任的部署，並且建立教育與訓練，以確保團隊的新成員瞭解策略及實作。
- 隨著自動功能演進，繼續將行動和回應自動化。

零信任的資源

下列技術文件、白皮書、網路廣播、影片及其他資源可為您提供零信任策略的更多資訊和背景資料。除了本文件中的資訊和列出的資源之外，亦可請 Palo Alto Networks 專業服務的專家團隊協助您設計及實作零信任策略。

- 如何建置零信任網路 (隨選網路廣播)
- 破解實作零信任的相關迷思 (隨選網路廣播)
- 零信任介紹
- 零信任 (Palo Alto Networks 的零信任網頁)
- 零信任之上執行的最佳做法 (轉型發展藍圖)
- 使用五步驟方法簡化零信任的實作 (白皮書)
- 保護雲端安全：零信任雲端的安全性
- 零信任雲端的安全性 (影片)
- 關於零信任的真相 (資訊圖表)

Palo Alto Networks 技術文件

轉移至最佳做法：

- BPA 入門
- 如何執行 BPA (影片)
- 瞭解 BPA 結果 (影片)
- 即時社群最佳做法評估頁面

最佳做法文件入口網站：

- 最佳做法入門
- 網際網路閘道最佳作法安全性政策
- 資料中心最佳做法安全性原則
- 移轉至基於應用程式的政策的最佳做法
- 保護管理存取權的最佳做法
- 應用程式與威脅內容更新的最佳做法
- 解密最佳作法
- DoS 和區域保護最佳做法
- WildFire 部署最佳做法

Expedition

IronSkillet (第 1 天的設定範本)

客戶支援

預防狀態評估 (贈送您的預防能力諮詢評估)

Palo Alto Networks NextWave 技術合作夥伴