paloalto
TECHDOCS

進階 **Threat Prevention** 管理

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

Last Revised

May 18, 2023

Table of Contents

進階 Threat Prevention

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

Palo Alto Networks® 新世代防火牆威脅入侵防禦訂閱使用多管齊下的偵測機制來抵禦整個威脅格局，從而保護您的網路免受商品威脅和進階持續性威脅 (APT) 的侵害。Palo Alto Networks 威脅防護解決方案包含以下訂閱：

- 進階 **Threat Prevention**—進階 Threat Prevention 雲端服務使用內嵌深度學習和機器學習模型來即時偵測規避性和從未見過的未知 C2 威脅，以及零時差弱點入侵。作為超低延遲原生雲端服務，這種可延伸且可無限擴展的解決方案始終透過模型訓練改進保持最新狀態。此外，也支援本機深度學習，透過提供一種機制來對零時差威脅和其他規避性威脅執行基於本機深度學習的快速分析，從而補充了進階 Threat Prevention 的內嵌雲端分析元件。進階 Threat Prevention 授權包括 Threat Prevention 附帶的所有好處。
- **Threat Prevention**—基礎 Threat Prevention 訂閱是以從各種 Palo Alto Networks 服務收集的惡意流量資料所產生的特徵碼為根據。防火牆使用這些特徵碼來強制執行基於特定威脅的安全性政策，其中包括：命名與控制 (C2)，各種類型的已知惡意軟體和漏洞入侵；結合防火牆上的 App-ID 和 User-ID 識別技術，您可以交互參照內容資料以產生精緻化的政策。作為威脅緩解政策的一部分，您還可以識別和封鎖已知或有風險的檔案類型和 IP 位址，其中有幾個預製類別可用，包括指定防彈服務提供者和已知惡意 IP 的清單。如果使用專用工具和軟體，您可以建立您自己的漏洞特徵碼，以根據網路的獨特要求自訂入侵防禦功能。

為了盡可能進行威脅防護，Palo Alto Network 除了進階 | Threat Prevention 外還推薦以下訂閱服務：

- **DNS Security**—DNS Security 雲端服務，旨在保護您的組織免受基於 DNS 的進階威脅。透過將進階機器學習和預測分析套用於各種威脅情報來源，DNS Security 可產生增強型 DNS 特徵碼集，並可以即時分析 DNS 要求，以保護您的網路免受新產生的惡意網域的侵害。DNS Security 可以偵測各種 C2 威脅，包括 DNS 通道、DNS 重新繫結攻擊、使用自動產生建立的網域、惡意軟體主機等等。DNS Security 需要您的進階 Threat Prevention 或 Threat Prevention 訂閱并與之協同工作，以全面覆蓋各種 DNS 威脅。

Palo Alto Networks 的各種入侵防禦訂閱協同工作，以提供全面的解決方案，在攻擊過程的各個階段攔截和破壞鏈，並提供可見度，以防止網路基礎結構上的安全性遭到破壞。

進階 Threat Prevention 偵測服務

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

進階 Threat Prevention 是一種入侵防禦系統 (IPS) 解決方案，可以使用多層防禦系統（其元件在防火牆和雲端中運作）來偵測和封鎖所有連接埠和通訊協定中的惡意軟體、弱點利用以及命令與控制 (C2)。Threat Prevention 雲端使用來自 Palo Alto Networks 服務的合併威脅資料來執行大量偵測服務，以建立特徵碼，每個特徵碼都處理特定的可識別模式，並在偵測到相符的威脅和惡意行為時由防火牆用於執行安全政策。這些特徵碼根據威脅類型進行分類，並指派有唯一的識別碼。為了偵測與這些特徵碼對應的威脅，防火牆會執行分析引擎，這些引擎會檢查表現出異常特徵的網路流量並對其進行分類。

除了以特徵碼為基礎的偵測機制之外，進階 Threat Prevention 還提供內嵌偵測系統，以防止未知和規避性 C2 威脅，包括透過 Empire 框架產生的威脅，以及命令注入和 SQL 注入弱點。進階 Threat Prevention 雲端執行可延伸的深度學習模型，這些模型在防火牆上應要求啟用內嵌分析功能，以分發防護，並防止零時差威脅進入網路。這允許您透過使用內嵌偵測器的即時流量檢查來防止未知威脅。進階 Threat Prevention 雲端中的這些基於深度學習、機器學習的偵測引擎會分析流量是否存在運用 SQL 注入和命令注入的未知 C2 及弱點，以避免零時差威脅。為了提供威脅脈絡和全面的偵測詳細資料，系統會產生報告，其中包括攻擊者使用的工具/技術、偵測範圍和影響，以及 MITRE ATT&CK® 架構定義的相應網路攻擊分類。

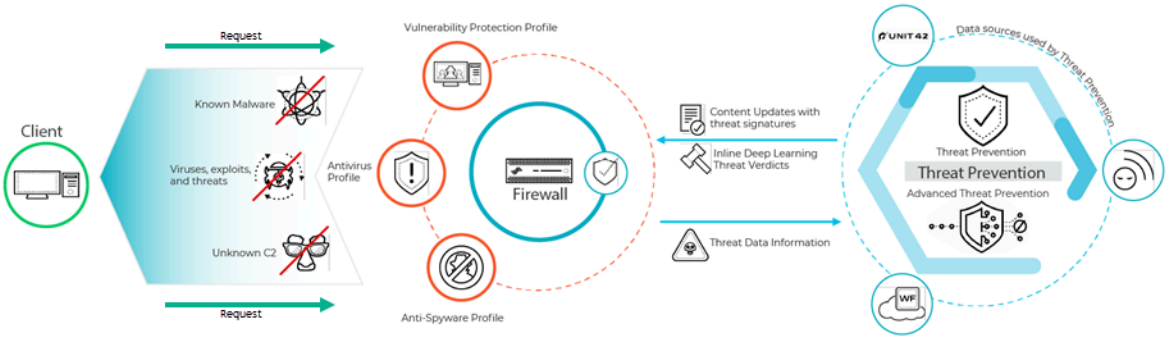
MITRE ATT&CK® 是針對網路攻擊者行為策劃的知識庫和模型。本工作經 *MITRE Corporation* 許可重製和分發。*MITRE Corporation (MITRE)* 特此授予您一個非獨有的免版稅授權，以將 *ATT&CK®* 用於研究、開發和商業用途。您為此類用途製作的任何副本均獲授權，前提是您在任何此類副本中重製 *MITRE* 的版權指定和本授權。

透過執行基於雲端的偵測引擎，您可以存取各種自動更新和部署的偵測機制，而無需使用者下載內容套件或執行會消耗資源的程序密集型、基於防火牆的分析器。使用 WildFire 的 C2 流量資料集持續監控和更新基於雲端的偵測引擎邏輯，並得到 Palo Alto Networks 威脅研究人員的額外支援（這些研究人員為高度準確的偵測增強提供人工干預）。進階 Threat Prevention 深度學習引擎支援透過 HTTP、HTTP2、SSL、未知 UDP 和未知 TCP 應用程式分析基於 C2 的威脅。其他分析模型透過內容更新提供，但是，對現有模型的增強是作為雲端更新執行的，不需要防火牆更新。

進階 Threat Prevention 還支援本機深度學習，提供機制來執行快速、以本機深度學習為基礎的零時差和其他避險性威脅分析，作為進階 Threat Prevention 內嵌雲端分析元件的補充功能。與 Palo Alto Networks 發佈特徵碼集相符的已知惡意流量會被刪除（或套用其他使用者定義的動作）；不過，符合可疑內容條件的某些流量會重新路由，使用深度學習分析偵測模組進行分析。如果需要進

