paloalto TECHDOCS

網際網路閘道最佳作法安全性政策

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

Palo Alto Networks, Inc.
www.paloaltonetworks.com

© 2023-2023 Palo Alto Networks, Inc. Palo Alto Networks is a registered trademark of Palo Alto Networks. A list of our trademarks can be found at www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

Last Revised

July 24, 2023

Table of Contents

©2024 Palo Alto Networks, Inc.

©2024 Palo Alto Networks, Inc.

最佳做法網際網路閘道安全性原則

攻擊者進入網路的其中一種最廉價最簡單的方式是透過存取網際網路的使用者。成功入侵端點後，攻擊者可以進入網路並橫向移動到最終目標：竊取原始碼、外洩客戶資料，還是拿下基礎架構。為保護網路免遭網路攻擊並改善整個安全狀態，需實作最佳做法網際網路閘道安全性政策。使用最佳做法政策，您可以透過對所有流量、所有連接埠、所有時段進行控制，安全地啟用應用程式、使用者和內容。

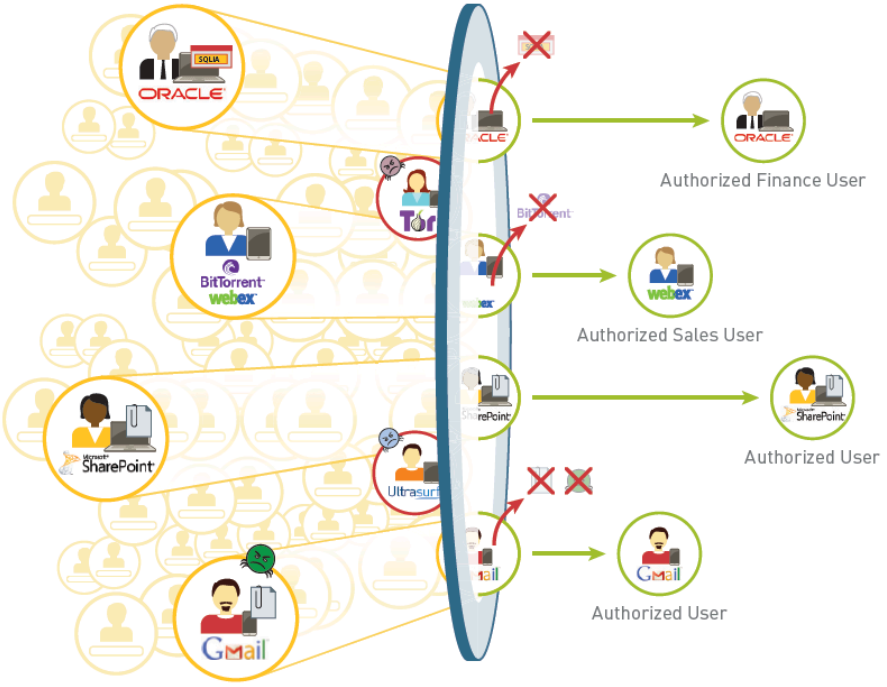
請參閱 Palo Alto Networks 的最佳做法書籍系列，以了解有關解密、DoS 和區域保護（包括封包緩衝區保護）等主題的最佳做法建議。

最佳做法網際網路閘道安全性原則是什麼？

最佳做法網際網路閘道安全性政策具有兩個主要的安全性目標：

- 最大限度降低成功入侵的機會—與傳統基於連接埠之為了網路安全利益封鎖一切或者為了企業利益啟用一切的安全性政策不同，最佳做法安全性政策則是利用 App-ID、User-ID、Content-ID 和 Device-ID（適用於 IoT 安全性，但這不是本書要討論的內容）來確保在所有連接埠、所有使用者、所有時段範圍內安全啟用應用程式，同時掃瞄所有流量是否存在已知和未知威脅。
- 識別攻擊者的存在—最佳做法網際網路閘道安全性原則提供內部機制，協助您識別規則庫中的弱點並偵測網路上的危險行為及潛在威脅。

為了達到這些目標，最佳做法網際網路閘道安全性政策使用基於應用程式的規則，允許使用者存取特定應用程式、掃瞄所有流量以偵測並封鎖所有已知威脅，並向 WildFire 傳送未知檔案，以識別新威脅並產生封鎖它們的特徵碼。



最佳做法政策會依據以下方法來制定，而這些方法可確實地在攻擊生命週期的多個階段進行偵測和預防。

最佳做法方法	這為何如此重要？
檢查所有流量的可見度	由於您無法防禦看不見的威脅，因此請務必始終對所有使用者及應用程式具有完整可見度： • 部署 GlobalProtect，將新一代安全性平台延伸至各地的使用者和裝置。

©2024 Palo Alto Networks, Inc.

最佳做法方法	這為何如此重要？
	• 啟用解密，因此防火牆可以檢查加密流量（每年會加密更高百分比的企業網路流量，而且有更多的惡意軟體活動會使用加密）。 • 啟用 User-ID 以將應用程式流量和相關威脅對應到使用者/裝置，並啟用政策來追蹤造訪任何地方的使用者。 • 如果公司政策允許網路上有使用者的裝置（未安裝 GlobalProtect 或其他安全性管理應用程式的 BYOD 或企業裝置），SaaS 安全性 API 上的未受管理裝置存取控制可讓使用者從個人裝置、任何位置存取您的雲端 SaaS 應用程式，而不需要不當地放入您有風險的資料或組織。流量會透過防火牆進行重新導向，以強制執行政策和防範威脅。 由於有原生 App-ID、Content-ID 和 User-ID 技術，有了完整檢視能力的防火牆可以檢查所有流量（包括應用程式、威脅和內容），並將其繫結至使用者，而不受位置或裝置類型、連接埠、加密或規避性技術所影響。 完整查看網路上的應用程式、內容和使用者，是邁向明智政策控制的第一步。
減少攻擊面	在對網路上應用程式、內容和使用者的情況有所了解後，請建立基於應用程式的安全性政策規則，以允許業務關鍵應用程式並封鎖沒有合法商業使用案例的高風險應用程式。 為了進一步減少攻擊面，可以向所有規則附加檔案封鎖及 URL 篩選設定檔，從而讓應用程式流量來防止使用者造訪容易遭受威脅的網站並防止他們上傳或下載危險的檔案類型（不管是有意還是無意）。為了防止攻擊者成功執行網路釣魚攻擊，請設定認證網路釣魚防禦。
預防已知威脅	將安全性設定檔附加到所有允許規則，以便防火牆可以偵測並封鎖網路和應用程式層的弱點入侵、緩衝區溢位、DoS 攻擊、連接埠掃描和已知的惡意軟體變體（包括隱藏在壓縮檔案或壓縮 HTTP/HTTPS 流量內的惡意軟體變體）。若要啟用加密流量的檢查，請啟用解密。 除了基於應用程式的安全性原則規則以外，還可建立規則來封鎖已知惡意 IP 位址（根據 Palo Alto Networks 的威脅情報和可信協力廠商摘要）。
偵測未知威脅	將所有未知檔案轉送至 WildFire 以進行分析。WildFire 可直接觀察及執行雲端或 WildFire 設備上虛擬化環境中的未知檔案，來識別隱藏於檔案內的未知或針對性惡意程式（亦稱進階持續性威脅或

©2024 Palo Alto Networks, Inc.

最佳做法方法	這為何如此重要？
	APT）。如果 WildFire 偵測到惡意軟體，便會自動開發特徵碼，並可以即時或按照您選擇的時間間隔將特徵碼傳遞給您。

©2024 Palo Alto Networks, Inc.

我為什麼需要最佳做法網際網路閘道安全性原則？

最佳做法安全性政策可讓您隨時分類所有連接埠上的所有流量（包括加密流量），以安全地啟用應用程式。請確定每個應用程式的商業使用案例，以建立可允許和保護相關應用程式存取權的安全性政策規則。最佳做法安全性政策會利用 Palo Alto Networks 企業安全平台上的新世代技術（App-ID、Content-ID、User-ID 和 Device-ID（適用於 IoT 安全性），但這不是本書要討論的內容），並且會：

- 識別所有連接埠、通訊協定、規避性技術或加密相關的應用程式。
- 識別並控制所有 IP 位址、位置或裝置的使用者。
- 提供保護，抵禦已知及未知的應用程式所攜帶的威脅。
- 對應用程式存取及功能提供精緻化的可見度和政策控制。
- 如果您有 IoT 部署，請遵循 IoT 安全性最佳做法。

最佳做法安全性政策會使用分層方法來確保您可以安全地啟用已認可的應用程式，同時封鎖沒有合法使用案例的應用程式。在從基於連接埠的強制執行移至基於應用程式的強制執行時，為了降低中斷應用程式的風險，最佳做法規則庫會納入臨時的安全性政策規則，以識別規則庫漏洞、偵測危險活動和潛在威脅、確保應用程式不會在轉換期間中斷，並讓您可以監控應用程式使用情況，以便制定適當的規則。舊版的基於連接埠政策所允許的某些應用程式，可能會是您不想允許的應用程式，或是您想要限制只有一組更精細的使用者能夠使用的應用程式。

最佳做法安全性政策可讓您更輕鬆地進行管理和維護，因為每個規則都符合特定的企業目標，並且會允許特定使用者群組或使用者存取某個應用程式或應用程式群組。每個規則的應用程式和使用者比對規則可讓您更輕鬆地了解規則會強制執行的流量。最佳做法安全性政策規則庫還會利用標籤和物件，讓規則庫能夠更輕鬆地進行掃描以及更輕鬆地與不斷變化的環境保持同步。

©2024 Palo Alto Networks, Inc.

我如何部署最佳做法網際網路閘道安全性原則？

目標是構建基於應用程式的最佳做法安全性政策，該政策要與您的企業目標和可接受的使用政策保持一致、簡化管理、減少出錯的可能性，並對網路存取套用零信任原則。

與任何技術一樣，通常會有漸進式方法可供您完成實作。請仔細規劃部署階段，使轉換過程盡可能順利，盡量減少對一般使用者的影響。通常，實施最佳做法網際網路閘道安全性政策的工作流程為：

- 評估您的業務並識別您需要保護的項目—在部署安全性架構時，第一步是評估您的業務。識別您最有價值的資產以及這些資產面臨的最大威脅。例如，如果您是一間科技公司，您的智慧財產權是最重要的資產。在此情況下，您的其中一個最大威脅是原始碼遭竊。
- 使用介面和區域將網路分段—只有在安全性政策規則允許時，流量才能在區域之間流動。對於已獲得網路存取權的攻擊者，有一個強大的防禦措施可防止其在網路中橫向移動，那就是定義精細區域，並在每個區域中只允許需要存取應用程式或資源的特定使用者群組獲得存取權。將網路分割成精細區域可防止攻擊者在網路內建立通訊通道（透過惡意軟體或入侵合法應用程式），從而降低攻擊成功的可能性。
- 識別應用程式允許清單—在建立網際網路閘道最佳做法安全性政策之前，請先建立要在網路上允許的應用程式詳細目錄。單獨列出您管理的應用程式、正式認可的業務應用程式，以及容許員工使用的應用程式。在識別出要允許的應用程式後，如果要從基於連接埠的規則庫進行移轉，請將應用程式對應到基於連接埠的規則。如果基於連接埠的規則沒有與其對應的應用程式，則可能不需要該規則。
- 建立可存取所允許應用程式的使用者群組—在識別出打算允許的應用程式後，請識別需要存取每個應用程式的使用者群組。對於想要獲得您網路存取權的攻擊者來說，入侵一般使用者的系統是成本最低且最簡單的其中一種方法。若要顯著減少攻擊面，請只允許有合法業務需求的使用者群組獲得應用程式的存取權。
- 解密流量以進行全面檢視和威脅檢查—您無法保護網路免受看不見的威脅，並進行檢查。加密流量是攻擊者常用來傳遞威脅的方式。例如，攻擊者可能使用 Gmail（使用 TLS 加密）等網路應用將入侵程式或惡意軟體電郵至公司網路上存取應用的員工。或者，攻擊者可能入侵使用 TLS 加密的網站，來默默將入侵程式或惡意軟體下載給網站訪客。
- 建立網際網路閘道的最佳做法安全性設定檔—合法的應用程式會傳遞命令和控制流量、CVE、惡意內容的偷渡式下載、網路釣魚攻擊以及 APT。為防禦已知和未知威脅，請將嚴格的安全性設定檔附加到所有會允許流量的安全性政策規則。
- 定義初始網際網路閘道安全性政策—透過您建立的應用程式與使用者群組詳細目錄，定義可允許使用者或使用者群組存取應用程式的初始政策。初始政策規則庫還包含用於封鎖已知惡意 IP 位址的規則，以及可防止您可能不了解的應用程式發生中斷和識別現有設計中政策漏洞及安全性漏洞的臨時規則。
- 監控與微調政策規則庫—在制定臨時規則後，請監控與政策相符的流量，以便您可微調政策。由於臨時規則旨在發現網路上非預期的流量，例如非預設連接埠上執行的流量或來自不明使用者的流量，因此您必須評估與這些規則相符的流量並相應地調整應用程式允許規則。

©2024 Palo Alto Networks, Inc.

- 移除臨時規則—在數月監視期後，您應看到越來越少的流量符合臨時規則。在達到流量不再符合臨時規則的程度時，請移除臨時規則以完成最佳做法網際網路閘道安全性政策。
- 維護規則庫—鑑於應用程式的動態性質，您必須持續監控應用程式允許清單、調整規則以適應新的應用程式，以及判斷新的或經過修改的 App-ID 會如何影響您的政策。由於最佳做法規則庫中的規則與企業目標一致並且利用政策物件來簡化管理，因此新增對新的應用程式或者新的或經過修改的 App-ID 的支援往往就像向應用程式群組新增應用程式或從其移除應用程式或者修改應用程式篩選器那樣簡單。

©2024 Palo Alto Networks, Inc.

識別應用程式允許清單

應用程式允許清單包含您為業務、基礎架構和使用者工作目的所佈建和管理的認可應用程式，以及您選擇允許供個人使用的容許應用程式。在建立網際網路閘道安全性政策之前，請先建立您要允許的應用程式詳細目錄。

- 將應用程式與企業目標對應以獲得簡化的規則庫
- 使用臨時規則來調整允許清單
- 應用程式允許清單範例

將應用程式與企業目標對應以獲得簡化的規則庫

在您清查網路上的應用程式時，需考慮企業目標及可接受的使用原則並確定與每個原則對應的應用程式。這可讓您建立以目標為導向的規則庫。例如，企業目標可能是允許銷售與支援組存取客戶資料庫。建立與每個目標對應的允許規則，並將與目標一致的所有應用程式分組到單一規則中。此方法可讓您建立個別規則較少，且每個規則都有明確用途的規則庫。

由於您建立的個別規則與企業目標一致，因此可以使用應用程式物件對允許的應用程式分組，進一步簡化規則庫的管理：

- 為每一組認可的應用程式建立應用程式群組—建立只明確包含已認可應用程式集的應用程式群組。應用程式群組可簡化政策的管理，因為其可讓您不用修改個別的安全性政策規則就新增和移除已認可的應用程式。一般來說，如果對應至相同目標的應用程式有相同的存取需求（例如，它們全都有指向網際網路的目的地位址，它們全都會向任何已知使用者允許存取權，以及您希望只在其預設連接埠上啟用它們），您就會將它們新增到相同的應用程式群組。

  標記所有認可的應用程式，方法是採用預先定義的已認可標籤。*Panorama* 和防火牆將沒有「認可的」標籤的應用程式視為未認可的應用程式。
- 建立應用程式篩選器以允許一般應用程式的每個類型—除了您正式認可的應用程式外，您還需要決定要允許使用者存取其他哪些應用程式。應用程式篩選器可讓您根據標籤、類別、子類別、技術、風險係數與特性，安全地啟用某些類別的應用程式。根據業務用途與個人用途將不同類型的應用程式分開。為每類應用程式建立單獨的篩選器，以便更輕鬆地了解每種政策規則。

使用臨時規則來調整允許清單

基於應用程式的安全性政策的最終目標，是明確允許您要允許的應用程式流量，並隱含拒絕您不想要的流量。但是，初始規則庫需要一些可確保您會全面了解網路上所有應用程式的臨時規則，以便您可以正確調整政策。初始規則庫包括以下類型的規則：

- 您出於業務目的正式認可並部署的應用程式的允許規則。
- 用於按照合理的使用政策安全地為您要允許的容許應用程式啟用存取權的允許規則。
- 會封鎖沒有合法使用案例的應用程式的封鎖規則。這些規則可防止惡意流量進入您的網路，臨時規則則會發現政策規則庫沒有考慮到的應用程式。

©2024 Palo Alto Networks, Inc.

- 臨時允許規則讓您透視網路上執行的所有應用程式，以便您可以調整規則庫。

臨時規則：

- 可讓您了解您不知道其位於網路上的應用程式。
- 防止您不知道的合法應用程式遭到封鎖。
- 識別未知使用者、未知應用程式以及在非標準連接埠上執行的應用程式（攻擊者通常會在非標準連接埠上使用標準應用程式作為惡意活動的規避技術）。

識別在非標準連接埠上執行的合法應用程式（例如，內部開發的應用程式），以便您可以修改應用程式使用的連接埠，或建立自訂應用程式以在政策中使用。

如果您有為了定義一組連接埠的自訂工作階段逾時而建立的應用程式取代政策規則，請透過設定基於服務的工作階段逾時，將應用程式取代政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時。然後，將每個規則移轉為基於應用程式的規則。應用程式取代政策是基於連接埠的，並且應用程式無法看見流量，因此您無法知道或控制哪些應用程式使用連接埠。基於服務的工作階段逾時既可實現自訂逾時，同時又能維持應用程式的可見度。

應用程式允許清單範例

您不必在初始詳細目錄中擷取您網路上可能正在使用的每個應用程式。相反地，請將重點放在您想要允許的應用程式上。臨時規則會擷取您網路上可能存在的其他應用程式，因此您不會在轉換為基於應用程式的政策期間，忙著應付有關應用程式損壞的抱怨。下表顯示企業閘道部署的範例應用程式允許清單。

應用程式類型	保護的最佳做法
SaaS 應用程式	SaaS 應用程式服務供應商擁有和管理軟體與基礎架構，但您保有對資料的完整控制，包括可以建立、存取、分享和傳輸的人。若要控制 SaaS 應用程式，請使用 SaaS 安全性（需要訂閱）。如果您使用 SaaS 安全性，請使用 SaaS 政策建議來控制防火牆上的 SaaS 應用程式。 如果您沒有 SaaS 安全性訂閱，請產生 SaaS 應用程式使用情況報告，以檢查目前使用的 SaaS 應用程式是否有不適當的裝載特點，例如以前有過資料外洩情形或缺少正確的認證。根據企業需求和您願意承受的風險量，請使用資訊： • 立刻封鎖有不適當的裝載特點的現有應用程式。 • 建議細化的政策，封鎖有不適當的裝載特點的應用程式以避免將來違規。 • 找出有不適當的裝載特點的前幾個應用程式的網路流量趨勢，因此您可以相應的調整政策。 許多 SaaS 應用程式都有企業版本和消費者（個人）版本，但不受限制的使用會增加敏感資料離開您網路的風險。HTTP 標頭插入可讓您控制您

©2024 Palo Alto Networks, Inc.