一步分析，流量會傳送到進階 Threat Prevention 雲端進行其他分析，以及必要的假陽性和假陰性檢查。深度學習偵測模組是以在進階 Threat Prevention 雲端中運作的已驗證偵測模組為根據，因此具有相同的零時差和進階威脅偵測功能。此外，還具有處理較高流量的附加優勢，而且不會產生與雲端查詢相關聯的延遲。這使您可以在更短的時間內，檢查更多流量並接收裁定。在因應具有挑戰性的網絡條件時，這特別有幫助。

Palo Alto Networks 還提供「威脅防護」訂閱，該訂閱不包含雲端進階 *Threat Prevention* 授權中的功能。



防火牆使用的威脅特徵碼大致分為三種類型：防毒、反間諜軟體和弱點，並由相應的安全設定檔用於執行使用者定義的政策。

Palo Alto Networks 雲端交付的安全服務還為各自的服務產生 *WildFire* 和 *DNS C2* 特徵碼，以及檔案格式特徵碼，這些特徵碼可以指定檔案類型來代替威脅特徵碼；例如，作為特徵碼例外。

- 防毒特徵碼可偵測各種類型的惡意軟體和病毒，包括蠕蟲、特洛伊木馬程式和間諜軟體下載。
- 反間諜軟體特徵碼可偵測受感染主機上的 C2 間諜軟體，使其無法嘗試將呼叫總部或信標傳輸到外部 C2 伺服器。
- 漏洞特徵碼可偵測利用系統漏洞。

特徵碼具有預設嚴重程度等級，並具有相關的預設動作；例如，在高度惡意威脅的情況下，預設動作為「重設兩者」。此設定基於 Palo Alto Networks 的安全建議。

在存在專用內部應用程式或使用開放原始碼 Snort 和 suricata 規則的協力廠商情報摘要的部署中，可以建立自訂特徵碼以實現專門建置的保護。

防火牆以兩個更新套件的形式接收特徵碼更新：每日防毒內容和每週應用程式和威脅內容更新。防毒內容更新包括防毒和反間諜軟體安全性設定檔分別使用的防毒特徵碼和 DNS (C2) 特徵碼。應用程式和威脅的內容更新包括弱點與反間諜軟體安全性設定檔分別使用的弱點和反間諜軟體特徵碼。更新套件還包括由其他服務和子功能利用的其他內容。如需詳細資訊，請參閱動態內容更新。

威脅特徵碼類別

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

有三種類型的 Palo Alto Networks 威脅特徵碼，在掃描網路流量時，每種用於偵測不同類型的威脅：

- 防毒特徵碼—偵測在執行檔和檔案類型中發現的病毒和惡意軟體。
- 反間諜軟體特徵碼—偵測命令和控制 (C2) 活動，即受感染用戶端上的間諜軟體在未經使用者同意的情況下收集資料和/或與遠端攻擊者通訊。
- 漏洞特徵碼—偵測攻擊者可能試圖利用的系統缺陷。

特徵碼的嚴重程度指示所偵測事件的風險，特徵碼的預設動作（例如，封鎖或警示）為 Palo Alto Networks 建議您強制執行相符流量的方式。

您必須設定防毒、反間諜軟體及漏洞保護，以定義在偵測到威脅時要採取的動作，並且您可以根據 Palo Alto Networks 建議輕鬆使用預設安全性設定檔來開始封鎖威脅。對於每個特徵碼類型、類別，甚至特定特徵碼，您都可繼續修改或新建設定檔，以更細微地強制執行潛在威脅。

下表按下列類型列出了所有可能的特徵碼類別：防毒、間諜軟體和漏洞，並包含了用於在每個類別中提供特徵碼的內容更新（應用程式與威脅、防毒或 WildFire）。您還可以移至 Palo Alto Networks Threat Vault 以進一步瞭解威脅特徵碼。

威脅類別	提供這些特徵碼的內容更新	說明
防毒特徵碼		
apk	防毒軟體 WildFire	惡意的 Android 應用程式 (APK) 檔案。
MacOSX	防毒軟體 WildFire	惡意 MacOSX 檔案，包括： • Apple 磁碟映像 (DMG) 檔案。 • Mach 物件檔案 (Mach-O)，包括執行檔、程式庫以及物件程式碼。

威脅類別	提供這些特徵碼的內容更新	說明
		• Apple 軟體安裝程式套件 (PKG)
flash	防毒軟體 Wildfire 或 WildFire Private	網頁中內嵌的 Adobe Flash applet 和 Flash 內容。
jar	防毒軟體 Wildfire	Java Applet（JAR/Class 檔案類型）。
ms-office	防毒軟體 Wildfire 或 WildFire Private	Microsoft Office 檔案，包括文件（DOC、DOCX、RTF）、活頁簿（XLS、XLSX）及 PowerPoint 簡報（PPT、PPTX）。這還包括 Office Open XML (OOXML) 2007+ 文件。
pdf	防毒軟體 Wildfire 或 WildFire Private	可攜式文件格式 (PDF) 檔案。
pe	防毒軟體 Wildfire 或 WildFire Private	可攜式執行檔 (PE) 檔案可自動執行於 Microsoft Windows 系統，並僅在獲得授權時允許。這些檔案類型包括： • 物件程式碼。 • 字型 (FON)。 • 系統檔案 (SYS)。 • 驅動程式檔案 (DRV)。 • Windows 控制台項目 (CPL)。 • DLL（動態連結程式庫）。 • OCX（適用於 OLE 自訂控制或 ActiveX 控制的程式庫）。 • Windows 螢幕保護程式檔案 (SCR)。 • 可延伸韌體介面 (EFI) 檔案，可執行於作業系統和韌體之間，便於更新裝置和執行啟動作業。 • 程式資訊檔案 (PIF)。
linux	防毒軟體 Wildfire	可執行和可連結格式 (ELF) 檔案。
archive	防毒軟體	Roshal Archive (RAR) 和 7-Zip (7z) 歸檔檔案。

威脅類別	提供這些特徵碼的內容更新	說明
	Wildfire	
間諜軟體特徵碼		
廣告軟體	應用程式與威脅	偵測顯示可能不需要的廣告的程式。某些廣告軟體修改瀏覽器以強調顯示網頁上最常搜尋的關鍵字並對其設定超連結 - 這些連結將使用者重新導向至廣告網站。廣告軟體還可以從命令和控制 (C2) 伺服器擷取更新，並將這些更新安裝到瀏覽器或用戶端系統中。 這一類別中最新發佈的保護措施很少見。
autogen	防毒軟體	這些基於有效負載的特徵碼用於偵測命令和控制 (C2) 流量，並會自動產生。重要的是，即使 C2 主機未知或快速變更，自動產生的特徵碼也可以偵測 C2 流量。
後門	應用程式與威脅	偵測允許攻擊者未經授權而遠端存取系統的程式。
殭屍網路	應用程式與威脅	指示僵屍網路活動。殭屍網路是指攻擊者控制之受惡意軟體感染的電腦（「bot」）的網路。攻擊者可以集中對殭屍網路中的每台電腦發出命令，以同時執行協同動作（例如，啟動 DoS 攻擊）。
browser-hijack	應用程式與威脅	偵測正在修改瀏覽器設定的外掛程式或軟體。瀏覽器駭客可能會接管自動搜尋或追蹤使用者的 Web 活動，並將此資訊傳送到 C2 伺服器。 這一類別中最新發佈的保護措施很少見。
cryptominer	應用程式與威脅	（有時稱為 cryptojacking 或「挖礦軟體」）偵測由設計用於使用計算資源在使用者不知道的情況下挖掘加密貨幣的惡意程式產生的下載嘗試或網路流量。Cryptominer 二進位檔通常由 shell 指令碼下載程式傳遞，試圖確定系統架構並終止系統上的其他挖礦軟體程序。一些挖礦軟體在其他程序中執行，例如，呈現惡意網頁的 Web 瀏覽器。
data-theft	應用程式與威脅	偵測將資訊傳送給已知 C2 伺服器的系統。 這一類別中最新發佈的保護措施很少見。
dns	防毒軟體	偵測連線至惡意網域的 DNS 要求。 DNS 和 dns-wildfire 特徵碼用於偵測相同的惡意網域；然而，DNS 特徵碼包含在每日的防毒內容更新中，而

威脅類別	提供這些特徵碼的內容更新	說明
		dns-wildfire 特徵碼包含在每 5 分鐘發佈一次保護的 WildFire 更新中。
dns-security	防毒軟體	偵測連線至惡意網域的 DNS 要求。 除 DNS 安全性服務產生的唯一特徵碼之外，dns-security 還包含來自 dns 和 dns-wildfire 的特徵碼。
dns-wildfire	Wildfire 或 WildFire Private	偵測連線至惡意網域的 DNS 要求。 DNS 和 dns-wildfire 特徵碼用於偵測相同的惡意網域；然而，DNS 特徵碼包含在每日的防毒內容更新中，而 dns-wildfire 特徵碼包含在每 5 分鐘發佈一次保護的 WildFire 更新中。
下載程式	應用程式與威脅	（也稱為病毒植入程式、傳輸器載荷或載入程式）偵測使用網際網路連線來連線到遠端伺服器以在遭入侵系統上下載並執行惡意軟體的程式。最常見的使用案例是將下載程式部署為網路攻擊第一階段的最高點，其中下載程式擷取的裝載執行被視為第二階段。Shell 指令碼（Bash、PowerShell 等）、特洛伊木馬和惡意誘餌文件（也稱為 maldocs）（例如 PDF 和 Word 檔案）是常見的下載程式類型。
詐騙	應用程式與威脅	（包括 form-jacking、網路釣魚和詐騙）偵測對確定為註入惡意 JavaScript 代碼以從電子商務網站結帳頁面上擷取的付款表單收集敏感使用者資訊（如姓名、地址、電子郵件、信用卡號、CVV、到期日期）的遭入侵網站的存取。
駭客工具	應用程式與威脅	偵測由一些軟體工具產生的流量，這些軟體工具被惡意行為者用來進行偵查、攻擊或存取易受攻擊的系統，外洩資料，或建立命令和控制通道來未經授權暗中控制電腦系統。這些程式與惡意軟體和網路攻擊密切相關。駭客工具可能會在 Red Team 和 Blue Team 運營、滲透測試和研發中使用時以良性方式進行部署。無論意圖如何，在某些國家/地區使用或擁有這些工具可能是非法的。
鍵盤記錄木馬程式	應用程式與威脅	透過記錄按鍵和擷取螢幕畫面，偵測允許攻擊者秘密追蹤使用者活動的程式。 鍵盤記錄木馬程式使用各種 C2 方法，定期將日誌和報告傳送給預先定義的電子郵件地址或 C2 伺服器。透過鍵盤記錄木馬程式監控，攻擊者可以擷取允許網路存取的認證。

威脅類別	提供這些特徵碼的內容更新	說明
網路蠕蟲	應用程式與威脅	偵測用於自我複制並在系統間進行傳播的程式。網路蠕蟲可能會使用共用資源或利用安全性故障來存取目標系統。
phishing-kit	應用程式與威脅	當使用者嘗試連線至網路釣魚套件登入頁面時（可能在收到含有惡意網址連結的電子郵件后）進行偵測。網路釣魚網站誘使使用者提交攻擊者可以竊取的認證，以獲取對網路的存取權限。 除了封鎖對網路釣魚套件登入頁面的存取權限之外，還請啟用多因素驗證以及認證網路釣魚防禦，以防在所有階段中發生網路釣魚攻擊。
後攻擊	應用程式與威脅	偵測指示攻擊之後攻擊階段的活動，即攻擊者試圖評估遭入侵系統的價值。這可能包括評估儲存在系統上的資料的敏感性，以及系統在進一步危及網路方面的實用性。
webshell	應用程式與威脅	偵測 Web Shell 和 Web Shell 流量，包括植入內容偵測以及命令和控制互動。Web Shell 首先必須由惡意行為者植入遭入侵的主機上，通常是針對 Web 伺服器或架構。隨後與 Web Shell 檔案的頻繁通訊可讓惡意行為者能夠在系統中建立立足點，並在 Web 伺服器使用者的上下文中列舉服務和網路、外洩資料及執行遠端代碼。最常見的 Web Shell 類型有 PHP、.NET 和 Perl 標記指令碼。攻擊者還可以利用感染了 Web Shell 的 Web 伺服器（Web 伺服器可以是面向網際網路的系統，也可以是內部系統）來攻擊其他內部系統。
間諜軟體	應用程式與威脅	偵測輸出 C2 通訊。這些特徵碼可自動產生，也可以由 Palo Alto Networks 研究人員手動建立。 間諜軟體和自動產生的特徵碼均偵測到輸出 *C2* 通訊；然而，自動產生的特徵碼以有效負載為基礎，可以唯一地偵測與未知或快速變更之 *C2* 主機的 *C2* 通訊。
弱點特徵碼		
暴力密碼破解	應用程式與威脅	暴力密碼破解特徵碼偵測在特定時間範圍內多次出現的情況。雖然隔離的活動可能為良性，但暴力密碼破解特徵碼表明活動發生的頻率和速率比較可疑。例如，單一 FTP 登入失敗並不表示惡意活動。然而，短時間內多次

威脅類別	提供這些特徵碼的內容更新	說明
		失敗的 FTP 登入則有可能表示攻擊者試圖使用密碼組合存取 FTP 伺服器。 對於暴力密碼破解特徵碼，您可以 調整動作和觸發條件。
指令碼執行	應用程式與威脅	偵測程式碼執行漏洞，攻擊者可用該漏洞在具有已登入使用者權限的系統上執行程式碼。
程式碼混淆	應用程式與威脅	偵測已轉換為隱藏某些資料同時保留其功能的程式碼。混淆的程式碼很難或不可能被讀取，因此不清楚程式碼正在執行哪些命令或者與其交互的程式。最常見的是，惡意行為者會混淆程式碼來隱藏惡意軟體。更為罕見的是，合法開發人員可能會混淆程式碼以保護隱私權、智慧財產權或改進使用者體驗。例如，某些類型的混淆（如縮小）會減小檔案大小，從而減少網站載入時間和頻寬使用。
dos	應用程式與威脅	偵測拒絕服務 (DoS) 攻擊，即攻擊者試圖使目標系統不可用，暫時中斷系統和相關的應用程式和服務。要執行 DoS 攻擊，攻擊者可能會使目標系統爆流或傳送導致其失敗的資訊。DoS 攻擊剝奪了合法使用者（如員工、成員和帳戶持有者）預期存取的服務或資源。
exploit-kit	應用程式與威脅	偵測漏洞攻擊套件登入頁面。漏洞攻擊套件登入頁面通常包含多個漏洞，並針對多個瀏覽器和外掛程式中的一個或多個通用漏洞和風險披露 (CVE)。由於目標 CVE 快速變更，exploit-kit 特徵碼會根據漏洞攻擊套件登入頁面（而不是 CVE）觸發。 當使用者造訪帶有漏洞攻擊套件的網站時，漏洞攻擊套件會掃描目標 CVE 並試圖以無訊息方式將惡意有效負載傳送到受害者的電腦。
info-leak	應用程式與威脅	偵測軟體漏洞，攻擊者可以利用該漏洞竊取敏感資訊或專有資訊。通常，可能存在資訊洩漏，因為不存在用來保護資料的全面檢查，並且攻擊者可以透過傳送設計的要求來利用資訊洩漏。
insecure-credentials	應用程式與威脅	偵測為軟體、網路設備和 IoT 裝置使用弱密碼、遭入侵密碼和製造商預設密碼的情況。
溢位	應用程式與威脅	偵測溢位漏洞，即攻擊者可能會利用對要求缺乏適當檢查的情況。成功發起攻擊，可能會導致使用應用程式、伺服器或作業系統的權限遠端執行程式碼。