應用程式類型	保護的最佳做法
	網路上允許的 SaaS 應用程式版本。例如，您可以允許企業版本的 Box 或 Office 365，但封鎖消費者版本。HTTP 標頭插入可藉由僅允許您想要認可或容許使用者個人使用的每個 SaaS 應用程式的版本，以減少攻擊面。

認可的應用程式	以下為 IT 部門專為組織內企業用途而管理或為網路及應用程式提供基礎架構的應用程式。例如，在網際網路閘道應用程式部署中，這些應用程式歸屬於以下類別：
	• 基礎架構應用程式—必須允許才能啟用網路和安全性的應用程式（例如 ping、NTP、SMTP 和 DNS）。
	• **IT** 認可的應用程式—為使用者佈建和管理的應用程式。這些應用程式歸屬於兩類：
	  • **IT** 認可的內部部署應用程式—出於商業用途在資料中心安裝及裝載的應用程式。對於 IT 認可的內部部署的應用程式，應用程式基礎架構與資料 位於企業所有的裝置上。範例包括：Microsoft Exchange 與主動同步以及 Kerberos 和 LDAP 等驗證工具。
	  • **IT** 認可的 **SaaS** 應用程式—您的 IT 部門為了業務目的而認可的 SaaS 應用程式，例如 Salesforce、Box 和 GitHub。
	• 管理應用程式—僅特定群組的管理使用者可以存取以便管理應用程式及支援使用者的應用程式（例如遠端桌面應用程式）。
	標記所有認可的應用程式，方法是採用預先定義的認可的標籤。Panorama 和防火牆將沒有「認可的」標籤的應用程式視為未認可的應用程式。

容許的應用程式類型	除了您正式認可的應用程式外，您還需要允許使用者安全地存取其他類型的容許應用程式： • 通用型商務應用程式—例如，允許存取容許應用程式的軟體更新及網頁服務，例如 WebEx、Adobe 線上服務與 Evernote。 • 個人應用程式—例如，您可以允許使用者瀏覽網頁或安全地使用網頁型郵件、即時通訊或社群網路應用程式，包括有些 SaaS 應用程式的消費者版本。 從廣泛的應用程式篩選器開始，以了解您的網路上有哪些應用程式。決定您願意承擔多大風險，並削減應用程式允許清單。例如，您可能有多個使用中的傳訊應用程式，每個都會有遺失資料、傳輸感染惡意軟體的檔案等固有風險。 最好的做法是只認可一個傳訊應用程式，然後慢慢地從允許政策轉換為警示政策，並在充份警告使用者後，轉換為封鎖政策，以逐步淘汰其他

©2024 Palo Alto Networks, Inc.

應用程式類型	保護的最佳做法
	傳訊應用程式。您還可選擇讓一小組使用者依與合作夥伴共同執行工作職能之需，繼續使用其他傳訊應用程式。
特定於環境的自訂應用程式	為專有應用程式或在非標準連接埠上執行的應用程式建立自訂應用程式。這可讓您允許該應用程式作為認可的應用程式（並套用預先定義的「已認可」標籤），並將其鎖定至其預設連接埠。否則，您必須開啟其他連接埠（針對非標準連接埠上執行的應用程式），或允許未知流量（針對專有應用程式），此二者在最佳做法安全性政策中皆不推薦。 如果您有單獨用於定義一組連接埠的自訂工作階段逾時而建立的現有應用程式取代政策，請透過設定基於服務的工作階段逾時，將現有的「應用程式取代」政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時。然後，將每個規則移轉為基於應用程式的規則。應用程式取代政策是基於連接埠的，並且應用程式無法看見流量，因此您無法知道或控制哪些應用程式使用連接埠。基於服務的工作階段逾時既可實現自訂逾時，同時又能維持應用程式的可見度。

©2024 Palo Alto Networks, Inc.

為存取允許的應用程式建立使用者群組

安全地啟用應用程式意味著您要定義想要允許的應用程式清單，以及只為具有合法業務需求的使用者啟用存取權。例如，某些應用程式（例如會提供 Workday 或 Service Now 等人力資源服務存取權的 SaaS 應用程式）必須提供給網路上任何已知的使用者。但是，對於更敏感的應用程式，則應該透過只為出於業務目的需要使用應用程式的使用者啟用存取權來減少攻擊面。例如，IT 支援人員可能會合法地需要存取遠端桌面應用程式，但大多數使用者不需要。限制使用者對應用程式的存取權，可防止出現能讓攻擊者用來獲得網路中系統存取權和控制權的潛在安全漏洞。

若要啟用以使用者為基礎的應用程式存取權限：

- 在使用者從其啟動流量的區域中啟用 User-ID。
- 對於您定義的每個應用程式允許規則，請識別對應用程式有合法業務需求的使用者群組。相較於將基於連接埠的規則對應到使用者，將應用程式允許規則對應到企業目標（包括考慮哪些使用者對特定類型的應用程式有業務需求）會導致要管理的規則數量更少。
- 如果您在 Active Directory (AD) 伺服器上沒有現有的使用者群組，也可以建立自訂 LDAP 群組以符合需要存取特定應用程式的使用者群組。
- 一般使用者只要按一下網路釣魚連結並輸入認證，就能讓攻擊者取得網路的存取權。為了防禦這種簡單而有效的攻擊手段，請在您允許使用者存取網際網路的所有安全性政策規則上，設定認證網路釣魚防禦。以基於 Windows 的使用者 ID 代理程式設定認證偵測，確保您能在使用者向未經授權類別的網站提交公司認證時及時偵測到。

©2024 Palo Alto Networks, Inc.

解密完全透視與威脅檢查的流量

請將敏感類別（包括金融服務、健康和醫療、政府等 URL 類別）以及出於業務、法律或監管原因而不解密的其他流量以外的所有流量解密。使用 URL 類別、自訂 URL 類別和外部動態清單 (EDL) 即可指定不解密的流量。

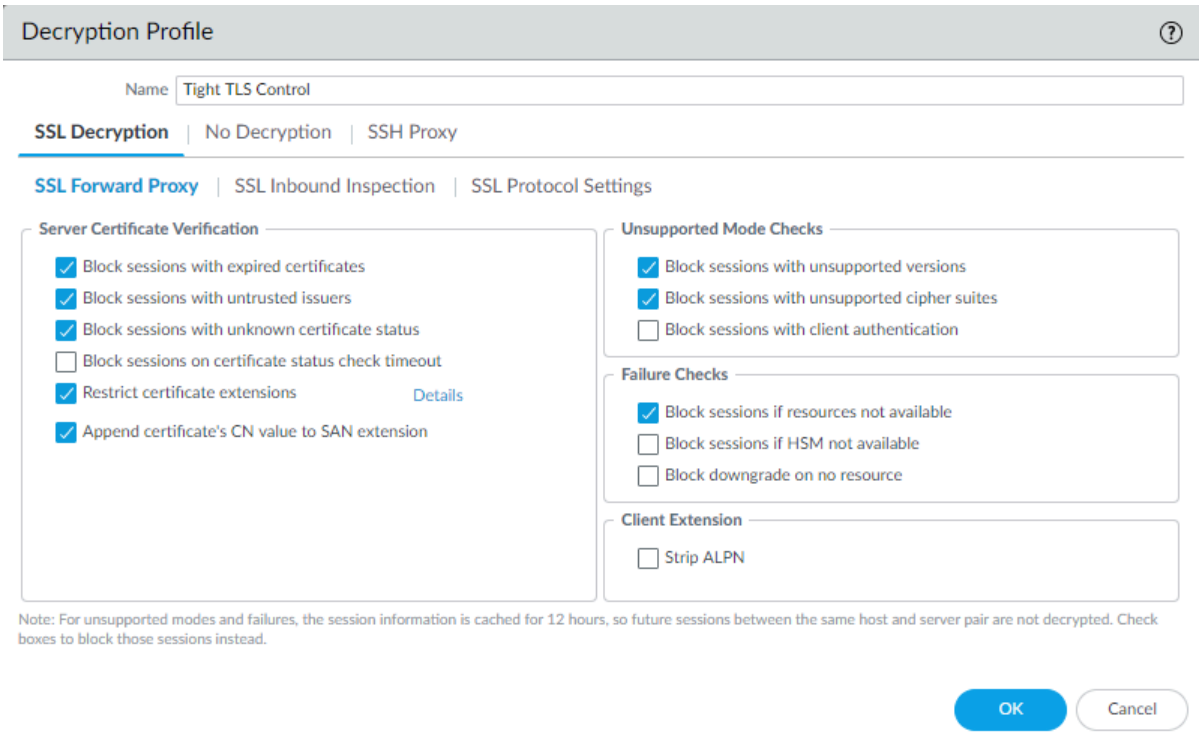
請只在需要時使用解密例外狀況。務必要精確，以確實地根據需要將例外狀況限制到特定應用程式或使用者：

- 如果解密中斷一個重要的應用程式，則為與應用程式關聯的憑證中的特定 IP 位址、網域或通用名稱建立一個例外狀況。
- 如果出於法規、業務或法律原因而需要排除特定使用者，請建立只適用於該使用者的例外狀況。

若要確保解密期間所出示的憑證有效，請執行 CRL/OCSP 檢查。

將嚴格的解密設定檔新增至解密政策規則。在設定 SSL 正向 Proxy 前，建立最佳做法解密設定檔（**Objects**（物件） > **Decryption Profile**（解密設定檔））以附加至解密政策規則，以及遵循一般解密最佳做法：

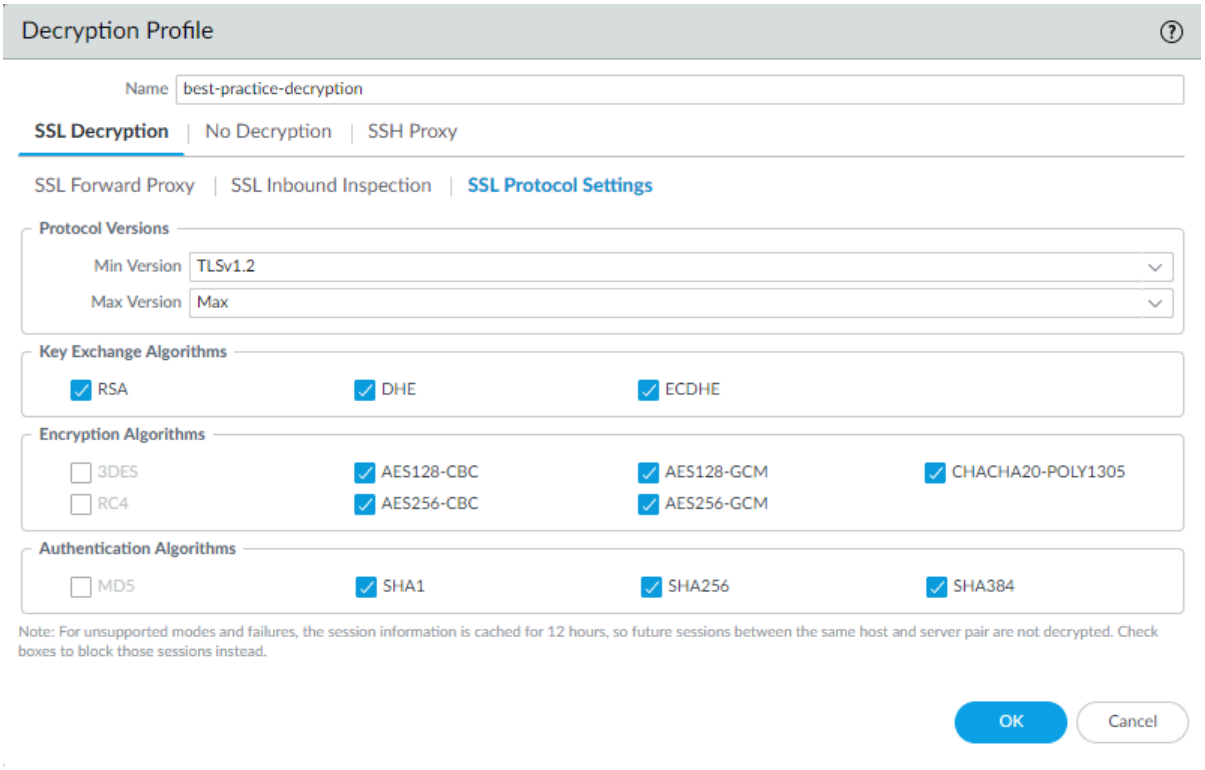
STEP 1 | 完成 **SSL Decryption**（**SSL** 解密） > **SSL Forward Proxy**（**SSL** 正向 **Proxy**）設定，以封鎖 TLS 交涉期間的例外以及無法解密的工作階段：



Block sessions if resources not available（資源不可用時封鎖工作階段）可防止在防火牆沒有資源可執行解密時允許可能有危險的連線，但封鎖因這個理由而無法解密的流量可能會影響使用者體驗。

©2024 Palo Alto Networks, Inc.

STEP 2 | 設定 **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 通訊協定設定），以封鎖有弱點的 SSL/TLS 版本（TLSv1.0、TLSv1.1 和 SSLv3）並避免脆弱的演算法（MD5、RC4 和 3DES）：



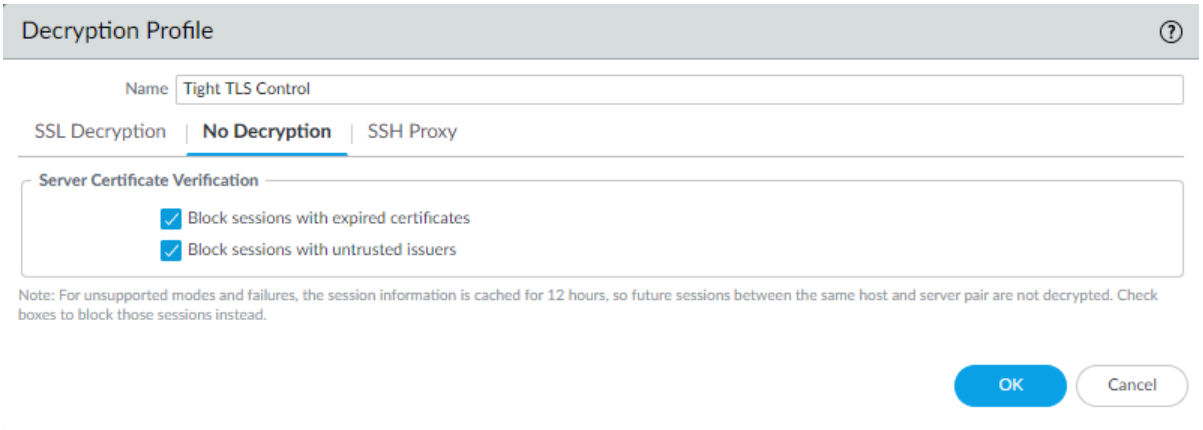
可以時，請使用 TLSv1.3（最安全的通訊協定）。許多行動應用程式會使用憑證釘選，但這會防止解密並導致防火牆丟棄流量。對於該流量，請使用 TLSv1.2。

檢閱您出於業務目的需要存取的網站。如果其中有任何一個使用 TLSv1.1，請為這些網站建立單獨的解密政策和設定檔，如此一來，只有您出於業務目的而必須存取的網站才能使用較不安全的通訊協定。

除非必要，否則請勿允許 SHA1 驗證演算法。請為您出於業務目的而必須存取，但其使用 SHA1 的網站，建立單獨的解密政策規則和設定檔。

©2024 Palo Alto Networks, Inc.

STEP 3 | 對於不解密的流量，完成 **No Decryption**（不解密）設定，對具有已過期憑證或不受信任發行者的網站封鎖加密的工作階段。



只針對 *TLSv1.2* 和更早版本使用不解密設定檔。請不要將不解密設定檔附加至您未解密的 *TLSv1.3* 流量。*TLSv1.3* 會加密未在舊版本加密的憑證資訊，這樣，防火牆就無法根據憑證資訊來封鎖工作階段。

©2024 Palo Alto Networks, Inc.

安全地轉換為最佳做法安全性設定檔

安全性設定檔可讓您檢查網路流量中是否有威脅（例如弱點入侵、惡意軟體、命令和控制 (C2) 通訊和未知威脅），並使用各種類型的威脅特徵碼、機器學習和 AI 來防止它們危害您的網路（部分保護需要訂閱）。

最終目標是達到所有安全性設定檔的最佳做法狀態。不過，若要確定業務關鍵應用程式的可用性，可能無法一開始就實作完整最佳做法安全性設定檔設定。在大部分情況下，您可以安全地封鎖一些特徵碼、檔案類型或通訊協定，同時對其他項目發出警示，直到您取得資訊並確信完成安全轉換至最佳做法安全性設定檔，而不影響可用性。

實作最佳做法安全性設定檔的路徑為：

1. 使用 AIOps 針對您的安全狀態產生隨選最佳做法評估 (BPA) 報告。檢閱您的最佳做法採用情況、識別採用方面的漏洞，並檢閱安全性設定檔設定。
2. 使用下列安全轉換步驟，以達成您安全性設定檔的最佳做法狀態。

問您自己下列問題，協助判斷正確的方式來啟用給定網路區段或安全性政策規則集的安全性設定檔：

1. 我是否已對保護類似應用程式或網路區段的規則啟用安全性設定檔？如果答案為是，您或許可以複製這些設定檔設定，包括您已認為安全而可啟用的封鎖動作。
2. 對我的業務而言，我所保護的網路區段是否重要？如果答案為是，而且您未在類似區段中啟用證明過的設定檔，則您可能會偏好先發出警示，並檢查造成警示的流量，確定設定檔不會封鎖關鍵應用程式後，再於時機成熟時進行封鎖。
3. 我在部署安全性設定檔時發生立即威脅嗎？如果答案為是，則建議您使用封鎖作為初始動作，而非發出警示。
4. 是否有防火牆變更程序允許及時調查和修復誤報？如果答案為是，您或許可以使用封鎖作為初始動作，而非發出警示。

> 大部分的「誤報」都是對您網路中沒有的弱點嘗試的攻擊。攻擊是真實的，但危險的原因不是弱點不存在，因此通常會將攻擊視為誤報。如果攻擊閾值設定太低，則暴力密碼破解攻擊特徵碼也可能會造成誤報。

請同時考慮您的目前安全性狀態與每種類型的安全性設定檔的指導來決定如何一開始部署設定檔，然後移至最佳做法指導。

- 將弱點保護設定檔安全地轉換為最佳做法
- 將反間諜軟體設定檔安全地轉換為最佳做法
- 將防毒設定檔安全地轉換為最佳做法
- 將 WildFire 設定檔安全地轉換為最佳做法
- 將 URL 篩選設定檔安全地轉換為最佳做法
- 將檔案封鎖設定檔安全地轉換為最佳做法

©2024 Palo Alto Networks, Inc.