威脅類別	提供這些特徵碼的內容更新	說明
網路釣魚	應用程式與威脅	當使用者嘗試連線至網路釣魚套件登入頁面時（可能在收到含有惡意網址連結的電子郵件后）進行偵測。網路釣魚網站誘使使用者提交攻擊者可以竊取的認證，以獲取對網路的存取權限。 除了封鎖對網路釣魚套件登入頁面的存取權限之外，還請啟用多因素驗證以及認證網路釣魚防禦，以防在所有階段中發生網路釣魚攻擊。
通訊協定異常	應用程式與威脅	偵測通訊協定異常，即通訊協定行為偏離標準和符合規定的使用。例如，錯誤封包、編寫品質較差的應用程式或在非標準連接埠上執行的應用程式都將被視為通訊協定異常，可能被用作規避工具。最佳做法是封鎖任何嚴重程度的通訊協定異常。
sql-injection	應用程式與威脅	偵測常見的駭客入侵技術，即攻擊者將 SQL 查詢插入應用程式的要求中，以便讀取或修改資料庫。此類技術通常用於未全面清理使用者輸入的網站。

保護網路發生 Layer 4 與 Layer 7 規避攻擊的最佳做法

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

為了監控網路並防止發生大多數的 Layer 4 與 Layer 7 攻擊，以下是一些建議。

- ❑ 升級至最新版的 PAN-OS 軟體與內容更新版本，以確保您有最新的安全性更新。請參閱安裝內容及軟體更新。
- ❑ 啟用 DNS 安全性（需要 Threat Prevention 和 DNS 安全性訂閱授權）以對惡意 DNS 要求執行 sinkhole 作業。Palo Alto Networks 建議在您的反間諜軟體設定檔中使用以下 DNS 安全性類別組態設定：

SIGNATURE SOURCE	LOG SEVERITY	POLICY ACTION	PACKET CAPTURE
: Palo Alto Networks Content			
default-paloalto-dns		sinkhole	extended-capture
: DNS Security			
Command and Control Domains	default (high)	sinkhole	extended-capture
Dynamic DNS Hosted Domains	default (informational)	sinkhole	disable
Grayware Domains	default (low)	sinkhole	disable
Malware Domains	default (medium)	sinkhole	disable
Parked Domains	default (informational)	sinkhole	disable
Phishing Domains	default (low)	sinkhole	disable
Proxy Avoidance and Anonymizers	default (low)	sinkhole	disable
Newly Registered Domains	default (informational)	sinkhole	disable

  - 對於日誌嚴重性設定，請使用預設設定：
  - 對於原則動作，將所有特徵碼來源設定為 **sinkhole**。
  - 對於封包擷取，將命令和控制網域設定為延伸擷取。將所有其他類別保留為預設設定。

  如需與反間諜軟體設定相關的更多資訊，請參閱最佳做法網際網路閘道反間諜軟體設定檔。
- ❑ 如果您有作用中的進階威脅防護訂閱，請啟用 內嵌雲端分析和本機深度學習（如果可用），以即時封鎖進階 C2 和間諜軟體威脅。每個分析引擎的預設動作都是 **alert**（警示），當偵測到對應的威脅時，會產生威脅日誌；不過，Palo Alto Networks 建議將所有分析模型動作設定為 **Reset-Both**（重設兩者）。這會丟棄相符的封包並將 RST 傳送到用戶端和伺服器，中斷連線並產生威脅日誌項目。

- 設定防火牆以用作 DNS Proxy 並啟用規避特徵碼：

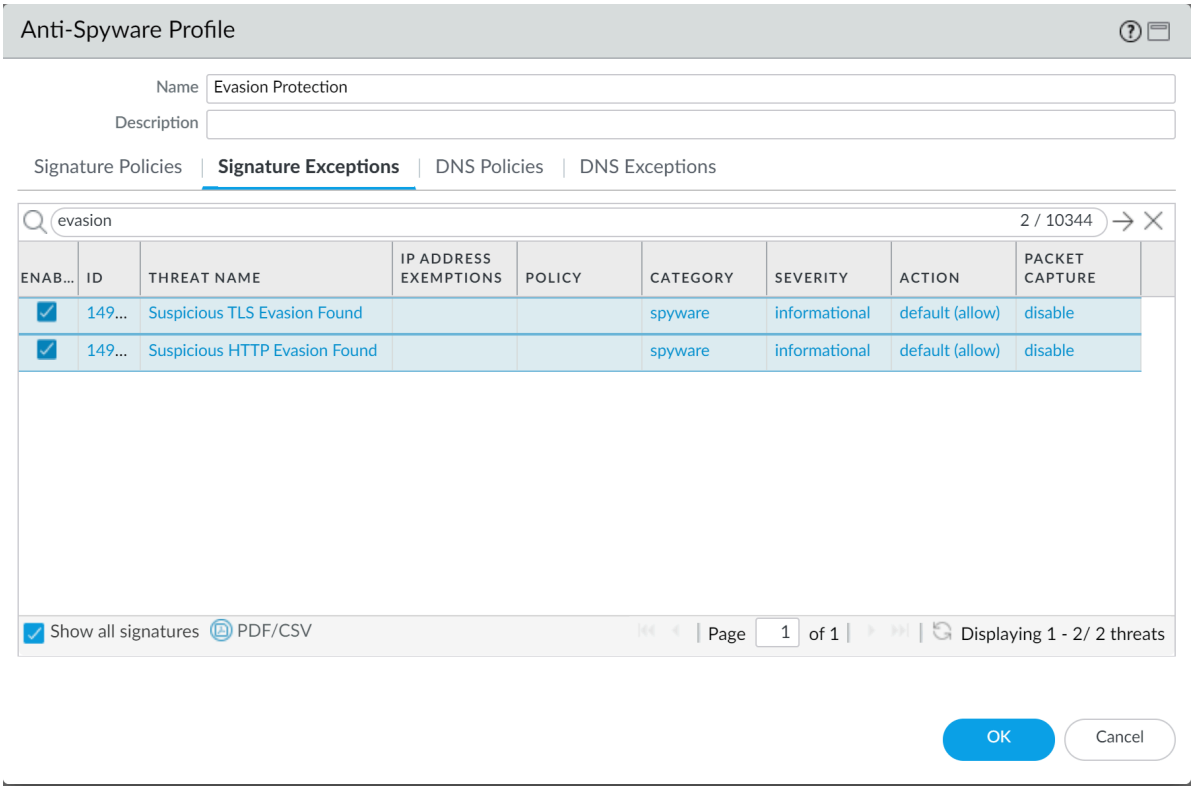
  DNS 代理程式不是防火牆安全性原則引擎的一部分；相反，它引導防火牆解析 *DNS* 主機名稱，同時保持網域到 *IP* 的對應，這對於防止 *TLS/HTTP* 迴避至關重要。