將弱點保護設定檔安全地轉換為最佳做法

第一次將弱點保護設定檔套用至流量時的封鎖或警示決定，取決於您的目前安全性狀態和您業務的安全性與可用性需求。在您開始轉換為最佳做法弱點保護設定檔時，下列指導可協助判定以封鎖還是警示動作開始。

弱點保護需要進階威脅防護或有效的舊版威脅防護訂閱。

為了識別和防止威脅，防火牆必須能夠了解應用程式流量。在當地法規、業務考量、隱私考量和技術能力允許的情況下，解密盡可能多的流量。如果您未解密流量，防火牆就無法分析加密的標頭和有效負載資訊。

此外，請遵循威脅內容更新最佳做法，以確保您的安全性設定檔特徵碼是最新的。

- 業務關鍵應用程式—通常最好將初始規則 **Action**（動作）設定為 **alert**（警示），以確保應用程式可用性。不過，在部分情況下，您可以一開始就使用 **block**（封鎖）動作。例如，如果您已使用可根據弱點特徵碼進行封鎖的弱點保護設定檔來保護類似應用程式，而且確信設定檔符合您的業務和安全性需求，則可以使用類似設定檔來封鎖弱點以及保護類似應用程式。

  警示可讓您先分析威脅日誌並在必要時建立例外狀況，再開始封鎖流量。在進行封鎖之前先發出警示並進行監控可讓您確信：

  - 當您部署初始設定檔時，初始設定檔不會封鎖業務關鍵應用程式。
  - 您在轉換為封鎖狀態時建立了必要的例外狀況以維持應用程式可用性。

  將您維護初始警示動作的時間長度保持為最小，以減少安全性洩漏的機會。如果您覺得您已識別出所有需要建立的例外狀況並據此設定好設定檔，請盡快轉換為封鎖狀態。
- 關鍵嚴重性和高嚴重性特徵碼—關鍵嚴重性和高嚴重性特徵碼的誤報率一般很低，而且通常表示有人攻擊您網路中沒有的弱點。針對非業務關鍵應用程式（例如網際網路存取），請一開始就封鎖（**reset-both**（重設兩者））關鍵嚴重性和高嚴重性特徵碼。
- 中嚴重性特徵碼—這些特徵碼可能會產生誤報，而且需要初始監控。從對中嚴重性特徵碼發出警示開始，並監控威脅日誌（**Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅））以查看您是否應該封鎖收到警示的應用程式，或是否需要允許它們。
- 請先微調發出警示的設定檔規則再轉換為加以封鎖（特別是對於面向網際網路的流量和資料中心流量）。請在您覺得時機成熟時盡快移至封鎖狀態。
- 將暴力密碼破解類別中的特徵碼設為警示，然後盡快移至封鎖。暴力密碼破解事件是當某個動作短時間發生多次時會觸發的彙總事件。例如，一次的 SSH 登入嘗試是一個資訊事件，但 10 秒內發生 100 次登入嘗試則會觸發暴力密碼破解特徵碼。雖然要花時間調整設定檔，才不會讓正常的網路流量觸發暴力密碼破解特徵碼，但還是請您根據時機成熟度，盡快安全地轉換為封鎖這些特徵碼。

©2024 Palo Alto Networks, Inc.

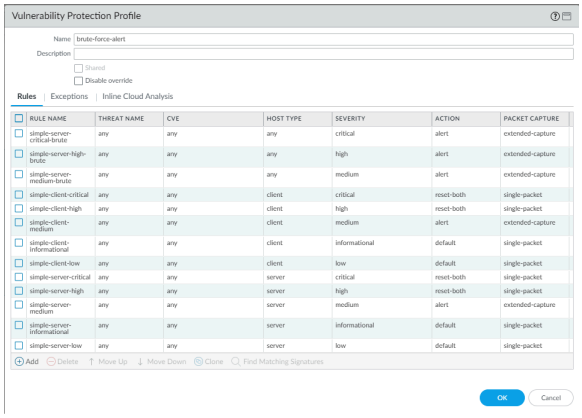


圖 **1:** 暴力密碼破解警示弱點保護設定檔

- 最低嚴重性和資訊嚴重性特徵碼的預設 **Action**（動作）是 **alert**（警示）或 **allow**（允許）。除非您特別需要對所有低和資訊特徵碼發出警示，否則請將 **Action**（動作）設定為 **default**（預設）。
- 如果有可用資源，請針對您發出警示的關鍵嚴重性、高嚴重性和中嚴重性特徵碼啟用延伸 Packet Capture（封包擷取）。針對已封鎖的特徵碼以及低嚴重性和資訊嚴重性特徵碼，請啟用單一封包擷取。啟用封包擷取可讓您在必要時更詳細地調查事件。在您移至最佳做法設定檔時，如果資訊事件建立太多封包擷取活動（流量太大），而且資訊沒有用，則可以轉換為停用資訊事件的封包擷取。

  封包擷取會耗用管理平面資源。請檢查系統資源（例如，***Dashboard***（儀表板） > ***System Resources***（系統資源））來了解實作封包擷取前後的使用量，以確保系統有足夠的資源可取得所有封包擷取。

- 對於 **Inline Cloud Analysis**（內嵌雲端分析），請使用與用於弱點保護規則相同的準則來警示與封鎖業務應用程式。如果您有現有的控制措施，則可以複製它們以封鎖流量。對於新的控制措施，請先警示至少一周再轉換為封鎖。請盡快移至封鎖狀態。

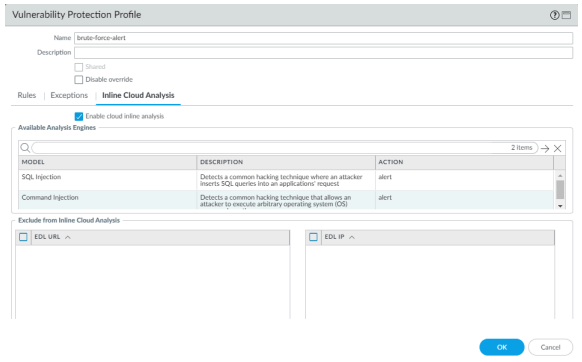


圖 **2:** 內嵌雲端分析警示弱點保護設定檔

當您的初始設定檔就緒時，請監控威脅日誌夠長的時間，確信您了解是否有任何業務關鍵應用程式造成警示或封鎖。視需要在每個設定檔中建立例外（必要時，請開啟支援票證），先修復確認的誤報，再轉換為完整的最佳做法弱點保護設定檔。轉換為最佳做法設定檔的完成速度取決於您的業

©2024 Palo Alto Networks, Inc.

務、應用程式和時機成熟度—請注意，某些應用程式只會每週、每月、每季或每年使用一次以進行稽核、定期事件和會議等。

將反間諜軟體設定檔安全地轉換為最佳做法

在您定義初始反間諜軟體設定檔並開始轉換為最佳做法設定檔時，下列指導可協助判定是以封鎖還是警示動作開始。

反間諜軟體需要進階威脅防護或有效的舊版威脅防護訂閱。

為了識別和防止威脅，防火牆必須能夠了解應用程式流量。在當地法規、業務考量、隱私考量和技術能力允許的情況下，解密盡可能多的流量。如果您未解密流量，防火牆就無法分析加密的標頭和有效負載資訊。

此外，請遵循威脅內容更新最佳做法，以確保您的安全性設定檔特徵碼是最新的。

- 業務關鍵應用程式—將初始動作設定為警示，以確保應用程式可用性。不過，在部分情況下，您可以一開始就使用封鎖動作。例如，如果您已使用可封鎖關鍵、高和（或）中特徵碼的反間諜軟體設定檔來保護應用程式，而且確信設定檔符合您的業務和安全性需求，則可以使用類似設定檔來封鎖間諜軟體以及保護這些應用程式。

  警示動作可讓您在移至封鎖動作之前分析威脅日誌，並在必要時建立例外。在進行封鎖之前先發出警示並進行監控可讓您確信：

  - 當您部署設定檔時，設定檔不會封鎖業務關鍵應用程式。
  - 您在轉換為封鎖狀態時建立了必要的例外狀況以維持應用程式可用性。

  如果您對識別到任何需要建立的例外並據此設定設定檔感到滿意，則請盡快轉換為最佳做法狀態。
- 關鍵嚴重性和高嚴重性特徵碼—誤報率一般很低。若是對業務不關鍵的應用程式，請一開始就封鎖關鍵嚴重性和高嚴重性特徵碼。
- 中嚴重性特徵碼—這些特徵碼可能會產生誤報，而且需要初始監控。先針對內部流量的中嚴重性特徵碼發出警示，並針對面向外部的流量封鎖中嚴重性特徵碼。監控威脅日誌（**Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅））以查看您是否應該封鎖收到警示的應用程式，或是否需要允許它們。
- 低嚴重性和資訊嚴重性特徵碼—這些特徵碼的預設動作大多是警示或允許。除非您特別需要對所有低和資訊特徵碼發出警示，否則請從預設動作開始。
- 如果您有資源，請在轉換期間為所有嚴重性特徵碼啟用單一封包擷取。啟用封包擷取可讓您在必要時更詳細地調查事件。在您移至最佳做法設定檔時，如果低和資訊事件建立太多封包擷取活動（流量太大），而且資訊沒有用，則可以轉換為停用這些嚴重性的封包擷取。

  封包擷取會耗用管理平面資源。請檢查系統資源（例如，***Dashboard***（儀表板） > ***System Resources***（系統資源））來了解實作封包擷取前後的使用量，以確保系統有足夠的資源可取得所有封包擷取。

©2024 Palo Alto Networks, Inc.

- 如果將內部應用程式與外部應用程式區別對待，則可能需要準備一個反間諜軟體設定檔用於面向網際網路的流量，並準備另一個反間諜軟體設定檔用於內部流量。
- **DNS Policies**（**DNS** 政策）：
  - 將 DNS 特徵碼的 **Policy Action**（政策動作） 設定為 **Sinkhole**，以識別嘗試存取可疑網域的潛在遭入侵主機。DNS Sinkhole 可讓您追蹤主機，並使其無法存取這些網域。（立即啟用 DNS Sinkhole 是最佳做法。） 將 **Packet Capture**（封包擷取）設定為 **extended-capture**（延伸擷取）。
  - 對所有 **DNS Security**（**DNS** 安全性）網域類型進行 Sinkhole 處理，並設定 **Packet Capture**（封包擷取），如圖 1 所示（PAN-OS 10.0 和更新版本）。
  - 此外，封鎖所有 DNS 記錄類型，因為加密的 DNS 查詢會使用這些類型。這可以防止用戶端在 DNS 解析過程中 Client Hello 進行加密，從而封鎖金鑰資訊的交換。

僅允許流量流向已認可的 *DNS* 伺服器。使用 DNS 安全性服務以防止有人連線到惡意的 *DNS* 伺服器。

在基於 *PAN-OS* 的系統上，將 *DNS Sinkhole* 位址設定為 *FQDN*（例如，*sinkhole.paloaltonetworks.com*），以便在 *IP* 位址發生變更時，此設定仍會有效。對於 *Prisma Access*，請使用 *Sinkhole IP* 位址。

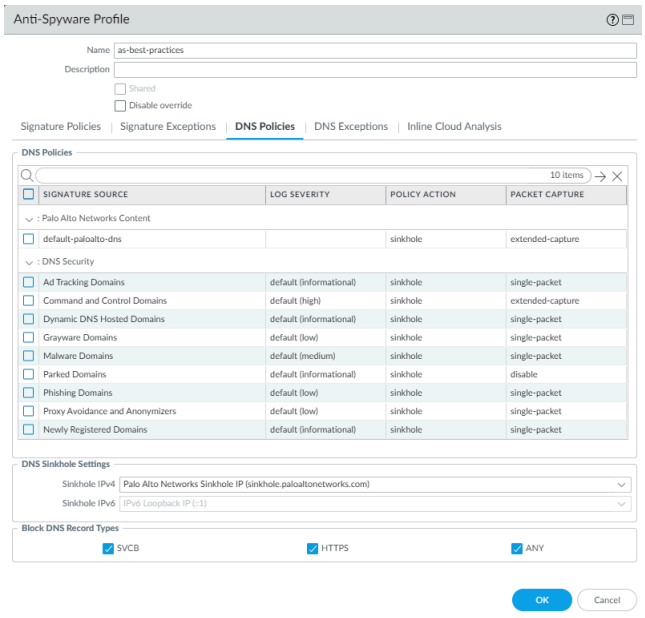


圖 **3:** 反間諜軟體設定檔 **DNS** 政策

- **Inline Cloud Analysis**（內嵌雲端分析）（需要進階威脅防護訂閱和 PAN-OS 10.2 或更新版本）—在所有輸出流量上 **Enable cloud inline analysis**（啟用雲端內嵌分析）。將所有模型的 **Action**（動作）設定為 **reset-both**（重設兩者）。

氣隙環境無法使用進階威脅防護，因為它是雲端服務，需要雲端連線。

©2024 Palo Alto Networks, Inc.

當您的初始設定檔就緒時，請監控威脅日誌夠長的時間，確信您了解是否有任何業務關鍵應用程式造成警示或封鎖。如果您覺得時機成熟了，請盡快轉換為最佳做法反間諜軟體設定檔。視需要在每個設定檔中建立例外（必要時，請開啟支援票證），先修復任何確認的誤報，再實作完整的最佳做法反間諜軟體設定檔。

將防毒設定檔安全地轉換為最佳做法

在您複製預設防毒設定檔並對其進行修改以定義初始設定檔並開始轉換為最佳做法設定檔時，下列指導可協助您判斷是要從封鎖還是警示動作開始。

防毒需要進階威脅防護或有效的舊版威脅防護訂閱。

為了識別和防止威脅，防火牆必須能夠了解應用程式流量。在當地法規、業務考量、隱私考量和技術能力允許的情況下，解密盡可能多的流量。如果您未解密流量，防火牆就無法分析加密的標頭和有效負載資訊。

此外，請遵循威脅內容更新最佳做法，以確保您的安全性設定檔特徵碼是最新的。

- 業務關鍵應用程式—將初始動作設定為警示，以確保應用程式可用性。不過，在部分情況下，您可以一開始就封鎖防毒特徵碼。例如，如果您已使用防毒設定檔來保護類似應用程式，而且確信設定檔符合您的業務和安全性需求，則可以使用類似設定檔來保護類似應用程式，因為您已了解您封鎖的項目。

  警示動作可讓您在移至封鎖動作之前分析威脅日誌（***Monitor***（監控） > ***Logs***（日誌） > ***Threat***（威脅）），並在必要時建立例外。在進行封鎖之前先發出警示並進行監控可讓您確信：

  - 當您部署設定檔時，設定檔不會封鎖業務關鍵應用程式。
  - 您在轉換為封鎖狀態時建立了必要的例外狀況以維持應用程式可用性。

  將您維護初始警示動作的時間長度保持為最小，以減少安全性事件的機會。如果您對識別到任何需要建立的例外並據此設定設定檔感到滿意，則請盡快轉換為最佳做法狀態。
- 關鍵嚴重性和高嚴重性特徵碼—部署最佳做法防毒設定檔來立即封鎖非業務關鍵應用程式的惡意流量是安全的，因為誤報率很低，因此很少發生不必要的封鎖。
- 如果將內部應用程式與外部應用程式區別對待，則可能需要準備一個防毒設定檔用於面向網際網路的流量，並準備另一個防毒設定檔用於內部流量。
- 在裝置上全域啟用即時特徵碼查閱以及在防毒設定檔中啟用即時特徵碼查閱，將檔案保留到防火牆從雲端收到最新的即時防毒特徵碼為止：
  - 全域啟用—**Device**（裝置） > **Setup**（設定） > **Content-ID** > **Content-ID Settings**（**Content-ID** 設定） > **Realtime Signature Lookup**（即時特徵碼查閱），啟用 **Hold for WildFire Real Time Signature Look Up**（保留以進行 **WildFire** 即時特徵碼查閱），並將 **Action on Real**

©2024 Palo Alto Networks, Inc.

Time Siganture Timeout（即時特徵碼逾時的動作）設定為 **Reset Both**（重設兩者）。您必須全域啟用即時特徵碼查閱，才能在防毒設定檔中啟用。

- 在防毒設定檔中啟用—**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒），然後啟用 **Hold for WildFire Real Time Signature Look Up**（保留以進行 **WildFire** 即時特徵碼查閱）。

保留檔案以確保 WildFire 獲得最新的防毒特徵碼可以保護您免受零時差惡意軟體和過時防毒特徵碼的危害，如果您不保留檔案以等待最新特徵碼就轉送檔案，便可能會暴露在這些危險之下。

- 如果流量產生的 WildFire 特徵碼引發重設或丟棄動作，防毒設定檔中的 WildFire Action（WildFire 動作）設定可能會影響流量。

當您的初始設定檔就緒時，請監控威脅日誌夠長的時間，確信您了解是否有任何業務關鍵應用程式造成警示或封鎖。也請監控 WildFire 提交日誌（**Monitor**（監控） > **Logs**（日誌） > **WildFire Submissions**（**WildFire** 提交））夠長的時間，確信您了解是否有任何業務關鍵應用程式因防毒設定檔 WildFire 動作而造成警示或封鎖。視需要在每個設定檔中建立例外（必要時，請開啟支援票證），先修復任何確認的誤報，再實作完整的最佳做法防毒設定檔。轉換為最佳做法設定檔的速度取決於您的業務、應用程式和時機成熟度—請注意，某些應用程式只會每週、每月、每季或每年使用一次以進行稽核、定期事件和會議等。

將 WildFire 設定檔安全地轉換為最佳做法

下列指導可協助定義 WildFire 分析設定檔的初始設定。

Palo Alto Networks 新世代防火牆包括基本的 WildFire 服務，不需要進階 WildFire（或有效的舊版 WildFire）訂閱。基本服務可讓防火牆轉送 PE 檔案以進行分析，並且每 24 到 48 小時更新一次防毒和/或威脅防護來擷取進階 WildFire 特徵碼。進階 WildFire 訂閱（PAN-OS 10.0 或更新版本）或舊版 WildFire 訂閱包含更多功能，例如即時接收更新、支援更多檔案類型，以及 API。

為了識別和防止威脅，防火牆必須能夠了解應用程式流量。在當地法規、業務考量、隱私考量和技術能力允許的情況下，解密盡可能多的流量。如果您未解密流量，防火牆就無法分析加密的標頭和有效負載資訊。

WildFire 特徵碼產生高度精確，而且誤報極少。部署預設 WildFire 分析設定檔（這是最佳做法設定檔）不會影響網路流量。（不過，如果流量產生的 WildFire 特徵碼引發重設或丟棄動作，防毒設定檔中的 WildFire Action（WildFire 動作）設定可能會影響流量。）

當您的初始設定檔就緒時，請監控 WildFire 提交日誌（**Monitor**（監控） > **Logs**（日誌） > **WildFire Submissions**（**WildFire** 提交））夠長的時間，確信您了解是否有任何業務關鍵應用程式因防毒設定檔 WildFire 動作而造成警示或封鎖。視需要在防毒設定檔中建立例外（必要時，請開啟支援票證），以修復任何確認的誤報。

©2024 Palo Alto Networks, Inc.

將 URL 篩選設定檔安全地轉換為最佳做法

在您定義初始 URL 篩選設定檔並開始轉換為最佳做法設定檔時，下列指導可協助判定是以封鎖還是警示動作開始。將 URL 篩選檔案套用至網際網路流量（請不要將 URL 篩選設定檔套用至內部流量）。

您必須啟用解密才能利用 *URL* 篩選，因為您必須解密流量以顯示確切的 *URL*，以便防火牆可以採取適當的動作。請至少解密高風險和中風險流量。

進階 URL 篩選需要訂閱。

- 預先定義的 URL 類別很精確，因此可以根據允許或拒絕存取不同類型的網站的公司政策來安全地實作已設定類別動作的 URL 篩選設定檔。
- 從一開始就封鎖下列已知不良 URL 類別的 **Site Access**（網站存取）和 **User Credential Submission**（使用者認證提交），包括：惡意軟體、命令和控制、侵犯著作權、極端主義、網路釣魚、勒索軟體、動態 DNS、入侵（但為內部 PEN 測試人員設定例外）和代理程式規避與匿名者。
- 針對未知（尚未識別網站 PAN-DB）、寄放（通常用於認證網路釣魚）、灰色軟體（惡意或可疑）和新註冊的網域（通常用於惡意活動）URL 類別，請一開始就發出警示以便監控 URL 篩選日誌（**Monitor**（監控） > **Logs**（日誌） > **URL Filtering**（**URL** 篩選）），以防合法網站在您移至封鎖這些類別的最佳做法之前觸發警示。
- 將所有其他 URL 類別設定為 **alert**（警示）以產生流量日誌。當存取權設定為 **allow**（允許）時，防火牆不會記錄流量。監控 URL 篩選日誌以查看是否要封鎖任何其他類別。

  您可以將高風險、中風險和低風險類別與其他類別結合起來，以確定要允許、封鎖和解密哪些流量。例如，您可以封鎖所有屬於金融服務之高風險網站的存取權。或者，如果您的防火牆需要節約資源，則您可以解密某些類別的所有高風險和中風險流量，而不解密這些類別的低風險流量。

當您的初始設定檔就緒時，請監控 URL 篩選日誌夠長的時間，確信您了解在從發出警示轉換為封鎖再轉換為最佳做法 URL 篩選設定檔時是否將封鎖任何業務關鍵網站。如果您認為未正確分類給定的 URL，請要求 URL 重新分類，以將 URL 放在正確的類別中。轉換為最佳做法設定檔的速度取決於您的業務、應用程式和時機成熟度。

將檔案封鎖設定檔安全地轉換為最佳做法

在您定義初始檔案封鎖設定檔並開始轉換為最佳做法設定檔時，下列指導可協助判定是以封鎖還是警示動作開始。請發出警示（而非允許檔案類型）以產生日誌並了解流量。

©2024 Palo Alto Networks, Inc.

- 不同類型的應用程式通常會有不同的最佳做法檔案封鎖設定檔，輸入、輸出和內部流量的設定檔可能也會不同。例如：
  - 如果內部應用程式取決於最佳做法檔案封鎖設定檔建議封鎖的檔案類型傳輸，則請為這些內部應用程式允許這些檔案類型；.dll 檔案就是很好的範例。請只針對必要的內部應用程式（而非所有應用程式）允許這些檔案傳輸類型。
  - 針對基於網際網路的流量，請採取更嚴格的方式來防止攻擊者遞送惡意檔案以及減少攻擊面。
  - 針對資料中心流量，採取更嚴格的方式（但取決於您將封鎖的檔案傳輸類型的內部應用程式除外）以減少攻擊面並保護最重要的資產。
  - 在制定例外狀況時，請遵循最低權限原則，並只將例外狀況套用到出於業務目的需要存取該檔案類型的應用程式和使用者。
- 業務關鍵應用程式—從針對所有檔案類型的警示動作開始，並盡快移至最佳做法檔案封鎖設定檔。如果您已經設定了封鎖控制措施，請加以複製，並繼續封鎖您已經知道要封鎖的流量。
- 對於非業務關鍵應用程式，請開始轉換為最佳做法檔案封鎖設定檔：
  - 輸入和輸出流量—針對 7z、bat、chm、class、cpl、dll、dlp、hta、jar、ocx、pif、scr、torrent、vbe 和 wsf 檔案，將 **Action**（動作）設定為 **block**（封鎖）。針對所有其他檔案，將 **Action**（動作）設定為 **alert**（警示）。
  - 內部流量—封鎖 7z、bat、chm、class、cpl、dlp、hta、jar、ocx、pif、scr、torrent、vbe 和 wsf 檔案（這與輸入/輸出設定檔相同，但它會對 .dll 檔案發出警示，而不是將其封鎖）。對所有其他檔案發出警示。
  - 請針對不需要出於業務目的使用以下檔案類型的使用者，盡量將這些類型全都封鎖起來：cab、exe、flash、msi、Multi-Level-Encoding、PE、rar、tar、加密 rar 和加密 zip。

如有必要，請為 *IT* 團隊和其他需要對任何這些檔案類型進行合法業務存取的人員建立例外狀況。如果您已封鎖任何其他檔案類型，請繼續封鎖它們。

如果您覺得時機成熟了，請盡快轉換為最佳做法檔案封鎖設定檔。

請微調發出警示的設定檔規則，並在您覺得時機成熟時盡快將其轉換為封鎖狀態（特別是對於面向網際網路的流量和資料中心流量）。監控資料篩選日誌（**Monitor**（監控）> **Logs**（日誌）> **Data Filtering**（資料篩選）），以了解在為特定檔案類型設定封鎖動作之前的檔案類型使用方式。當您了解業務關鍵應用程式和內部自訂應用程式需要哪些檔案類型時，請轉換為最佳做法檔案封鎖設定，並根據需要進行修改以支援您的業務需求。

©2024 Palo Alto Networks, Inc.

建立網際網路閘道的最佳做法安全性設定檔

大多數惡意軟體透過合法應用程式或服務潛入您的網路。若要安全地啟用應用程式，您必須掃描所有允許的流量以尋找其中是否有威脅。請將安全性設定檔附加至允許流量的所有安全性政策規則，以便您可以偵測網路流量中已知和未知的威脅。以下最佳做法建議著重於最嚴格的安全性。將 URL 篩選設定檔附加到允許網際網路繫結流量的所有規則，並將其他設定檔附加到所有允許規則。

超過 90% 的網路流量會進行加密。請啟用解密以了解流量、使用安全性設定檔檢查有效負載，以及防止惡意事件。

請考慮將最佳做法安全性設定檔新增到預設安全性設定檔群組。將安全性設定檔群組命名為預設時，防火牆會自動將其附加到您建立的每個新的安全性政策規則，並確保防火牆會檢查流量中是否存在惡意活動。

此外，請考慮為不同類型的流量建立專用的安全性設定檔群組。安全性設定檔群組可讓您輕鬆地將所有必要設定檔套用到安全性政策規則，並確保不會忘記任何關鍵的設定檔。

- 最佳做法網際網路閘道檔案封鎖設定檔
- 最佳做法網際網路閘道檔案防毒設定檔
- 最佳做法網際網路閘道漏洞保護設定檔
- 最佳做法網際網路閘道反間諜軟體設定檔
- 最佳做法網際網路閘道網址篩選設定檔
- 最佳做法網際網路閘道 WildFire 分析設定檔

最佳做法網際網路閘道檔案封鎖設定檔

使用預先定義的嚴格檔案封鎖設定檔以封鎖通常會包含在惡意軟體攻擊活動中且沒有實際上傳和下載使用案例的檔案類型。封鎖這些檔案類型可以減少攻擊面。預先定義的嚴格設定檔會封鎖批次檔案、DLL、Java 類別檔案、說明檔、Windows 捷徑 (.lnk)、BitTorrent 檔、.rar 檔、.tar 檔、加密的 rar 和加密的 zip 檔、多層編碼檔（檔案編碼或壓縮最多四次）、.hta 檔和 Windows 可攜式執行檔 (PE)，其中包括 .exe、.cpl、.dll、.ocx、.sys、.scr、.drv、.efi、.fon 和 .pif 檔。預先定義的嚴格設定檔還將針對所有其他檔案類型發出警示，以透視其他檔案傳輸，因此您可以判斷是否需要執行政策變更。

在有些情況中，支援關鍵應用程式的需求可能妨礙您封鎖所有嚴格設定檔的檔案類型。遵循將檔案封鎖設定檔安全地轉換為最佳做法建議，以協助判斷您是否需要建立例外套用在不同區域的網路。檢閱資料篩選日誌（***Monitor***（監控） > ***Logs***（日誌） > ***Data Filtering***（資料篩選））以識別檔案類型，並且與企業利益關係人討論有關其應用程式所需的檔案類型。根據這些資訊，複製嚴格的設定檔並視需要修改，以便僅允許您需要支援的關鍵應用程式的其他檔案類型。您還可使用 ***Direction***（方向）設定來限制檔案類型在兩個方向的傳輸，或封鎖檔案在一個方向的傳輸，但不封鎖在另一個方向傳輸。

©2024 Palo Alto Networks, Inc.

	NAME	LOCATION	RULE NAME	APPLICATIONS	FILE TYPES	DIRECTION	ACTION
☐	basic file blocking	Predefined	Block high risk file types	any	7z, bat, chm, class, cpl, dll, exe, hlp, hta, jar, ocx, PE, pif, rar, scr, torrent, vbe, wsf	both	block
			Continue prompt encrypted files	any	encrypted-rar, encrypted-zip	both	continue
			Log all other file types	any	any	both	alert
☑	strict file blocking	Predefined	Block all risky file types	any	7z, bat, cab, chm, class, cpl, dll, exe, flash, hlp, hta, jar, msi, Multi-Level-Encoding, ocx, PE, pif, rar, scr, tar, torrent, vbe, wsf	both	block
			Block encrypted files	any	encrypted-rar, encrypted-zip	both	block
			Log all other file types	any	any	both	alert

您還可以要求一些常用於 Windows 更新等活動惡意用途的通訊協定。嚴格檔案封鎖設定檔會封鎖 .exe、.dll、.pe 和 .cab 檔案。若要設定例外狀況以允許 Windows 更新等特定活動的通訊協定，請執行以下操作：

1. 建立特定的安全性政策規則，以便僅允許必要的使用者和業務應用程式使用您要針對其他流量進行封鎖的通訊協定。
2. 複製嚴格的檔案封鎖設定檔，對其進行修改以允許必要的通訊協定，然後將其附加到規則。
3. 將規則放在其檔案封鎖設定檔會封鎖所有其他流量通訊協定的安全性政策規則之上。

這個方法可讓您以安全的方式使用可能有惡意的檔案類型，從而在封鎖惡意流量的同時啟用業務應用程式。微調設定檔和規則庫以允許任何必要的例外狀況。

我為什麼需要此設定檔？

攻擊者可以通過多種方式傳遞惡意檔案：

- 公司或個人電子郵件中的附件或連結。
- 社交媒體和其他來源中的連結或 IM。
- 入侵程式套件。
- 檔案共用應用程式（如 FTP、Google 雲端硬碟或 Dropbox）。
- USB 磁碟機。
-

附加嚴格檔案封鎖設定檔可防止這些類型的攻擊並減少攻擊面。

如果您選擇不封鎖所有 PE 檔案，則須向 WildFire 傳送所有未知檔案進行分析。將動作設定為 **continue**（繼續）以防止偷渡式下載；偷渡式下載是指一般使用者下載會安裝惡意檔案（例如 Java applet 或可執行檔）的內容而對此不知情。偷渡式下載可能在使用者造訪網站、檢視電子郵件訊息或者按一下有意欺騙他們的快顯視窗時發生。教育使用者：如果系統提示他們繼續不明的檔案傳輸，可能遭受惡意下載。此外，如果必須允許可能帶有威脅的檔案類型，請搭配使用檔案封鎖和 URL 篩選來限制使用者可以傳輸檔案的類別，以減少攻擊面。

最佳做法網際網路閘道檔案防毒設定檔

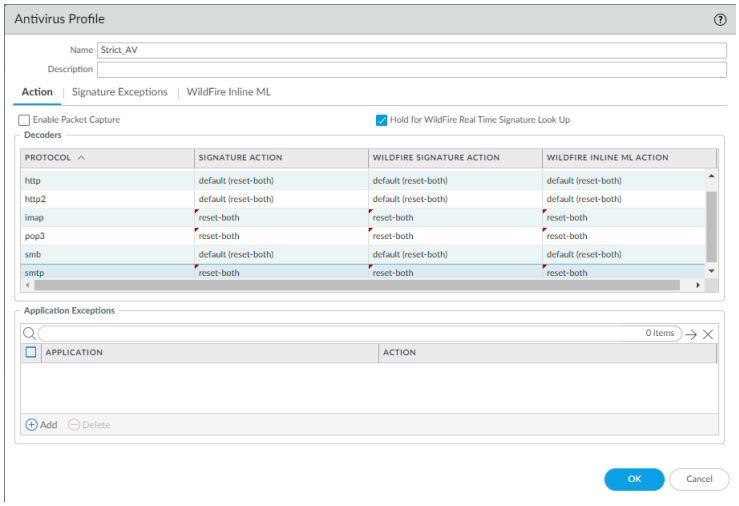
若要確定業務關鍵應用程式可用性，請在您從目前狀態移至最佳做法設定檔時遵循將防毒設定檔安全地轉換為最佳做法建議。目標是轉換為如這裡所說的設定檔，並將其附加到允許流量的所有安全性政策規則。防毒設定檔有通訊協定解碼器，可偵測和防止超過七個通訊協定傳輸的病毒和惡意軟體：FTP、HTTP、HTTP2、IMAP、POP3、SMB 以及 SMTP。

©2024 Palo Alto Networks, Inc.

請為這七種通訊協定都設定 WildFire 特徵碼和 WildFire 內嵌 ML 動作（防毒設定檔還會根據 WildFire 特徵碼強制執行動作），並且如果您尚未這麼做，請啟用即時特徵碼查閱，如將防毒設定檔安全地轉換為最佳做法所示。

設定複製的防毒設定檔，重設用於七個通訊協定解碼器和 WildFire 動作的用戶端和伺服器，然後將設定檔附加到安全性政策允許規則。

如果將內部應用程式與外部應用程式區別對待，則可能需要準備一個防毒設定檔用於面向網際網路的流量，並準備另一個防毒設定檔用於內部流量。



全域啟用即時特徵碼查閱以及在防毒設定檔中啟用即時特徵碼查閱，將檔案保留到防火牆從雲端收到最新的即時防毒特徵碼為止：

- 全域啟用：**Device**（裝置）> **Setup**（設定）> **Content-ID** > **Content-ID Settings**（**Content-ID** 設定）> **Realtime Signature Lookup**（即時特徵碼查閱），啟用 **Hold for WildFire Real Time Signature Look Up**（保留以進行 **WildFire** 即時特徵碼查閱），並將 **Action on Real Time Siganture Timeout**（即時特徵碼逾時的動作）設定為 **Reset Both**（重設兩者）。您必須全域啟用即時特徵碼查閱才能在防毒設定檔中加以啟用。
- 在防毒設定檔中啟用 **Hold for WildFire Real Time Signature Lookup**（保留以進行 **WildFire** 即時特徵碼查閱）。保留檔案以確保 WildFire 獲得最新的防毒特徵碼可以保護您免受零時差惡意軟體和過時防毒特徵碼的危害，如果您不保留檔案以等待最新特徵碼就轉送檔案，便可能會暴露在這些危險之下。

我為什麼需要此設定檔？

透過將防毒設定檔附加至所有安全性規則，您可封鎖進入網路的已知惡意檔案（惡意軟體、勒索軟體 Bot 和病毒）。使用者收到惡意檔案的常見方式包括電子郵件附件、可下載惡意檔案的連結，以及入侵程式套件所促成的無訊息入侵（入侵程式套件會先入侵弱點，然後向一般使用者的裝置自動下載惡意的有效負載）。

©2024 Palo Alto Networks, Inc.