  - 設定 DNS Proxy 物件。

    當用作 DNS Proxy 時，防火牆會解析 DNS 要求並快取主機名稱至 IP 位址對應，以快速高效地解析未來的 DNS 查詢。

  - 啟用規避特徵碼

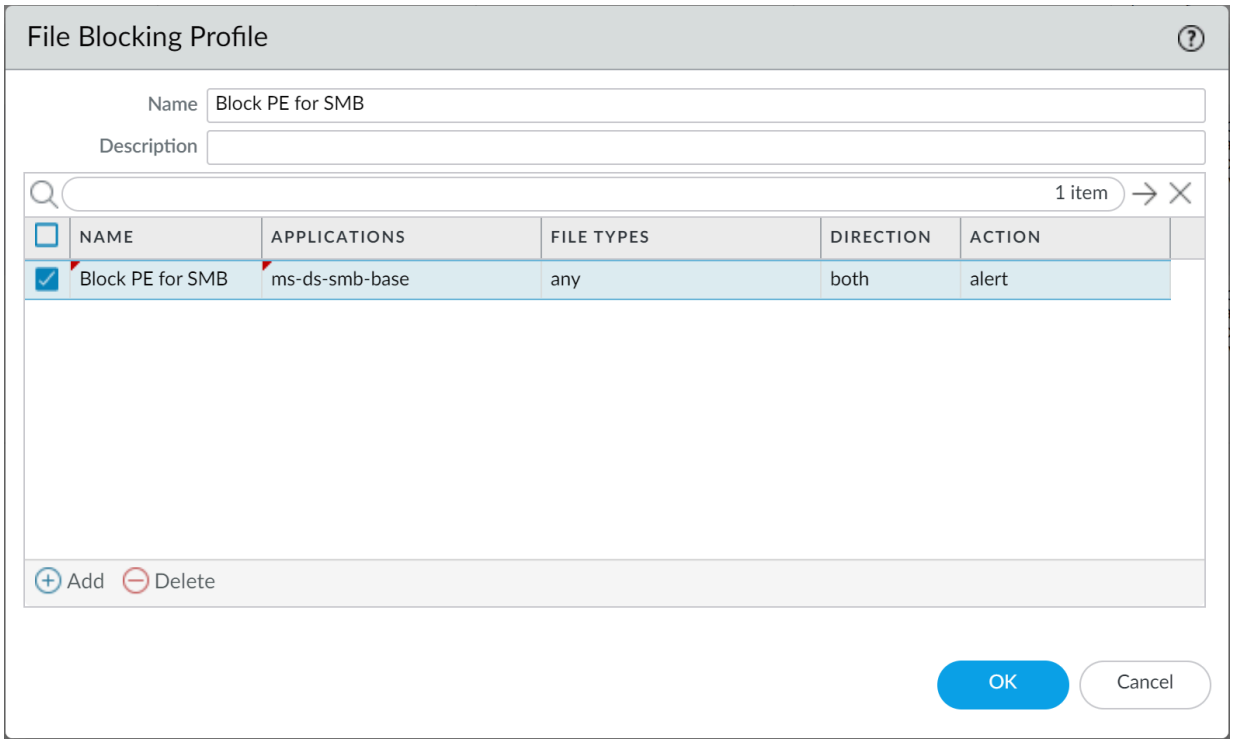
    偵測所建立之 HTTP 或 TLS 要求的規避特徵碼，可在用戶端連線至非原始 DNS 要求指定的網域時傳送警示。確保在啟用規避特徵碼之前設定 DNS Proxy。在不啟用 DNS Proxy 的情況下，規避特徵碼可在 DNS 負載平衡組態中的 DNS 伺服器向防火牆與用戶端傳回不同的 IP 位址（適用於裝載相同資源的伺服器）時觸發警示。



- 對於執行 Prisma Access 的部署或沒有內部 DNS 伺服器的網路，請將您的 DNS 政策設定為使用 Palo Alto Networks Sinkhole IP 位址 (72.5.65.111)，而不是預設的 Sinkhole FQDN (sinkhole.paloaltonetworks.com)。

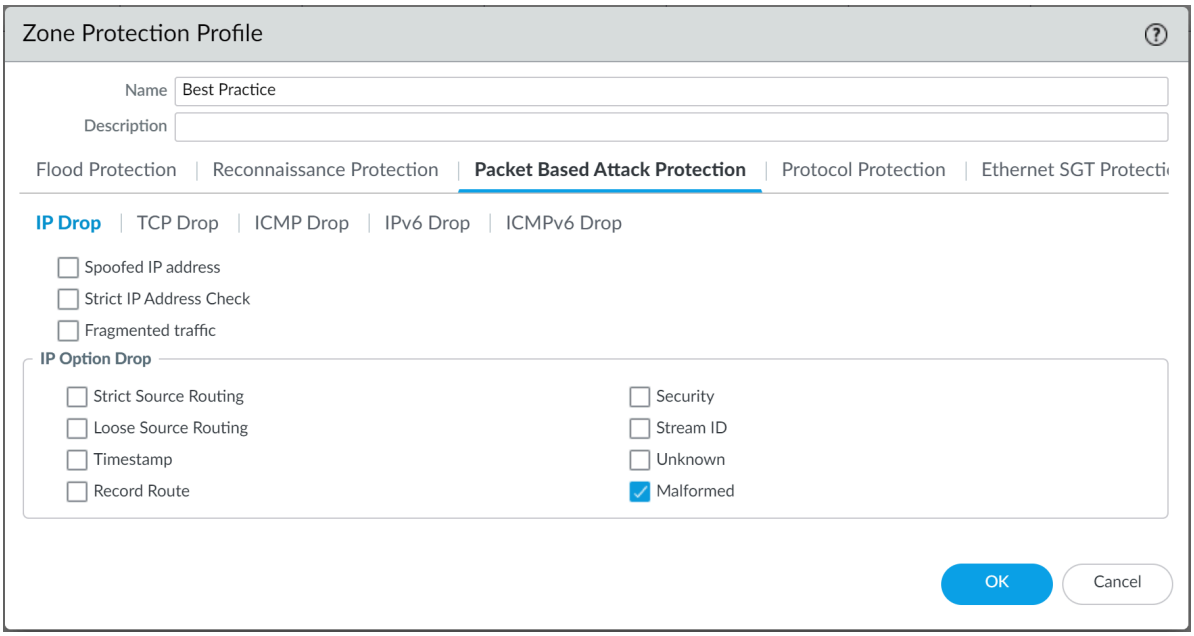
  反間諜軟體設定檔使用的 DNS Sinkhole 使防火牆能夠偽造針對以下網域的 DNS 查詢的回應，以協助識別受危害的主機：符合為指定的 Sinkhole 伺服器進行 Sinkhole 動作而設定的類別。使用預設的 Sinkhole FQDN 時，防火牆會將 CNAME 記錄作為回應傳送給用戶端，預期內部 DNS 伺服器將解析 CNAME 記錄，允許記錄從用戶端到已設定的 Sinkhole 伺服器的惡意通訊並容易識別。不過，如果用戶端正在執行 Prisma Access、位於沒有內部 DNS 服務器的網路中或正在使用無法將 CNAME 正確解析為 A 記錄回應的其他軟體或工具，則 DNS 要求會遭到捨棄，進而產生對於威脅分析而言至關重要的不完整流量日誌詳細資料。
- 對於伺服器，建立安全性原則規則以僅允許每個伺服器上認可的應用程式。確認應用程式的標準連接埠符合伺服器上的接聽連接埠。例如，為確保僅允許 SMTP 流量進入電子郵件伺服器，請將應用程式設為 **smtp** 並將服務設為 **application-default**（應用程式預設值）。若伺服器僅使用標準連接埠的一個子集（例如，如果在 SMTP 應用程式將標準連接埠定義為 25 和 587 時，SMTP 伺服器僅使用連接埠 587），則建立僅包括連接埠 587 的新自訂服務，並使用安全性原則規則中的新服務，而非使用應用程式預設值。此外，還需確保將存取權限制為特定來源和目的地區域和 IP 位址集。
- 使用安全性原則封鎖所有未知的應用程式和流量。一般而言，唯一會被歸類為未知流量的應用程式是您網路上的內部或自訂應用程式，以及潛在威脅。未知流量可能是異常的不相容應用程式或通訊協定，或是使用非標準連接埠的已知應用程式，這兩種都應封鎖。請參閱管理自訂或未知的應用程式。

- 設定檔案封鎖，用於封鎖網際網路式 SMB（伺服器訊息區塊）流量的可攜式執行檔 (PE) 檔案類型，使其無法從信任區域周遊至不信任區域（ms-ds-smb 應用程式）。



- 即時封鎖 PE（可攜式執行檔）、ELF 和 MS Office 檔案以及 PowerShell 和 Shell 指令碼的惡意變體。啟用 WildFire Inline ML 可讓您在防火牆上使用機器學習動態分析檔案。這層額外的防毒保護為基於 WildFire 的特徵碼提供了補充，從而將防護範圍覆蓋到尚不存在特徵碼的檔案。

- 建立並設定區域防護設定檔，令其防禦封包式攻擊（**Network**（網路） > **Network Profiles**（網路設定檔） > **Zone Protection**（區域防護））：
  - 選取此選項以丟棄 **Malformed**（格式錯誤的）IP 封包（**Packet Based Attack Protection**（基於封包的攻擊防護） > **IP Drop**（**TCP** 丟棄））。



  - 啟用丟棄 **Mismatched overlapping TCP segment**（不相符的重疊 **TCP** 區段） 選項（**Packet Based Attack Protection**（基於封包的攻擊防護） > **TCP Drop**（**TCP** 丟棄））。

    攻擊者會透過刻意建構重疊但資料不同的連線，嘗試造成錯誤解讀連線的意圖，並刻意引發誤判或漏報。攻擊者還會使用 IP 詐騙與序號預測方法來攔截使用者連線，並將自己的資料插入該連線。選取**Mismatched overlapping TCP segment**（不相符的重疊 **TCP** 區段），指定

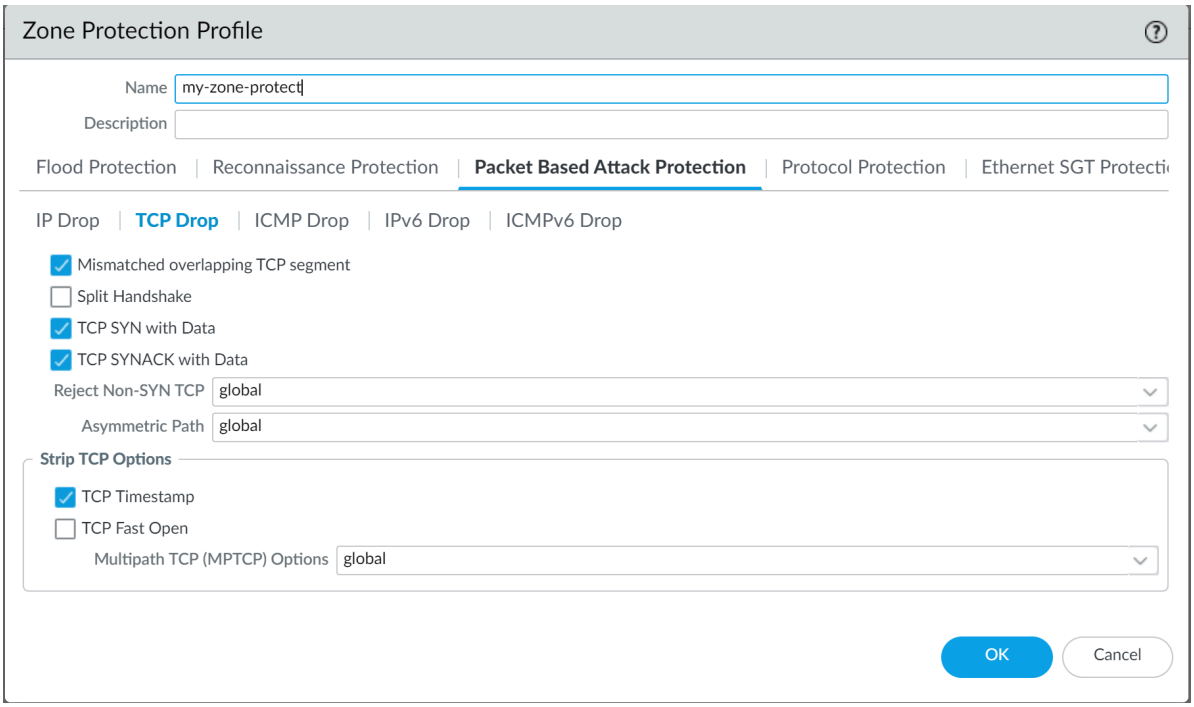
PAN-OS 丟棄具有不相符及重疊資料的框架。如果接收的區段包含在另一個區段內、與另一個區段部分重疊或者包含另一個完整區段，將會被丟棄。

- 啟用丟棄 **TCP SYN with Data**（帶資料的 **TCP SYN**）和丟棄 **TCP SYNACK with Data**（帶資料的 **TCP SYNACK**）選項（**Packet Based Attack Protection**（基於封包的攻擊防護） > **TCP Drop**（**TCP** 丟棄））。

  在三向交握時丟棄裝載中包含資料的 SYN 和 SYN-ACK 封包，可以封鎖裝載中包含的惡意軟體，防止其在完成 TCP 交握之前擷取未經授權資料，從而提升安全性。

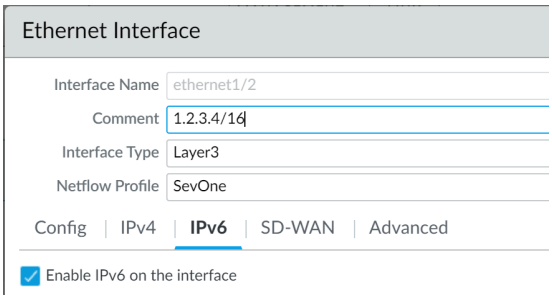
- 在防火牆轉送封包之前，將 TCP 時間戳記從 SYN 封包中剝離（**Packet Based Attack Protection**（基於封包的攻擊防護） > **TCP Drop**（**TCP** 丟棄））。

  當您選取 SYN 封包中的 **Strip TCP Options - TCP Timestamp**（剝離 **TCP** 選項 **- TCP** 時間戳記）選項時，TCP 連線兩端的 TCP 堆疊將不支援 TCP 時間戳記。這可以防禦在多個相同序號的封包上使用不同時間戳記的攻擊。