最佳做法網際網路閘道漏洞保護設定檔

將漏洞保護設定檔附加至所有允許的流量，以防禦緩衝區溢位、非法程式碼執行及其他嘗試利用用戶端及伺服器端漏洞的行為。若要確定業務關鍵應用程式可用性，請在您從目前狀態移至最佳做法設定檔時遵循將弱點保護設定檔安全地轉換為最佳做法建議。複製預先定義的嚴格弱點保護設定檔，並對其進行編輯以建立最佳做法設定檔：

- 將三個暴力密碼破解規則中的 **Action**（動作）變更為 **reset-both**（重設兩者），並將 **Packet Capture**（封包擷取）變更為 **single-packet**（單一封包），以從警示暴力密碼破解攻擊事件轉換為封鎖這些事件。
- 將伺服器和用戶端的關鍵嚴重性、高嚴重性和中嚴重性事件合併到一個規則中。將 **Action**（動作）設定為 **reset-both**（重設兩者），並將 **Packet Capture**（封包擷取）設定為 **single-packet**（單一封包）。這可簡化設定檔並起到作用，因為設定檔對這些嚴重性使用相同的動作和相同的封包擷取設定。

  若為控制內部（東西向）流量的設定檔，封鎖中嚴重性事件可能會影響業務應用程式。如果進行封鎖會影響業務應用程式，請在設定檔中為中嚴重性事件建立單獨的規則，並將 ***Action***（動作）設定為 ***alert***（警示）。請只將設定檔套用至內部流量。
- 若要簡化設定檔，請將伺服器和用戶端的低嚴重性事件合併到一個規則中。將 **Action**（動作）設定為 **default**（預設），並將 **Packet Capture**（封包擷取）設定為 **single-packet**（單一封包）。
- 將伺服器和用戶端的資訊事件合併到一個規則中。將 **Action**（動作）設定為 **default**（預設），並將 **Packet Capture**（封包擷取）設定為 **disable**（停用）。

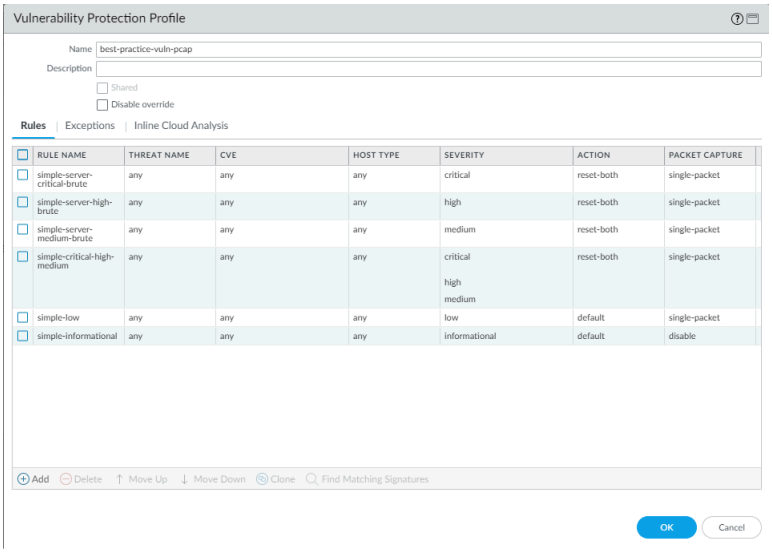
  資訊事件的 PCAP 會產生相對大量的流量，而這些流量相較於潛在威脅的相關擷取來說，通常沒什麼用。
- 請將延伸的 PCAP（而非單一 PCAP）套用到您套用 **alert**（警示）動作的高價值流量中。使用您用來決定要記錄哪些流量的相同邏輯來套用 PCAP，並取得所記錄流量的 PCAP。套用單一 PCAP 至您封鎖的流量。延伸 PCAP 記錄然後傳送到管理面的預設封包數目是五個封包，也就是建議的值。在大多數情況中，擷取五個封包提供充份的資訊以分析威脅。如果有太多 PCAP 流量進入管理平面，則擷取超過五個封包可能導致 PCAP 下降。

如果您想要更精細地微調設定檔，請使用 ***Action***（動作）和 ***Packet Capture***（封包擷取）設定來建立單獨的規則，如前所述。例如，為伺服器建立關鍵嚴重性、高嚴重性和中嚴重性規則，並為用戶端建立另一個類似的規則，或者為用戶端和為伺服器的每個嚴重性分別建立單獨的規則，以實現所需的精細程度和控制程度。

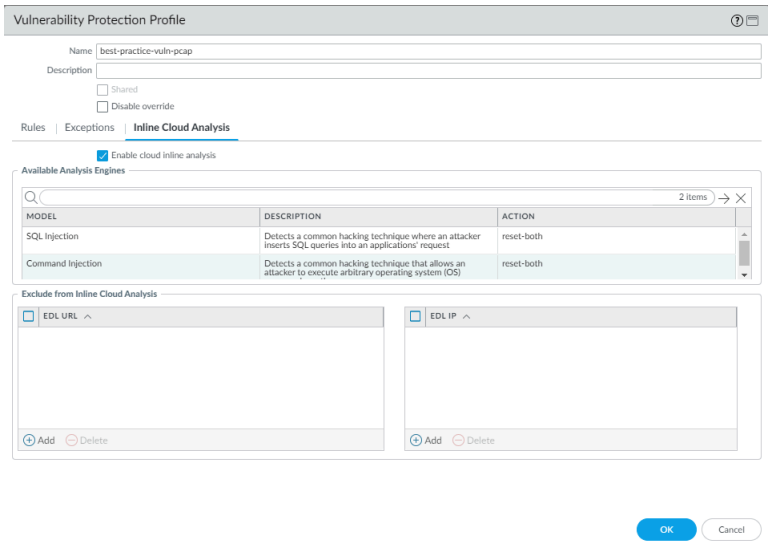
封包擷取會耗用管理平面資源。請檢查系統資源（例如，***Dashboard***（儀表板） > ***System Resources***（系統資源））了解實作封包擷取前後的使用量，以確保系統有足夠的資源可取得所需的封包擷取。

為每個規則啟用封包擷取 (PCAP)，以便能夠追蹤潛在攻擊來源。自動下載內容更新並盡快安裝，使特徵碼集始終保持最新狀態。

©2024 Palo Alto Networks, Inc.



對於 **Inline Cloud Analysis**（內嵌雲端分析），將 **Action**（動作）變更為 **reset-both**（重設兩者）以封鎖常見的入侵技術



我為什麼需要此設定檔？

沒有嚴格的漏洞保護，攻擊者可利用用戶端及伺服器端漏洞來入侵一般使用者。例如，攻擊者可利用弱點來在用戶端系統上安裝惡意程式碼或使用入侵程式套件自動向一般使用者傳遞惡意有效負載。弱點保護設定檔可防止攻擊者使用內部主機上的弱點以在網路內橫向移動。

最佳做法網際網路閘道反間諜軟體設定檔

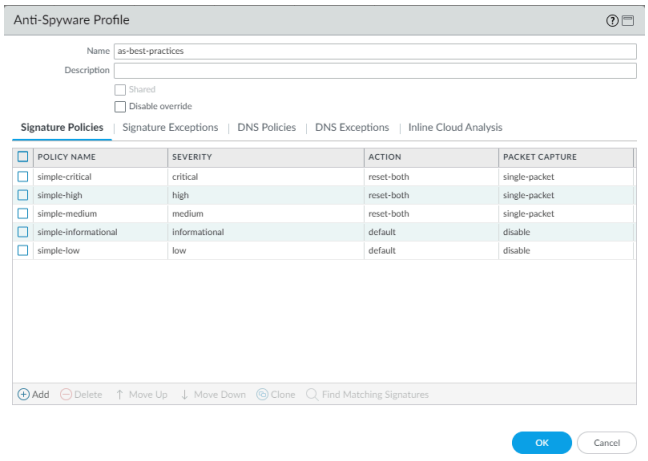
將反間諜軟體設定檔附加到所有允許的流量，以偵測從伺服器或端點上執行的惡意程式碼啟動的命令和控制流量 (C2) 並防止遭入侵的系統從您的網路建立輸出連線。複製預先定義的嚴格反間諜軟體設定檔並進行編輯。若要確保業務關鍵應用程式的可用性，請將反間諜軟體設定檔安全地轉換為最佳做法。編輯設定檔以啟用 DNS Sinkhole 和封包擷取 (PCAP)，協助您追蹤嘗試解析惡意網域的

 ©2024 Palo Alto Networks, Inc.

端點。保留預設 **Action**（動作），以在防火牆偵測到中嚴重性、高嚴重性或關鍵嚴重性威脅時重設連線，並為這些威脅啟用單一 PCAP。

請只允許流量流向認可的 *DNS* 伺服器。使用 DNS 安全性服務以防止有人連線到惡意的 *DNS* 伺服器。

如果將內部應用程式與外部應用程式區別對待，則可能需要準備一個反間諜軟體設定檔用於面向網際網路的流量，並準備另一個反間諜軟體設定檔用於內部流量。



請勿啟用資訊活動的 PCAP，因為其會產生相對大量的流量，相較於潛在威脅的 PCAP 來說，這通常沒什麼用。請將延伸的 PCAP（而非單一 PCAP）套用到您套用 **alert**（警示）動作的高價值流量中。使用您用來決定要記錄哪些流量的相同邏輯來套用 PCAP，並取得所記錄流量的 PCAP。套用單一 PCAP 至您封鎖的流量。延伸 PCAP 記錄然後傳送到管理面的預設封包數目是五個封包，也就是建議的值。在大多數情況中，擷取五個封包提供充份的資訊以分析威脅。如果有太多 PCAP 流量進入管理平面，則擷取超過五個封包可能導致 PCAP 下降。

封包擷取會耗用管理平面資源。請檢查系統資源（例如，***Dashboard***（儀表板） > ***System Resources***（系統資源））來了解實作封包擷取前後的使用量，以確保系統有足夠的資源可取得所需的一切封包擷取。

設定 DNS 政策，保護網路不對惡意網域進行 DNS 查詢。為了獲得最佳安全性，請使用 DNS 安全性服務來保護 DNS 流量。否則，請使用本機可用的可下載 DNS 特徵碼集（與防毒和 WildFire 更新封裝在一起）。

對惡意流量進行 Sinkhole 處理而不是加以封鎖，以透過追蹤主機並防止主機存取可疑網域，識別可能遭入侵而嘗試存取可疑網域的主機。對於構成更大威脅的網域類別，請設定更高的日誌嚴重性等級和/或封包擷取設定，以協助判斷攻擊是否成功、識別攻擊方法並提供更好的整體內容。

設定預設的 Palo Alto Networks DNS 和個別的 DNS 特徵碼來源類別（PAN-OS 10.0 和更新版本）：

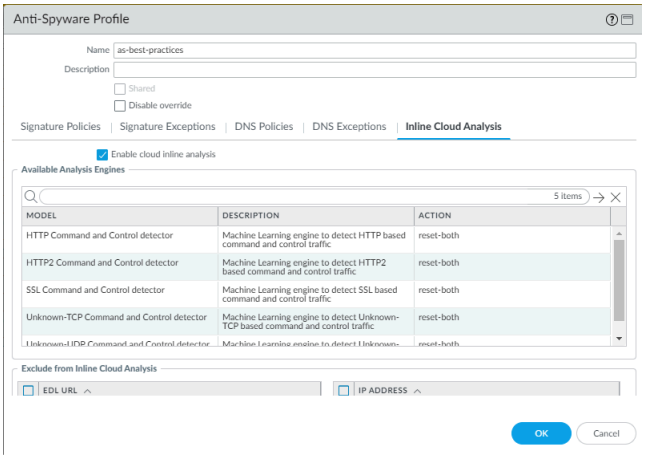
DNS 特徵碼來源	日誌嚴重性	政策動作	封包擷取
Palo Alto Networks 內容			

©2024 Palo Alto Networks, Inc.

DNS 特徵碼來源	日誌嚴重性	政策動作	封包擷取
default-paloalto-dns	預設值	Sinkhole	extended-capture
DNS 安全性			
命令和控制域	高（預設）	Sinkhole	extended-capture
動態 DNS 代管網域	資訊（預設）	Sinkhole	單一封包
灰色軟體網域	低（預設）	Sinkhole	單一封包
惡意軟體網域	中（預設）	Sinkhole	單一封包
寄放網域	資訊（預設）	Sinkhole	disable（預設值）
網路釣魚網域	低（預設）	Sinkhole	單一封包
代理程式規避與匿名者	低（預設）	Sinkhole	單一封包
新註冊的網域	資訊（預設）	Sinkhole	單一封包
AD 追蹤網域	資訊（預設）	Sinkhole	單一封包

對於 **Inline Cloud Analysis**（內嵌雲端分析）（需要進階威脅防護訂閱），請在所有輸出流量上 **Enable cloud inline analysis**（啟用雲端內嵌分析）。將所有模型的 **Action**（動作）設定為 **reset-both**（重設兩者）。

氣隙環境無法使用進階威脅防護，因為其為雲端服務，需要與雲端連線。



©2024 Palo Alto Networks, Inc.

最佳做法網際網路閘道網址篩選設定檔

使用進階 URL 篩選來防止有人存取有高風險屬於惡意活動的 Web 內容。將 URL 篩選設定檔附加至允許存取 Web 式應用程式的所有規則，以防禦 Palo Alto Networks 所發現裝載惡意軟體、潛在惡意軟體、責任風險或攻擊性內容的 URL。

您必須啟用解密才能利用 *URL* 篩選，因為您必須解密流量以顯示確切的 *URL*，以便防火牆可以採取適當的動作。請至少解密高風險和中風險流量。

若要確保業務關鍵應用程式的可用性，請 將 URL 篩選設定檔安全地轉換為最佳做法。最佳做法 URL 篩選設定檔會將所有已知的危險 URL 類別和認證提交設定為封鎖。目標是封鎖以下類別：

- 設定惡意 URL 類別的所有動作，以封鎖網站存取和使用者認證提交。視需要為 PEN 測試、威脅研究和資訊安全設定適當的例外狀況：
  - **command-and-control**（命令和控制）—惡意軟體或遭入侵系統用來與攻擊者的遠端伺服器通訊的 URL 和網域。
  - **grayware**（灰色軟體）—這些網站不符合病毒的定義或未構成直接的安全威脅，但會影響使用者以授與遠端存取權或執行其他未經授權的動作。灰色軟體網站包括詐騙、非法活動、犯罪活動、廣告軟體以及其他不需要和未經請求的應用程式，包括「誤植域名」網域。
  - **malware**（惡意軟體）—已知裝載惡意軟體或用於命令和控制活動的網站。
  - 網路釣魚—已知裝載認證和個人資訊網路釣魚頁面（包括技術支援詐騙和恐嚇軟體）的網站。
  - 勒索軟體—已知會散發勒索軟體的網站。
  - 掃描活動—會探查現有弱點或進行針對性攻擊的網站。

©2024 Palo Alto Networks, Inc.

- 某些 URL 類別有很大的可能是惡意的，但並非絕對。請設定這些 URL 類別的所有動作，以封鎖網站存取和使用者認證提交。視需要為 PEN 測試、威脅研究和資訊安全設定適當的例外狀況：
  - **dynamic-dns**（動態 **DNS**）—具有動態指派的 IP 位址的系統，通常用來傳遞惡意軟體有效負載或命令和控制惡意軟體。

    如果您有動態 *DNS* 網域的業務用途，則請確定 *URL* 篩選設定檔中允許這些 *URL*。
  - **hacking**（入侵）—與非法或可疑地存取或使用設備和軟體相關的網站。包括有助於繞過授權和數位版權系統的網站。

    請為適當的 *PEN* 測試和威脅研究使用者設定這個類別的例外情況。
  - 內容不足—提供測試頁面、未提供任何內容、提供並非用於一般使用者顯示的 API 存取，或要求驗證卻又不顯示任何其他內容的網站和服務。
  - 新註冊的網域—網域產生演算法經常會產生的網域或惡意行為者會為了惡意活動而產生的網域。
  - **not-resolved**（未解析）—如果 PAN-DB 雲端無法連線，且 URL 不在防火牆的 URL 篩選快取中，則防火牆無法解析和識別 URL 類別。

    為了獲得最高的安全性，請啟用 ***Hold client request for category lookup***（保留用戶端要求以進行類別查閱），以便防火牆有更多時間解析 *URL* 類別。這會延長防火牆向雲端查詢類別類型的時間，進而提高安全性，但可能會增加延遲。
  - **parked**（寄放）—經常用於認證網路釣魚或個人資訊竊取的網域。
  - **Proxy-avoidance-and-anonymizers (**代理程式規避與匿名者**)**—URL 和服務通常用於避開內容篩選產品。
  - 未知—Palo Alto Networks (PAN-DB) 尚未識別的網站。

    PAN-DB 即時更新會在首次嘗試存取未知網站後認識未知網站，因此防火牆可以快速識別未知 *URL*，然後根據網站的實際 *URL* 類別進行處理。

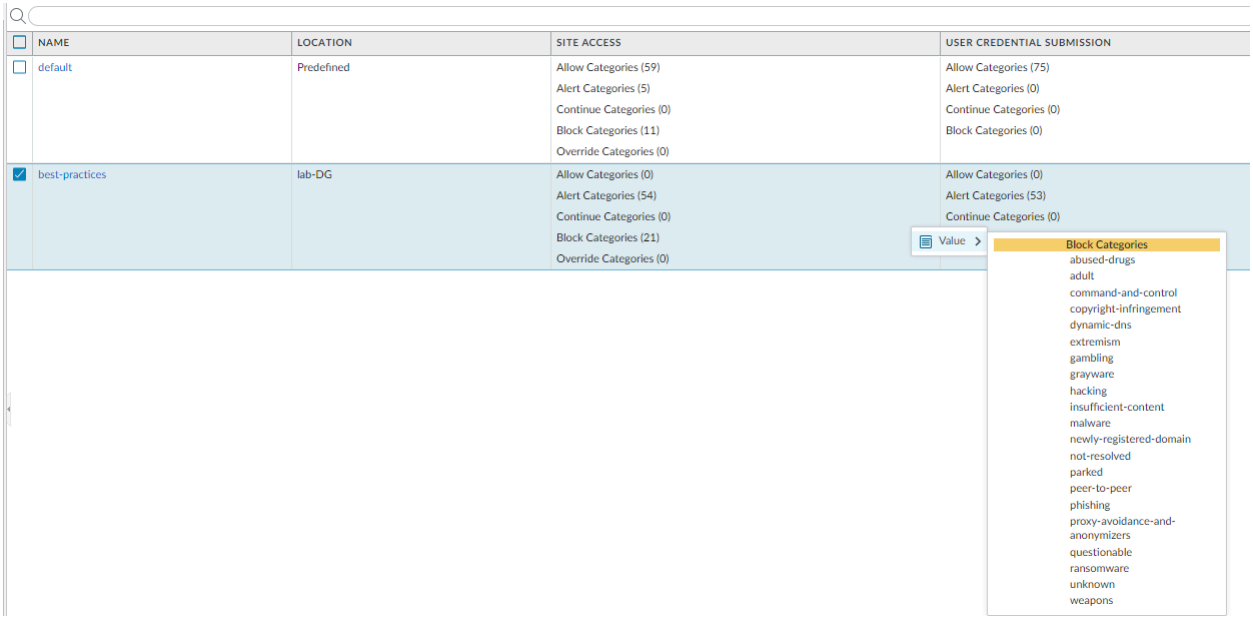
    如果可用性對您的業務來說非常關鍵，且您必須允許來自未知網站的流量，請對該流量套用最嚴格的安全性設定檔，並調查該流量的所有警示。

©2024 Palo Alto Networks, Inc.