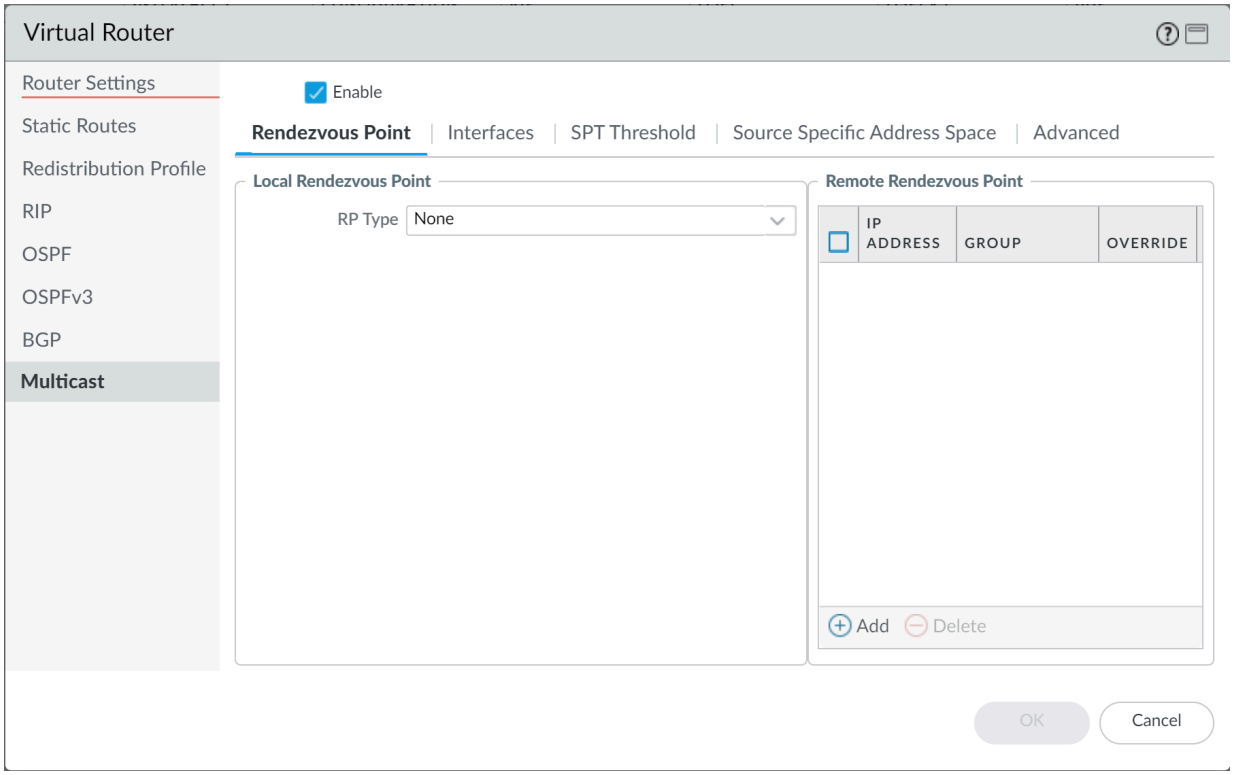


- 如果您在網路主機上設定 IPv6 位址，需確保支援 IPv6（若尚未啟用）（**Network**（網路） > **Interfaces**（介面） > **Ethernet**（乙太網路） > **IPv6**）。

  啟用對 IPv6 的支援將允許存取 IPv6 主機，還將篩選 IPv4 封包中封裝的 IPv6 封包，這可以防止 IPv6 over IPv4 多點傳送位址遭到網路偵察的利用。



- 允許支援多點傳送流量，讓防火牆可在多點傳送流量上執行原則（**Network**（網路） > **Virtual Router**（虛擬路由器） > **Multicast**（多點傳送））。



- 停用 **Forward datagrams exceeding UDP content inspection queue**（轉送資料包超過 **UDP** 內容檢驗佇列） 和 **Forward segments exceeding TCP content inspection queue**（轉送區段超

過 **TCP** 內容檢驗佇列）選項（**Device**（裝置） > **Setup**（設定） > **Content-ID** > **Content-ID Settings**（**Content-ID** 設定））。

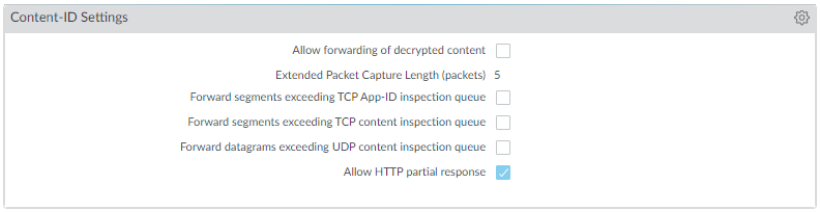
依預設，當 TCP 或 UDP 內容檢驗佇列已滿時，防火牆會跳過 TCP 區段或 UDP 資料包之超出 64 佇列限制的內容檢驗。停用此選項可確保對防火牆允許的所有 TCP 和 UDP 資料包執行內容檢驗。僅在特定情況下（例如，防火牆平台的大小不適當而無法與使用案例保持一致時），停用此設定才會影響效能。

- 停用 **Allow HTTP partial response**（允許 **HTTP** 部分回應）（**Device**（裝置） > **Setup**（設定） > **Content-ID** > **Content-ID Settings**（**Content-ID** 設定））。

  HTTP 部分回應選項允許用戶端僅擷取檔案的一部分。當轉送路徑中的下一代防火牆識別並丟棄惡意檔案時，它會終止帶有 RST 封包的 TCP 工作階段。若網頁瀏覽器實作 HTTP 標頭範圍選項，則可啟動新工作階段，以僅擷取檔案的剩餘部分，這可以防止防火牆因為缺少初始工作階段的內容而再次觸發相同特徵碼，同時還能允許網頁瀏覽器重新組合檔案並傳送惡意內容。停用此選項可防止發生此情況。

  依預設，在防火牆上啟用 Allow HTTP partial response（允許 HTTP 部分回應）。這提供了最大的可用性，但增加了網路攻擊成功的風險。為了取得最大的安全性，請停用此選項以防止網頁瀏覽器在防火牆因惡意活動而終止原始工作階段後，啟動新工作階段以擷取檔案的其餘部分。停用 HTTP 部分回應會影響使用 RANGE 標頭的基於 HTTP 的資料傳輸，這可能會導致某些應用程式的服務異常。停用 HTTP 部分回應後，驗證業務關鍵型應用程式的運作情況。

  如果業務關鍵型應用程式發生 HTTP 資料傳輸中斷，則可為該特定應用程式建立應用程式取代政策。由於應用程式取代會繞過 App-ID（包括威脅和內容檢查），請僅為特定的業務關鍵型應用程式建立應用程式取代政策，並指定來源和目的地以限制規則（最小特權存取原則）。除非必要，否則不要建立應用程式取代政策。如需應用程式取代政策的相關資訊，請參閱 https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClVLCA0。



- 建立弱點保護設定檔，封鎖通訊協定異常及所有高低嚴重性等級的弱點。

  在通訊協定行為偏離標準和合規用途時會出現通訊協定異常。例如，錯誤封包、編寫品質較差的應用程式或在非標準連接埠上執行的應用程式都將被視為通訊協定異常，可能被用作規避工具。

  如果您使用任務關鍵性網路，其中應用程式可用性的優先順序最高，則您應首先在一段時間內警示通訊協定異常，以確保沒有關鍵內部應用程式以非標準方式使用所建立的通訊協定。如果您發現某些關鍵應用程式觸發了通訊協定異常特徵碼，則您可以將這些應用程式從通訊協定異