- 設定網站存取和使用者認證提交的動作，以根據法律或業務需求以及潛在的責任風險封鎖以下 URL 類別。如果不封鎖這些網站，請對該流量發出警示並套用嚴格的安全性設定檔。
  - 藥物濫用—宣傳非法和合法藥物濫用的網站。
  - **adult**（成人）—包含任何類型成人內容（包括遊戲和漫畫，以及露骨材料、媒體、藝術、論壇和服務）的所有網站。
  - 侵犯著作權—包含非法內容且存在責任風險的網域。
  - **extremism**（極端主義）—宣揚恐怖主義、種族主義、剝削兒童等內容的網站。
  - **gambling**（賭博）—彩票和賭博網站。
  - **peer-to-peer**（點對點）—點對點分享種子、下載程式、媒體檔案或其他軟體應用程式。（不包括共享軟體或免費軟體網站。）
  - 可疑—宣傳低俗笑料、針對特定受眾特徵的攻擊性內容的網站。
  - **weapons**（武器）—出售、評論、描述或說明武器及其用法。

  還要考慮您要如何處理加密貨幣和煙酒 URL 類別。請根據您的業務需求，對其發出警示並對該流量套用嚴格的安全性設定檔或加以封鎖。
- 封鎖高風險類別的使用者認證提交。（不要封鎖高風險類別的網站存取。）

除了封鎖已知不良類別之外，您還應該針對所有其他類別發出警示，以查看使用者造訪的網站。如果您需要逐步採用封鎖政策，請設定類別以繼續並建立自訂回應頁面，向使用者講授您的可接受使用政策，並警示他們造訪的網站可能造成威脅的事實。這麼做可讓您在監控期過後封鎖這些類別。



請在設定檔中停用 **Log Container Page Only**（僅記錄容器頁面），此功能預設為啟用狀態。如果僅記錄容器頁面，便無法了解運作中的應用程式，例如發佈、上傳、下載等。停用 **Log Container Page Only**（僅記錄容器頁面）可查看完整日誌，而能夠看到真正的運作中應用程式。

如果你的環境是接受聯邦資助的學校，請啟用 **Safe Search Enforcement**（安全搜尋強制）（法律要求）。

©2024 Palo Alto Networks, Inc.

如果您執行的是 PAN-OS 9.0.4 或更新版本，請啟用保留用戶端要求的選項（依序輸入 **config** 和 **set deviceconfig setting ctd hold-client-request yes**），以確保防火牆會盡可能安全地處理使用者的 Web 要求。防火牆預設會在 PAN-DB 中查閱未快取的 URL 類別時允許要求，然後在伺服器回應時強制執行適當的政策。在此查閱期間保留要求以最大程度地提高安全性（這可能會增加延遲，卻是最安全的選項）。如需詳細資料，請參閱設定 URL 篩選。

如果我無法封鎖所有推薦的類別，該怎麼辦？

如果使用者出於業務目的需要存取所封鎖類別中的網站，請在僅允許必要使用者和應用程式的規則中建立只適用於特定網站的允許清單（如果您合理認為有風險的話）。請了解會管理您可以封鎖、無法封鎖和必須封鎖的網站類型的當地法律和法規。對於您決定允許存取的有風險類別，請設定認證網路釣魚保護，確保使用者不會向可能裝載網路釣魚攻擊的網站提交公司認證。

如果您允許流量流向惡意和有潛在惡意的 URL 類別或存在潛在責任問題的網站，則風險包括：

- 惡意 URL 類別：
  - **command-and-control (** 命令和控制**)**—惡意軟體和/或遭到入侵的系統使用的 Command-and-control URL 與網域和攻擊者的遠端伺服器暗中通訊，以接收惡意命令或外洩資料。
  - **grayware**（灰色軟體）—不符合病毒的定義但惡意或可疑的網站和服務，而且可能降低裝置性能並帶來安全性風險。在 8206 版內容發佈之前，防火牆將灰色軟體放置在惡意軟體或可疑 URL 類別中。如果不確定是否封鎖灰色軟體，請先在灰色軟體上發出警示並調查警報警示，然後決定是否封鎖灰色軟體還是繼續在灰色軟體上發出警示。
  - **malware**（惡意軟體）—已知裝載惡意軟體的網站或用於命令和控制 (C2) 流量且可能出現入侵程式套件的網站。
  - 網路釣魚—已知代管認證網路釣魚頁面或騙取個人身分資訊的網路釣魚。
  - 勒索軟體—已知會散發勒索軟體的網站。
  - 掃描活動—會探查現有弱點或進行針對性攻擊的網站。

©2024 Palo Alto Networks, Inc.

- 有潛在惡意的 URL 類別：
  - 動態 **DNS**—系統的主機與網域名稱，具有動態指派的 IP 位址並且時常用於傳遞惡意軟體裝載或 C2 流量。此外，動態 DNS 網域不會經歷與信譽良好的網域註冊公司註冊的網域一樣的審批程序，因此沒那麼值得信任。
  - **hacking**（入侵）—與非法或可疑地存取或使用設備和軟體相關的網站。包括有助於繞過授權和數位版權系統的網站。

    請為適當的 *PEN* 測試和威脅研究使用者設定這個類別的例外情況。

  - 內容不足—提供測試頁面、未提供任何內容、提供並非用於一般使用者顯示的 API 存取，或要求驗證卻又不顯示任何其他內容的網站和服務。
  - **newly-registered-domain**（新註冊網域）—新註冊網域通常是有目的或使用網域產生演算法產生的，用於惡意活動。
  - **not-resolved**（未解析）—如果 PAN-DB 雲端無法連線，且 URL 不在防火牆的 URL 篩選快取中，則防火牆無法解析和識別 URL 類別。

    為了獲得最高的安全性，請啟用 ***Hold client request for category lookup***（保留用戶端要求以進行類別查閱），以便防火牆有更多時間解析 *URL* 類別。這會延長防火牆向雲端查詢類別類型的時間，進而提高安全性，但可能會增加延遲。

  - 寄放—個人註冊的網域，通常後來發現用於認證的網路釣魚。這些網域可能與合法網域類似，例如 pal0alto0netw0rks.com，其意圖是騙取認證或個人身分資訊。或者，它們也可能是個人購買其權益以期望有朝一日可以升值的網域，例如 panw.net。
  - **Proxy-avoidance-and-anonymizers (**代理程式規避與匿名者**)**—URL 和服務通常用於避開內容篩選產品。
  - **unknown**（未知）—PAN-DB 尚未識別的網站。如果可用性對您的企業非常重要，且您必須允許流量，請對未知網站發出警示，將最佳做法安全性設定檔套用至流量，並調查警示。

    PAN-DB 即時更新在第一次嘗試存取某未知網站後會記住該網站，因此未知 *URL* 可被快速識別，成為已知 *URL*，以便防火牆根據實際 *URL* 類別進行處理。

- 具有潛在責任風險的 URL 類別：
  - **abused-drugs**（藥物濫用）—宣傳濫用合法和非法藥物、銷售和使用吸毒用具，以及製造或銷售毒品的網站。
  - **adult**（成人）—可能不適合工作場所的網站。
  - **Copyright-infringement**（侵犯著作權）—具有非法內容的網域，例如允許非法下載軟體或其他智慧財產權的內容，這些內容會帶來潛在的責任風險。引用此類別以遵守教育業要求的兒童保護法，以及有些國家要求網際網路供應商防止使用者透過他們的服務分享有著作權的材料的法律。
  - **Extremism**（極端主義）—網站宣揚恐怖主義、種族主義、法西斯主義或歧視不同種族背景、宗教或其他信仰的其他極端主義者的觀點。引用此類別以遵守教育業要求的兒童保護

©2024 Palo Alto Networks, Inc.

法。在某些地區，法律和法規可能會禁止存取極端主義網站，因為允許存取可能會帶來責任風險。

- 賭博—促成真實和/或虛擬貨幣交換的彩票或賭博網站。此外，還有提供有關賭博的教學課程、建議或其他資訊的網站，包括投注賠率和彩池。
- **peer-to-peer**（點對點）—會讓用戶端存取點對點種子分享、下載程式、媒體檔案或其他軟體應用程式的網站，主要用於防止 BitTorrent 下載功能。不包括共享軟體或免費軟體網站。
- 可疑—包含針對特定個人或團體、犯罪活動、非法活動和快速致富計劃的潛在攻擊性內容的網站。
- **weapons**（武器）—銷售、評論、描述或說明武器及其用法而可能不適合工作場所的網站。

預設 *URL* 篩選設定檔會封鎖惡意軟體、網路釣魚和命令和控制 *URL* 類別，但不會封鎖建議封鎖的類別以外的其餘類別。預設 *URL* 篩選設定檔還會封鎖藥物濫用、成人內容、賭博、可疑內容與武器等 *URL* 類別。是否封鎖這些 *URL* 類別視乎您的業務需求而定。例如，大學可能不會限制學生存取其中大部分的網站，因為可用性十分重要，但將安全性視為首要目標的公司則可能會封鎖全部項目。

URL 篩選範例

URL 篩選與檔案封鎖、解密、外部動態清單 (EDL)、記錄和其他安全性功能搭配運作，以建立不只封鎖或允許整個 URL 類別的精細政策。使用 URL 篩選安全轉換步驟，評估您想要允許的網站和您想要封鎖的網站，然後實作符合您業務需求的政策。例如：

- 將基於風險的 URL 類別（高風險、中風險和低風險）與其他 URL 類別結合使用，以將解密流量或封鎖流量作為目標。例如，您可以：
  - 封鎖流向金融服務類別的高風險網站流量。
  - 解密所有高風險和中風險 Web 流量。
  - 如果防火牆沒有足夠的資源來解密要解密的所有流量，請解密流向特定 URL 類別的高風險和中風險流量。
- 記錄高風險和中風險類別網域的所有使用者代理程式和轉介、所有 URL 以及所有檔案下載，來增加可見度。
- 允許在將檔案封鎖設定檔套用至流量時存取個人網站和部落格這類類別，以防止下載具風險的內容，例如 .exe、.scr 和其他潛在惡意檔案。
- 使用預先定義的 **Palo Alto Networks - Bulletproof IP addresses**（**Palo Alto Networks - Bulletproof IP** 位址）EDL，防止存取裝載在 Bulletproof ISP 上的網站，尤其是在您允許存取高風險或中風險金融網站的情況下。
- 使用 URL 類別的組合來簡化政策。

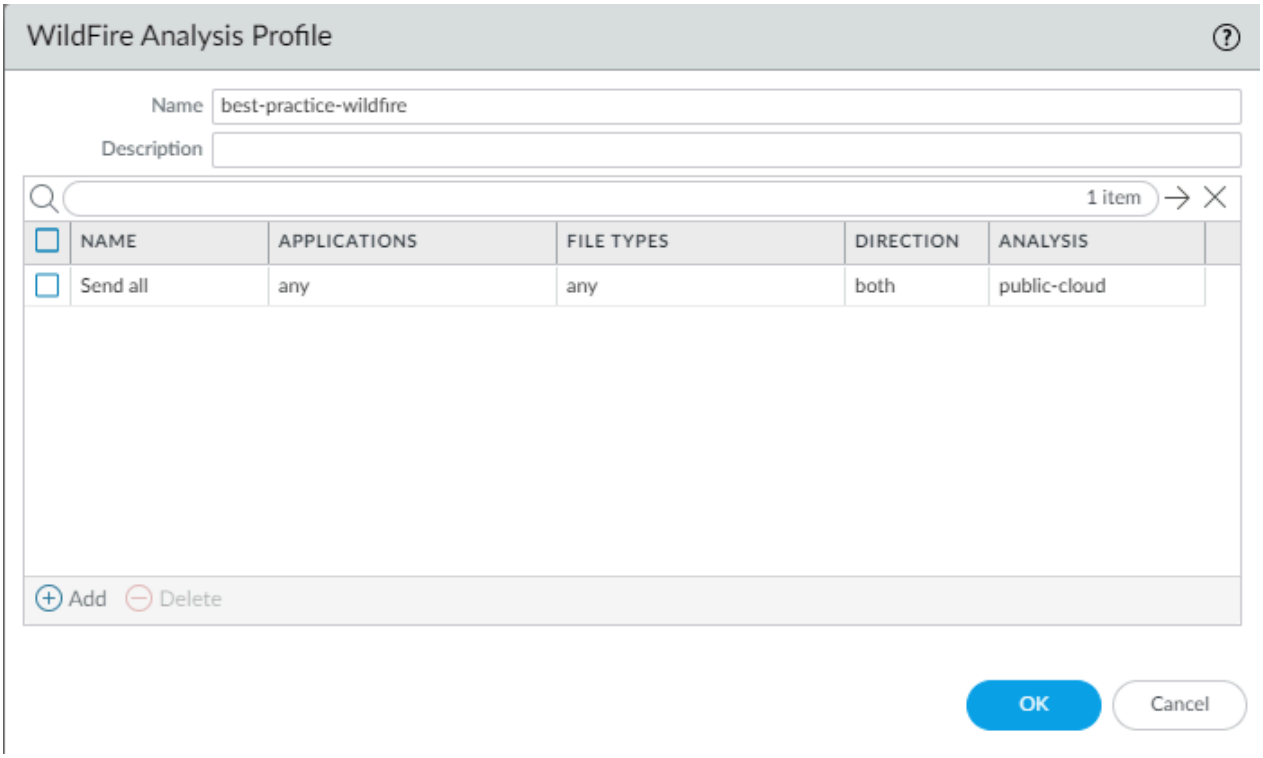
最佳做法網際網路閘道 WildFire 分析設定檔

請將檔案轉送到 WildFire 進行分析，以保護網路免於遭受未知威脅。若缺了這層保護，攻擊者便能滲透網路，入侵員工日常使用的應用程式中的弱點。由於 WildFire 可防禦未知威脅，因此它是您對抗進階持續性威脅 (APT) 的最佳防線。

©2024 Palo Alto Networks, Inc.

設定 WildFire 設備內容更新以自動即時下載和安裝，以便您可以一直獲得最新的支援。

最佳做法 WildFire 分析設定檔將所有檔案雙向（上傳和下載）傳送給 WildFire 進行分析。具體來說，需確保傳送所有的 PE 檔案（如果您未按照檔案封鎖最佳做法封鎖它們）、Adobe Flash 與 Reader 檔案（PDF、SWF）、Microsoft Office 檔案（PowerPoint、Excel、Word、RTF）、Java 檔案（Java、.CLASS）以及 Android 檔案 (.APK)。



透過電子郵件、SNMP 或系統記錄伺服器設定惡意軟體警告，以便防火牆在遇到潛在問題時立即通知您。隔離遭入侵主機的速度越快，先前的未知惡意軟體傳播到其他資料中心裝置的可能性就越低，修復問題也就越容易。

如有必要，您可以根據流量方向限制傳送進行分析的應用程式與檔案類型。

如果流量產生的 *WildFire* 特徵碼引發重設或丟棄動作，防毒設定檔中的 *WildFire Action*（*WildFire* 動作）設定可能會影響流量。您可以排除內部流量（例如用來部署自訂程式的軟體散佈應用程式），以便安全地轉換為最佳做法（否則，*WildFire* 可能會將自訂程式識別為惡意程式並為其產生特徵碼）。檢查 ***Monitor***（監控） > ***Logs***（日誌） > ***WildFire Submissions***（***WildFire*** 提交），以查看是否有任何內部自訂程式觸發了 *WildFire* 特徵碼。

©2024 Palo Alto Networks, Inc.

定義初始網際網路閘道安全性原則

最佳做法網際網路閘道安全性政策的目標是，使用允許的應用程式的積極實作。然而，要識別在您網路上執行的確切應用程式、哪些應用程式對您的業務來說很關鍵，以及誰需要存取每個應用程式，會很花時間。若要根據應用程式允許規則建立安全性政策，請從規則庫開始，規則庫可隨意允許您為使用者正式認可的應用程式，以及已容許的一般業務應用程式和個人應用程式（如果適合您的業務）。

初始政策包括明確封鎖已知惡意 IP 位址和應用程式的規則，以及可在您轉換為最佳做法政策時幫助完善政策並保持應用程式可用性的臨時允許規則。

若要跨多個位置套用一致的安全性政策，您可以重新使用範本和範本堆疊，這樣相同的政策會套用到在每個位置的每個網際網路閘道防火牆中。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

以下主題描述如何建立初始規則庫、描述每個規則有其必要的原因，並說明忽略最佳做法建議的風險：

- 步驟 1：根據受信任威脅情報來源建立規則
- 步驟 2：建立應用程式允許規則
- 步驟 3：建立應用程式封鎖規則
- 步驟 4：建立臨時調整規則
- 步驟 5：針對不符合任何規則的流量啟用記錄

步驟 1：根據受信任威脅情報來源建立規則

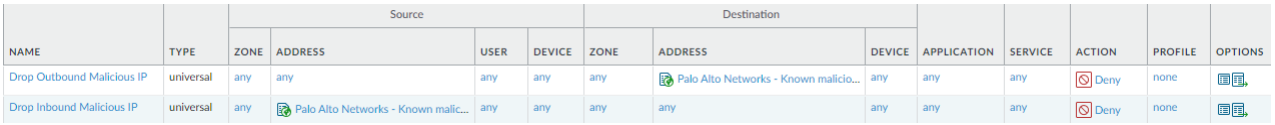
請封鎖 Palo Alto Networks 和受信任的第三方來源已證明是惡意的主機所傳來的流量。進階威脅防護授權（或有效的舊版威脅防護授權）包括內建的外部動態清單 (EDL)，這些清單中包含已知的惡意 IP 位址。請在政策中使用 EDL 來封鎖惡意流量。Palo Alto Networks 會根據最新的威脅情報編譯並動態更新這些清單。防火牆不必重新開機就能收到並實作動態更新。

STEP 1 | 封鎖傳送自/至 Palo Alto Networks 識別為惡意之 IP 位址的流量。

我為什麼需要這些規則？	規則重點
❑ 該規則可針對 Palo Alto Networks 已證實幾乎專用於散佈惡意軟體、啟動命令控制活動及發動攻擊之 IP 位址，為您提供保護。	• 一條規則用於封鎖輸出到已知惡意 IP 位址的流量，另一條規則用於封鎖從這些位址輸入的流量。 • 將外部動態清單 **Palo Alto Networks - Known malicious IP addresses**（**Palo Alto Networks -** 已知惡意 **IP** 位址）用作輸出流

©2024 Palo Alto Networks, Inc.

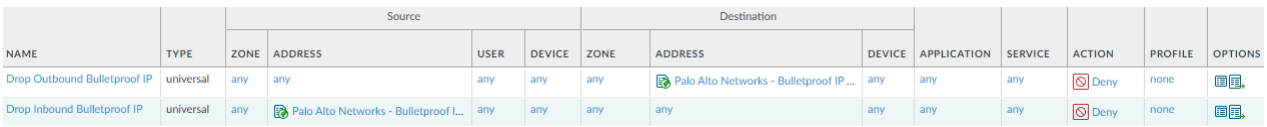
我為什麼需要這些規則？	規則重點
	量規則的目的地位址、輸入流量規則的來源位址。 • 拒絕與這些規則相符的流量。 • 針對與這些規則相符的流量啟用氣質記錄，以便您可調查網路上的潛在威脅。 • 由於這些規則可以阻止惡意流量，因此可以保護在任何連接埠上執行的任何使用者所傳來的流量。



NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Malicious IP	universal	any	any	any	any	any	Palo Alto Networks - Known malicio...	any	any	any	Deny	none	
Drop Inbound Malicious IP	universal	any	Palo Alto Networks - Known malic...	any	any	any	any	any	any	any	Deny	none	

STEP 2 | 封鎖與 Bulletproof 託管提供者之間的流量。

我為什麼需要這些規則？	規則重點
❑ 此規則會防禦 Palo Alto Networks 已顯示屬於 Bulletproof 託管提供者的 IP 位址。 Bulletproof 裝載提供者對內容沒有任何限制或具有有限的限制，而且不會記錄事件。Bulletproof 網站是啟動命令和控制 (C2) 攻擊和非法活動的理想位置，因為會執行所有項目，但不會進行任何追蹤。	• 一條規則用於封鎖輸出到已知 Bulletproof 託管 IP 位址的流量，另一條規則用於封鎖從這些位址輸入的流量。 • 將外部動態清單 **Palo Alto Networks - Bulletproof IP addresses**（**Palo Alto Networks**—**Bulletproof IP** 位址）設定為輸出流量規則的目的地位址以及輸入流量規則的來源位址。 • 拒絕與這些規則相符的流量。 • 針對與這些規則相符的流量啟用氣質記錄，以便您可調查網路上的潛在威脅。 • 由於這些規則可以阻止惡意流量，因此可以保護在任何連接埠上執行的任何使用者所傳來的流量。



NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Drop Outbound Bulletproof IP	universal	any	any	any	any	any	Palo Alto Networks - Bulletproof IP ...	any	any	any	Deny	none	
Drop Inbound Bulletproof IP	universal	any	Palo Alto Networks - Bulletproof I...	any	any	any	any	any	any	any	Deny	none	

©2024 Palo Alto Networks, Inc.

STEP 3 | 封鎖和記錄傳送自/至受信任威脅諮詢報告中高風險 IP 位址的流量。

我為什麼需要這些規則？	規則重點
雖然 Palo Alto Networks 沒有直接證據證明高風險 IP 位址摘要中的 IP 位址有惡意，但威脅諮詢報告認為這些位址存在惡意行為。 ❑ 封鎖並記錄流量，如這個範例所示。 ❑ 如果出於業務原因必須允許高風險 IP 位址，請建立具有嚴格安全性設定檔而只會允許該 IP 位址的安全性政策規則，並將其放在規則庫中高風險 IP 位址封鎖規則的前面。密切監控並記錄您選擇允許的任何高風險 IP 位址。	• 一條規則用於記錄輸出到高風險 IP 位址而遭到封鎖的流量，另一條規則用於記錄從這些位址輸入而遭到封鎖的流量。 • 將外部動態清單 **Palo Alto Networks - High risk IP addresses**（**Palo Alto Networks - 高風險 IP 位址**）用作輸出流量規則的目的地位址、輸入流量規則的來源位址。 • 如果您允許流量，則請套用最佳做法安全性設定檔。 • 由於這些規則可以阻止惡意流量，因此可以針對任何應用程式保護在任何連接埠上執行的任何使用者所傳來的流量。

		Source				Destination							
NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Outbound High Risk IPs	universal	any	any	any	any	any	Palo Alto Networks - High risk IP addresses	any	any	any	Deny	none	
Block Inbound High Risk IPs	universal	any	Palo Alto Networks - Known malicious IP addresses	any	any	any	any	any	any	any	Deny	none	

STEP 4 | 同樣地，使用 **Palo Alto Networks - Tor exit IP addresses**（**Palo Alto Networks - Tor 結束 IP 位址**）外部動態清單建立兩個規則來封鎖和記錄進出 Tor 結束節點的流量，這些流量往往（但非一定）與惡意活動有關聯，在企業環境中尤其如此。

步驟 2：建立應用程式允許規則

在建立應用程式允許規則前，要先識別您的應用程式允許清單。請根據應用程式（而非連接埠）建立允許規則。除了某些需要使用者存取才能讓防火牆識別使用者的基礎架構應用程式外，請只對已知使用者允許存取權。建立可存取所允許應用程式的使用者群組，並限制只有有存取每個應用程式之業務需求的特定使用者或使用者群組能獲得使用者存取權。

若要將基於連接埠的規則轉換為基於應用程式的規則，或從基於連接埠的防火牆進行移轉，請遵循移轉至基於應用程式的政策的最佳做法中的建議，該最佳做法會利用政策最佳化工具。政策最佳化工具可協助您分析基於連接埠的規則，並向您顯示與這些規則相符的確切應用程式。其還可協助您尋找未使用的規則、具有未使用應用程式的規則（過度佈建的規則），以及基於連接埠的現有規則。

請將特定規則放在安全性政策規則庫中的一般規則之上。否則，一般規則可能會遮蔽特定規則。（當您將廣泛規則放在規則庫中比特定規則更高的位置，而廣泛規則所包含的比對規則與更特定的規則相同時，便會發生遮蔽，因此流量會比對特定規則而不是比對一般規則。）

規則庫的這個部分包括識別為應用程式允許清單一部分的應用程式的允許規則，包括：

©2024 Palo Alto Networks, Inc.

- 為企業與基礎架構用途而佈建與管理的認可的應用程式。
- 一般的業務應用程式使用者可能需要完成他們的工作。
- 您選擇允許個人使用的容許應用程式。

標記所有認可的應用程式，方法是採用預先定義的認可的標籤。*Panorama* 和防火牆將沒有「認可的」標籤的應用程式視為未認可的應用程式。

附加最佳做法安全性設定檔以掃描所有允許的流量是否有已知和未知威脅。如果您尚未建立這些設定檔，請建立網際網路閘道的最佳做法安全性設定檔。由於您無法檢查看不到的內容，因此請將防火牆設定為解密流量以進行全面檢視和威脅檢查。

STEP 1 | 允許存取您的公司 DNS 伺服器。

請只允許流量流向認可的 *DNS* 伺服器。使用 DNS 安全性服務以防止有人連線到惡意的 *DNS* 伺服器。

我為什麼需要此規則？	規則重點
❑ DNS 的存取權提供了網路基礎架構服務，並且經常被攻擊者入侵。 ❑ 僅允許存取內部 DNS 伺服器可減小攻擊面。	• 由於此規則非常特定，因此請將其置於規則庫頂端附近。 • 建立位址物件以用於目的地位址，確保使用者僅存取資料中心的 DNS 伺服器。 • 由於使用者在登入前需要存取這些服務，因此請向任何使用者允許存取權。

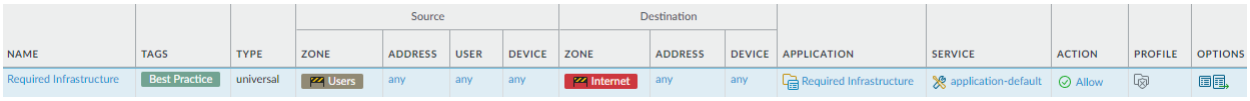
			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT DNS Services	Best Practice	universal	Users	any	any	any	IT Infrastructure	DNS Servers	any	dns	application-default	Allow		

STEP 2 | 允許存取其他必需 IT 基礎架構資源。

我為什麼需要此規則？	規則重點
❑ 啟用提供 NTP、OCSP、STUN 和 ping 等網路基礎架構及管理功能的應用程式。 ❑ 先前的規則將允許的 DNS 流量限於資料中心內的目的地位址，這些應用程式可能不在資料中心內，因此需要單獨的規則。	• 由於這些應用程式在預設連接埠上執行、會向任何使用者（因為需要這些服務的時間不一定，使用者可能還未登入且未被系統知悉）允許存取權，且目的地位址是 **any**（任何），因此請將這些應用程式新增到某個應

©2024 Palo Alto Networks, Inc.

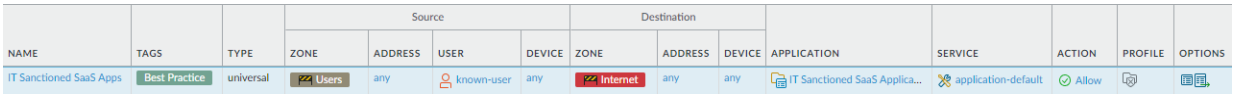
我為什麼需要此規則？	規則重點
	用程式群組，並建立一個規則來為所有應用程式啟用存取權。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Required Infrastructure	Best Practice	universal	Users	any	any	any	Internet	any	any	Required Infrastructure	application-default	Allow		

STEP 3 | 允許存取 IT 認可的 SaaS 應用程式。

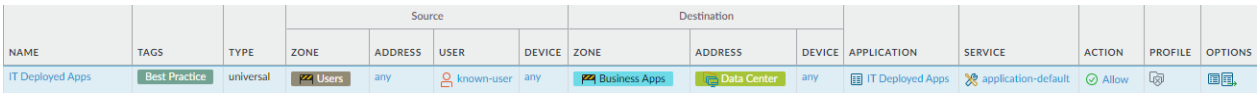
我為什麼需要此規則？	規則重點
❑ 使用 SaaS 應用程式時，專有資料位於雲端。此規則確保只有已知使用者可以存取這些應用程式（及基礎資料）。 ❑ 掃描允許的 SaaS 流量存在的威脅。	• 建立應用程式群組以控制所有認可的 SaaS 應用程式。 • SaaS 應用程式應一律在應用程式預設連接埠上執行。 • 限制存取權只能提供給已知的使用者。請參閱為存取允許的應用程式建立使用者群組。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Sanctioned SaaS Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	IT Sanctioned SaaS Applica...	application-default	Allow		

STEP 4 | 允許存取 IT 佈建的內部部署應用程式。

我為什麼需要此規則？	規則重點
❑ 攻擊通常會在外洩階段使用 FTP 等業務關鍵資料中心應用程式，或入侵應用程式弱點以進行橫向移動。 ❑ 許多資料中心應用程式會使用多個連接埠。將服務設定為 **application-default**（應用程式預設值）可在其標準連接埠上安全地啟用應用程式。請勿允許非標準連接埠上的應用程式，這些應用程式通常與規避性的行為相關聯。	• 建立應用程式群組將所有資料中心應用程式分組。 • 為資料中心伺服器位址建立一個位址群組。 • 限制存取權只能提供給已知的使用者。請參閱為存取允許的應用程式建立使用者群組。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
IT Deployed Apps	Best Practice	universal	Users	any	known-user	any	Business Apps	Data Center	any	IT Deployed Apps	application-default	Allow		

©2024 Palo Alto Networks, Inc.

STEP 5 | 允許存取管理使用者需要的應用程式。

我為什麼需要此規則？	規則重點
❑ 為了減少攻擊面，可建立可存取所允許應用程式的使用者群組。 ❑ 由於管理員通常需要存取敏感的帳戶資料及遠端存取其他系統（例如 RDP），若要減少攻擊面，請只向具有業務需要的管理員允許存取權。	• 此規則僅限 IT_admins 群組中的使用者存取。 • 為每個內部應用程式或非標準連接埠上執行的應用程式建立自訂應用程式，以便在其預設連接埠上強制執行它們，而非在網路上開啟其他連接埠。 • 如果您擁有針對不同應用程式的不同使用者群組，則建立單獨的規則以實現細化控制。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Administrative Apps	Best Practice	universal	Users	any	IT_Admins	any	IT Infrastructure	any	any	ms-rdp ssh	application-default	Allow		

STEP 6 | 允許存取通用型商務應用程式。

我為什麼需要此規則？	規則重點
❑ 除了您為使用者認可和管理的應用程式外，使用者通常還需要存取其他業務應用程式，例如 Zoom、Adobe 線上服務或 G Suite。 ❑ 此規則可讓您在掃描威脅的同時安全地允許網頁瀏覽。請參閱建立網際網路閘道的最佳做法安全性設定檔。	• 限制存取權只能提供給已知的使用者。請參閱為存取允許的應用程式建立使用者群組。 • 為了獲得可見度，需為要允許的每類應用程式建立應用程式篩選器。 • 附加最佳做法安全性設定檔以防止所有流量中的已知和未知威脅。

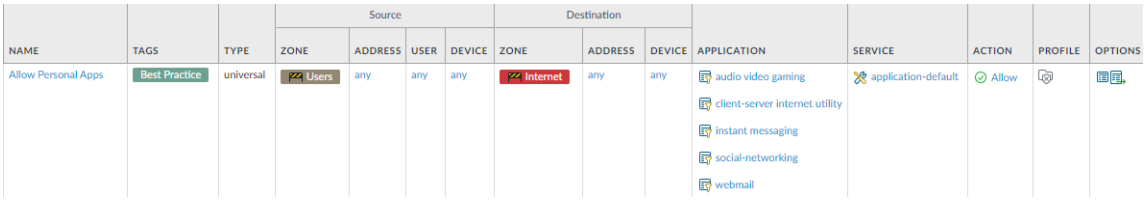
			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
General Business Apps	Best Practice	universal	Users	any	known-user	any	Internet	any	any	browser-based businesses office programs update software	application-default	Allow		

STEP 7 | (選用) 允許存取個人應用程式。

我為什麼需要此規則？	規則重點
❑ 隨著工作裝置與個人裝置之間的界線變得模糊，使用者存取的所有應用程式皆已安全啟用並且不存在威脅。 ❑ 在建立這個初始規則庫時，請使用應用程式篩選器以便安全地啟用個人應用程式的存取	• 限制存取權只能提供給已知的使用者。請參閱為存取允許的應用程式建立使用者群組。 • 為了獲得可見度，需為要允許的每類應用程式建立應用程式篩選器。

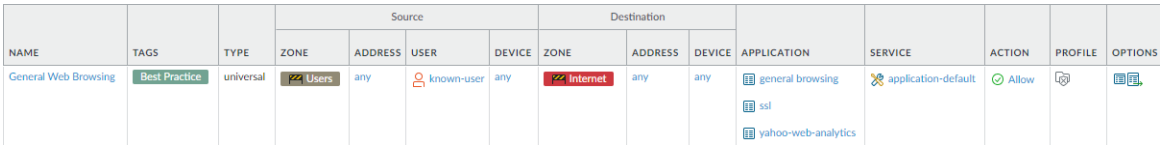
©2024 Palo Alto Networks, Inc.

我為什麼需要此規則？	規則重點
權。在評估正在使用的應用程式時，請使用此資訊來決定是否移除篩選器並提供適於可接受使用政策的個人應用程式的更小子集。	• 附加最佳做法安全性設定檔以防止所有流量中的已知和未知威脅。



STEP 8 | 提供一般網頁瀏覽。

我為什麼需要此規則？	規則重點
❑ 先前的規則允許存取個人應用程式（其中許多為以瀏覽器為基礎）。此規則允許一般的網頁瀏覽。 ❑ 一般網頁瀏覽比其他類型的應用程式流量更容易遭受風險。請建立最佳做法安全性設定檔並將其附加到此規則，以便安全地啟用網頁瀏覽。 ❑ 由於威脅通常隱藏於加密流量中，因此若要安全地啟用網頁瀏覽，請解密流量以進行全面檢視和威脅檢查。	• 使用與其他規則相同的最佳做法安全性設定檔，並盡可能收緊 URL 篩選設定檔。 • 若要協助防止帶有惡意軟體的裝置或嵌入式裝置連線到網際網路，請只允許已知使用者。 • 使用應用程式篩選器以允許存取通用型應用程式。 • 若要讓使用者能夠瀏覽您選擇不要列入解密範圍的 HTTPS 網站，請明確允許 SSL 作為應用程式。 • 將服務設定為 **application-default**（應用程式預設值）。



步驟 3：建立應用程式封鎖規則

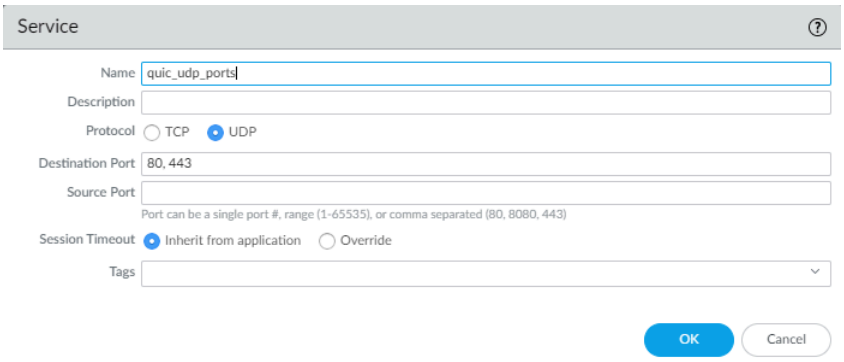
在開發和調整安全性政策規則庫時，應用程式封鎖規則可為您防範規避性應用程式和常被入侵的應用程式。臨時調整規則有助於找到政策漏洞並識別可能的攻擊。由於這些規則會擷取您不知道正在網路上執行的應用程式流量，因此其會允許可能構成安全風險的流量。下列封鎖規則會明確封鎖攻擊者常會使用的潛在惡意應用程式和通訊協定，例如公用 DNS 和 SMTP、加密通道、遠端存取和非認可的檔案共用應用程式。

©2024 Palo Alto Networks, Inc.

STEP 1 | 封鎖快速 UDP 網際網路連線 (QUIC) 通訊協定。

我為什麼需要此規則？	規則重點
❑ Chrome 和一些其他瀏覽器會使用 QUIC（而非 TLS）來建立工作階段。QUIC 會使用防火牆無法解密的專有加密，因此有潛在危險性的加密流量可能會進入網路。 ❑ 封鎖 QUIC 會強制瀏覽器回退到 TLS，並讓防火牆可以解密流量。	• 建立指定 UDP 連接埠 80 和 443 的服務（**Objects**（物件）> **Services**（服務））。 • 第一個規則會封鎖其 UDP 服務連接埠（80 和 443）上的 QUIC，並使用您已建立來指定這些連接埠的服務。 • 第二個規則會封鎖 QUIC 應用程式。

服務會指定要針對 QUIC 進行封鎖的 UDP 連接埠。



第一個規則會指定您為 QUIC 設定的服務，第二個規則會封鎖 QUIC 應用程式：

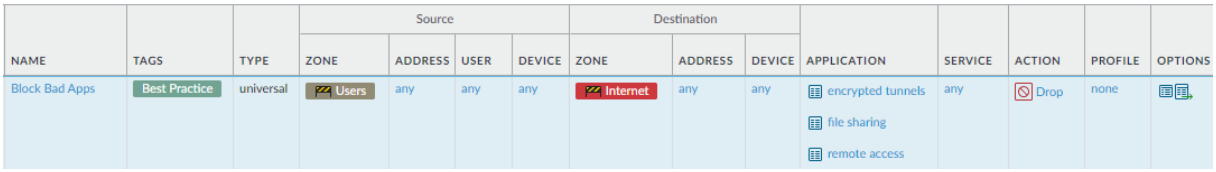
			Source				Destination							
	NAME	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	universal	l3-vlan-trust	any	any	any	l3-untrust	any	any	quic	application-default	Deny	none	

STEP 2 | 封鎖沒有合法使用案例的應用程式。

我為什麼需要此規則？	規則重點
❑ 封鎖有潛在惡意的應用程式，例如加密通道、點對點檔案共用以及 IT 尚未認可的 Web 式檔案共用應用程式。 ❑ 因為臨時調整規則可能會允許具有惡意意圖的流量，以及未如預期符合您政策規則的合法流量，因此其可能會允許有風險或惡意的流量。此規則會封鎖沒有合法使用案例的流	• 使用 **Drop**（丟棄）動作無訊息地丟棄流量，而不向用戶端或伺服器傳送訊號。 • 針對與此規則相符的流量啟用記錄，以便您可以調查網路上應用程式的潛在威脅及誤用情形。 • 由於此規則目的是攔截惡意流量，因此它會與來自任何使用者之任何連接埠上執行的流量比對。

©2024 Palo Alto Networks, Inc.

我為什麼需要此規則？	規則重點
量，以及攻擊者或疏忽的使用者可以使用的流量。	

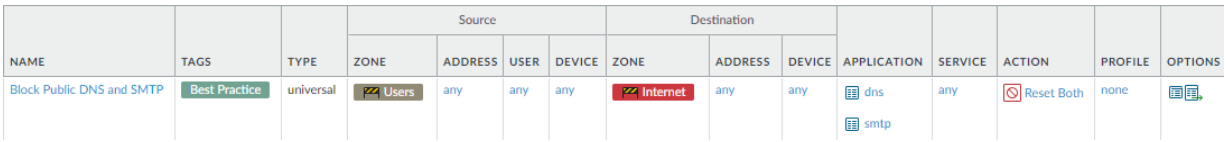


NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Bad Apps	Best Practice	universal	Users	any	any	any	Internet	any	any	encrypted tunnels file sharing remote access	any	Drop	none	

STEP 3 | 封鎖公共 DNS 和 SMTP 應用程式。

請只允許流量流向認可的 *DNS* 伺服器。使用 DNS 安全性服務以防止有人連線到惡意的 *DNS* 伺服器。

我為什麼需要此規則？	規則重點
❑ 封鎖公共 DNS/SMTP 應用程式以避免 DNS 通道、命令和控制流量以及遠端管理應用程式。	• 使用 **Reset both client and server**（重設用戶端與伺服器）傳送 TCP 重設訊息至用戶端及伺服器裝置。 • 為符合此規則的流量啟用記錄，以便您可以調查潛在威脅。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block Public DNS and SMTP	Best Practice	universal	Users	any	any	any	Internet	any	any	dns smtp	any	Reset Both	none	

步驟 4：建立臨時調整規則

臨時調整規則可協助您監控初始最佳做法規則庫中是否存在漏洞，並就危險行為向您發出警示。

例如，臨時規則可識別來自未知使用者的流量，或來自在非預期連接埠上執行的應用程式的流量。監控與臨時規則相符的流量，以全面了解網路上使用中的所有應用程式（並在轉換為最佳做法規則庫時確保應用程式可用性）。使用此資訊可以幫助您微調允許清單，方法是為您不知道您需要的應用程式新增允許規則，或是縮小允許規則的範圍，並以應用程式群組或特定應用程式取代應用程式篩選器。當流量不再符合這些規則時，便可以移除臨時規則。

某些臨時調整規則的優先順序會高於封鎖不良應用程式的規則，某些規則的優先順序則會較低，以確保目標流量與適當的規則相符，同時確保不良流量不會進入您的網路。

©2024 Palo Alto Networks, Inc.

STEP 1 | 允許已知使用者在非標準連接埠上進行網頁瀏覽和 SSL，以確定非標準連接埠上是否有任何合法應用程式正在執行。

我為什麼需要此規則？	規則重點
❑ 此規則可協助您確定您的政策中是否存在漏洞，在該政策中，使用者無法存取在非標準連接埠上執行的合法應用程式。 ❑ 監控與此規則相符的所有流量。對於合法流量，請將適當的應用程式新增到適當的允許規則中。視情況建立自訂應用程式。	• 與僅允許預設連接埠上的應用程式的允許規則不同，此規則會允許任何連接埠上的網頁瀏覽與 SSL 流量，以尋找允許清單中的漏洞。 • 由於此規則會尋找政策漏洞，因此請將其限制為只能用於網路上的已知使用者。 • 如果您要允許使用者瀏覽未解密的 HTTPS 網站（例如金融服務和醫療保健網站），請在此規則中明確允許 SSL 作為應用程式。 • 附加最佳做法安全性設定檔以掃描威脅。 • 將此規則新增至應用程式封鎖規則之上，否則不會有流量符合此規則。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected Port SSL and Web	Best Practice	universal	Users	any	known-user	any	Internet	any	any	ssl web-browsing	any	Allow		

STEP 2 | 允許連接埠上來自未知使用者的網頁瀏覽與 SSL 流量，以反白顯示所有連接埠上的所有未知使用者。

我為什麼需要此規則？	規則重點
❑ 此規則有助於您確定 User-ID 涵蓋範圍內是否有漏洞。 ❑ 此規則有助於您識別嘗試連線到網際網路的遭入侵裝置或嵌入式裝置。 ❑ 務必封鎖非標準的連接埠使用，即使針對網頁瀏覽流量也不例外，因為這是一種規避技術。	• 雖然大多數應用程式允許規則適用於已知使用者或特定使用者群組，此規則會明確比對來自 **unknown**（未知）使用者的流量。 • 此規則必須位列應用程式封鎖規則之上，或流量從不符合此規則。 • 附加最佳做法安全性設定檔以掃描威脅。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unknown User SSL and Web	Best Practice	universal	Users	any	unknown	any	Internet	any	any	ssl web-browsing	any	Allow		

©2024 Palo Alto Networks, Inc.

STEP 3 | 允許應用程式預設值連接埠上的所有應用程式識別非預期的應用程式。

我為什麼需要此規則？	規則重點
❑ 此規則對網路上執行之您不知道的應用程式提供透視，因此您可微調您的應用程式允許清單。 ❑ 監控與此規則相符的所有流量，以確定流量是否代表潛在威脅，或者您是否需要修改允許規則以存取更多的應用程式。	• 由於此規則允許所有應用程式，因此您必須將其新增在應用程式封鎖規則之後，以防止不良應用程式在網路上執行。 • 如果您執行的是 PAN-OS 7.0.x 或更舊版本，為了適當地識別非預期的應用程式，請建立應用程式篩選器並於其中包括所有應用程式，而不是將規則設為允許 **any**（任何）應用程式。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Traffic	Best Practice	universal	Users	any	any	any	Internet	any	any	All apps	application-default	Allow		

STEP 4 | 允許任何連接埠上的任何應用程式識別在非標準連接埠上執行的應用程式。

我為什麼需要此規則？	規則重點
❑ 此規則有助於識別未知連接埠上執行的合法、已知的應用程式。 ❑ 此規則有助於識別需要為其建立自訂應用程式並新增至應用程式允許規則的未知應用程式。 ❑ 符合此規則的流量是可操作的。追蹤流量來源並確保不會允許未知的 tcp、udp 或非 syn-tcp 流量。	• 由於這是一個很一般的規則，會允許來自任何連接埠上任何使用者的任何應用程式，因此請將其放在規則庫底部。 • 針對與此規則相符的流量啟用記錄，以便您可調查應用程式的誤用及潛在威脅，或者識別需要自訂應用程式的合法應用程式。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected Port Usage	Best Practice	universal	Users	any	any	any	Internet	any	any	any	any	Allow		

步驟 5：針對不符合任何規則的流量啟用記錄

與您定義的規則不相符的網際網路閘道流量，會與規則庫底部的預先定義區域間預設規則相符並遭到拒絕。若要了解與您建立的規則不相符的流量，請針對區域間預設規則啟用記錄：

STEP 1 | 在規則庫中選取區域間預設規則的所在列，然後 **Override**（取代）規則以進行編輯。

STEP 2 | 選取 **interzone-default**（區域間預設）規則名稱以開啟規則供編輯。

©2024 Palo Alto Networks, Inc.

STEP 3 | 在 **Actions**（動作）頁籤上，選取 **Log at Session End**（工作階段結束時記錄），然後按一下 **OK**（確定）。

STEP 4 | 建立自訂報告以監控與規則相符的流量：

1. 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告）。
2. **Add**（新增）報告，並為它設定具描述性的 **Name**（名稱）。
3. 將 **Database**（資料庫）設為 **Traffic Summary**（流量摘要）。
4. 選取 **Scheduled**（已排程）核取方塊。
5. 將 **Rule**（規則）、**Application**（應用程式）、**Bytes**（位元組）、**Sessions**（工作階段）新增到 Selected Columns（選定欄）清單。
6. 設定所需的 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式）欄位。
7. 定義查詢以比對符合區域間預設規則的流量：

   ```
   (rule eq 'interzone-default')
   ```

STEP 5 | **Commit**（交付）您對規則庫執行的變更。

©2024 Palo Alto Networks, Inc.

監控與微調政策規則庫

建立最佳做法安全性政策是一個反覆的過程。在定義初始網際網路閘道安全性政策後，請監控與用於識別政策漏洞及危險行為的臨時規則相符的流量，並相應地調整您的政策。監控與這些規則相符的流量可讓您適當調整永久規則，以及確定所有流量都會與應用程式允許規則相符，或是評估您是否應該允許未與任何規則相符的應用程式。

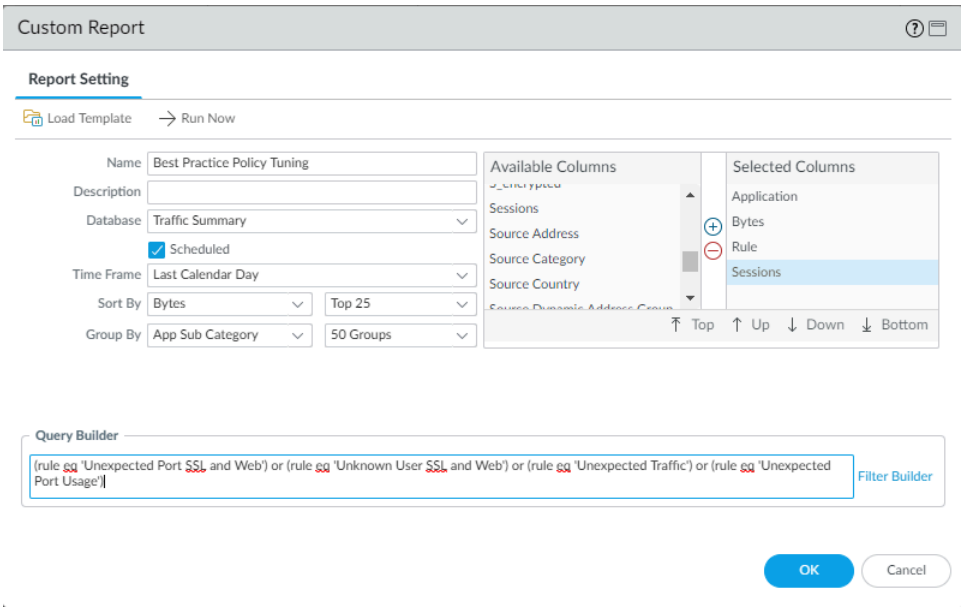
在調整規則庫時，您應該會看到您想要允許與臨時規則相符的流量變得越來越少。當您不再看到想要允許與這些規則相符的流量時，就表示您的積極實施允許規則已經完成，因此可以移除臨時規則（區域間預設拒絕規則會自動拒絕沒有任何規則明確允許的流量）。

由於每月的內容發行中會增加新的 *App-ID*，因此請檢閱 App-ID 變更對您安全性政策的影響。

©2024 Palo Alto Networks, Inc.

STEP 1 | 建立自訂報告以便監控與識別出政策漏洞的規則相符的流量。

1. 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告）。
2. **Add**（新增）報告，並為它設定具描述性的 **Name**（名稱），以指出您正在調查的特定政策漏洞。
3. 將 **Database**（資料庫）設為 **Traffic Summary**（流量摘要）。
4. 選取 **Scheduled**（排程）。
5. 將 **Rule**（規則）、**Application**（應用程式）、**Bytes**（位元組）、**Sessions**（工作階段）新增到 Selected Columns（選定欄）清單。
6. 設定所需的 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式）欄位。
7. 定義查詢以比對與找到政策漏洞和危險行為的規則相符的流量。您可以建立會詳述與任何規則相符（使用 **or** 運算子）之流量的單一報告，也可以建立個別報告以監控每個規則。以下範例查詢會使用範例政策中定義的規則名稱：
   - `(rule eq 'Unexpected Port SSL and Web')`
   - `(rule eq 'Unknown User SSL and Web')`
   - `(rule eq 'Unexpected Traffic')`
   - `(rule eq 'Unexpected Port Usage')`



STEP 2 | 定期檢閱報告以了解流量為何符合每個調整規則。更新規則以包含合法的應用程式和使用者，或使用報告中的資訊來評估應用程式的風險並實作政策改革。

©2024 Palo Alto Networks, Inc.

移除臨時規則

在經過數個月監控初始網際網路閘道最佳做法安全性政策並調整規則庫後，您會發現想要允許的與臨時規則相符的流量會越來越少。當您不再發現想要允許的與這些規則相符的流量時，就已達成轉換為完全基於應用程式的安全性政策規則庫的目標。您這時可以移除臨時規則（包括適用於沒有合法使用案例的應用程式以及適用於公用 DNS 和 SMTP 應用程式的應用程式封鎖規則），因為預設的區域間預設拒絕規則會自動封鎖該流量，因為它未與任何明確的允許規則相符。（請保留 QUIC 的規則。）

STEP 1 | 選取 **Policies**（政策） > **Security**（安全性）。

STEP 2 | 選取規則，然後按一下 **Delete**（刪除）。

或者，將規則 **Disable**（停用） 一段時間，然後再刪除。這可讓您在流量日誌顯示您想要允許的流量與區域間預設拒絕規則相符時，再次 **Enable**（啟用）規則。

STEP 3 | **Commit**（提交）變更。

©2024 Palo Alto Networks, Inc.

維護規則庫

企業和應用程式會不斷發展，因此您的安全性政策規則庫也需要進化。當您認可的應用程式發生變更時，請盡可能對現有的政策規則進行相應的變更，以符合應用程式的商業使用案例，而不是新增規則。政策的變更通常只是將新的應用程式新增至應用程式群組或從應用程式群組中移除已淘汰的應用程式。

在 *Panorama* 或獨立防火牆上，使用政策規則命中計數器分析規則庫的變更。例如，當您新增應用程式時，在您允許應用程式在網路上的流量前，將允許規則新增到規則庫中。若流量命中規則且計數器增加，不是表示即使您尚未啟用該應用程式，符合該規則的流量可能已在網路中，就是表示您可能需要調整規則。透過檢查 ***ACC*** > ***Threat Activity***（威脅活動） > ***Applications Using Non Standard Ports***（使用非標準連接埠的應用程式） 和 ***ACC*** > ***Threat Activity***（威脅活動） > ***Rules Allowing Apps On Non Standard Ports***（允許非標準連接埠上使用應用程式的規則）*Widget*，查看非標準連接埠上的流量是否導致非預期的規則符合。

使用政策規則符合計數器的關鍵在於當您進行變更時重設計數器，例如在引進新應用程式或變更規則的意義時。重設符合計數器確保您看到變更的結果，包括變更前發生的變更和事件。

如果您使用 *Panorama* 管理防火牆，請監控防火牆健康情況以比較它們的基準效能，以及互相比較以發現與正常行為的差異。

將 Palo Alto Networks 內容更新設定為自動下載，並盡快安排在防火牆上安裝。每當安全性設定檔特徵碼需要更新時，便會發生應用程式和威脅內容更新。每月第三個星期二發送的內容更新也包含新的和經過修改的 App-ID（應用程式更新；在極少數情況下，應用程式更新可能會延遲一兩天）。評估新的和經過修改的 App-ID 在非生產環境中如何影響您的安全性政策規則庫，並視需要修改規則。

遵循內容更新最佳做法，盡快安裝更新以保護網際網路閘道，並為所有內容更新設定日誌轉送。

STEP 1 | 在安裝新的內容更新前，請先檢閱新的和經過修改的 App-ID，以確定變更是否會影響政策。

STEP 2 | 視需要修改現有的安全性政策規則以容納 App-ID 變化。如果某些 App-ID 需要更多測試，您可以停用所選 App-ID，然後安裝其餘的新的和經過修改的 App-ID。在下個月釋出內容和新 App-ID 到達（每個月的第三個星期二）前，完成測試和任何必要的政策修改以避免重複。

STEP 3 | 準備政策更新以考慮內容發行中包括的 App-ID 變更，將新認可的應用程式新增至允許規則中，或從允許規則中移除應用程式。

©2024 Palo Alto Networks, Inc.