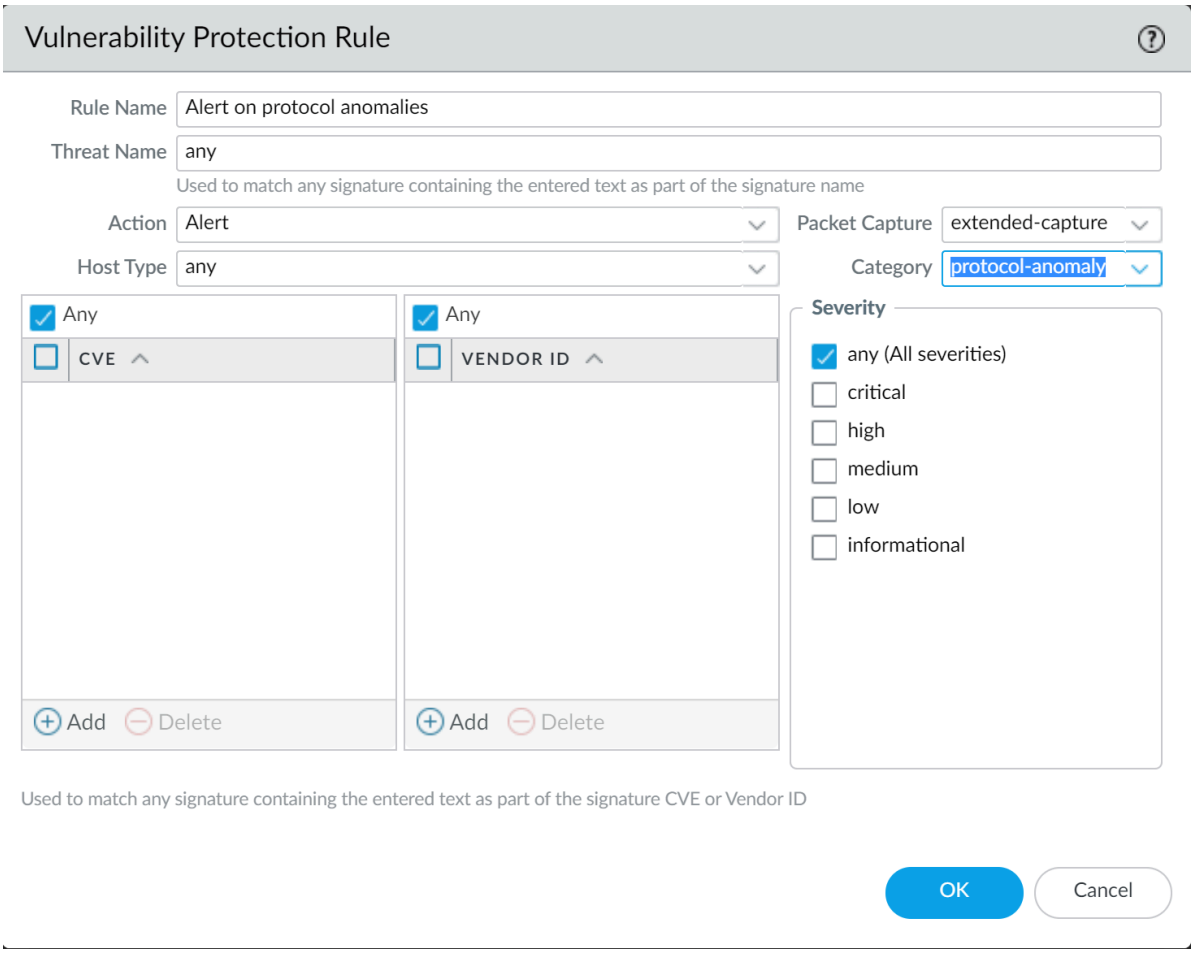
常執行。為此，在漏洞保護設定檔中新增另一個規則，允許通訊協定異常，再將該設定檔附加於對傳送自/至關鍵應用程式執行的安全性原則規則。

確保允許關鍵內部應用程式的通訊協定異常的漏洞保護設定檔規則和安全性原則規則列於封鎖通訊協定異常的規則之上。將對照安全性原則規則及相關漏洞保護設定檔規則，自上而下地評估流量，並根據第一項相符的規則執行。

- 首先針對通訊協定異常發出警示：

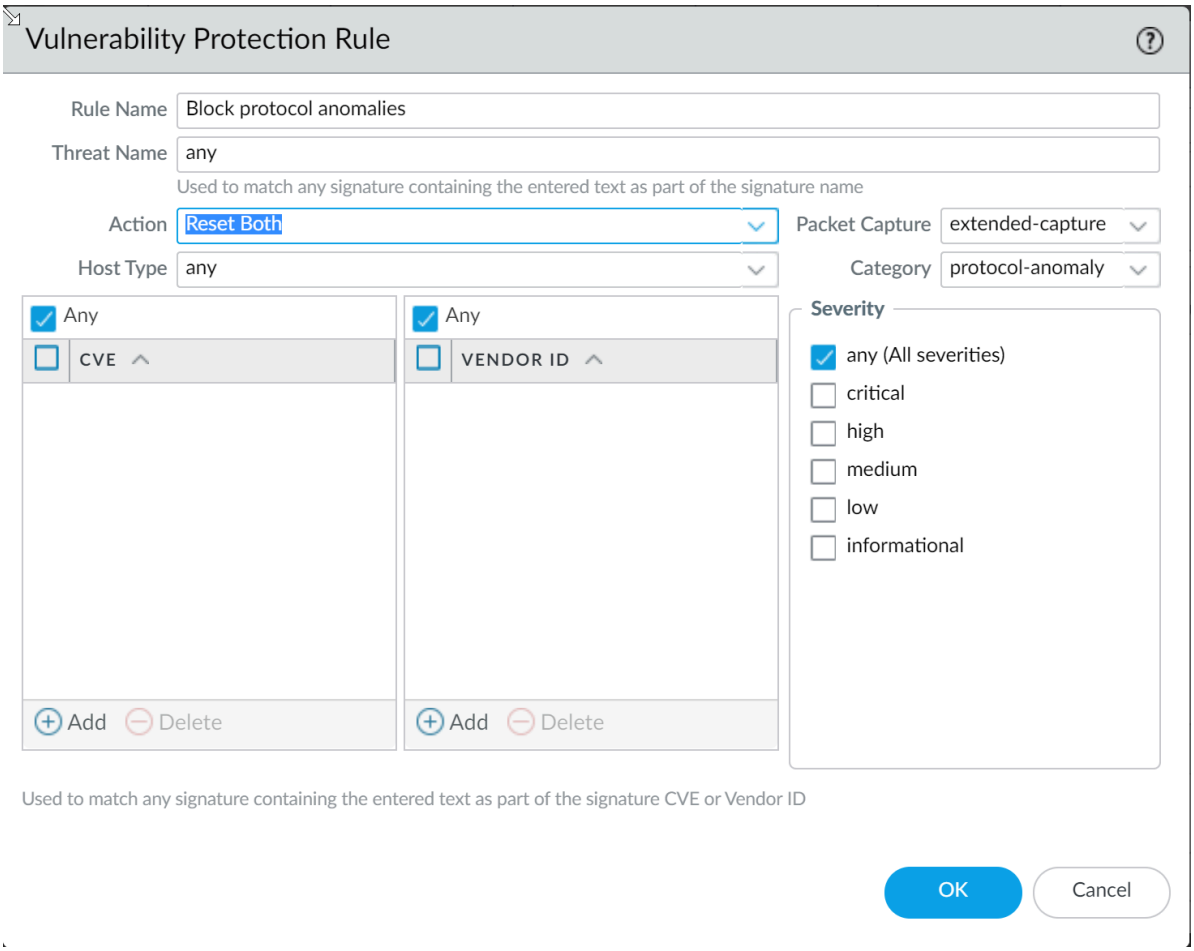
  建立漏洞保護設定檔規則，將 **Action**（動作）設定為 Alert（警示），**Category**（類別）設定為 protocol-anomaly（通訊協定異常），**Severity**（嚴重性）設定為 Any（任何）。監控流量，以確定是否有任何關鍵內部應用程式在以非標準方式使用所建立的通訊協定。若存在

這種情況，則繼續允許這些應用程式的通訊協定異常，然後封鎖所有其他應用程式的通訊協定異常。



- 封鎖通訊協定異常：

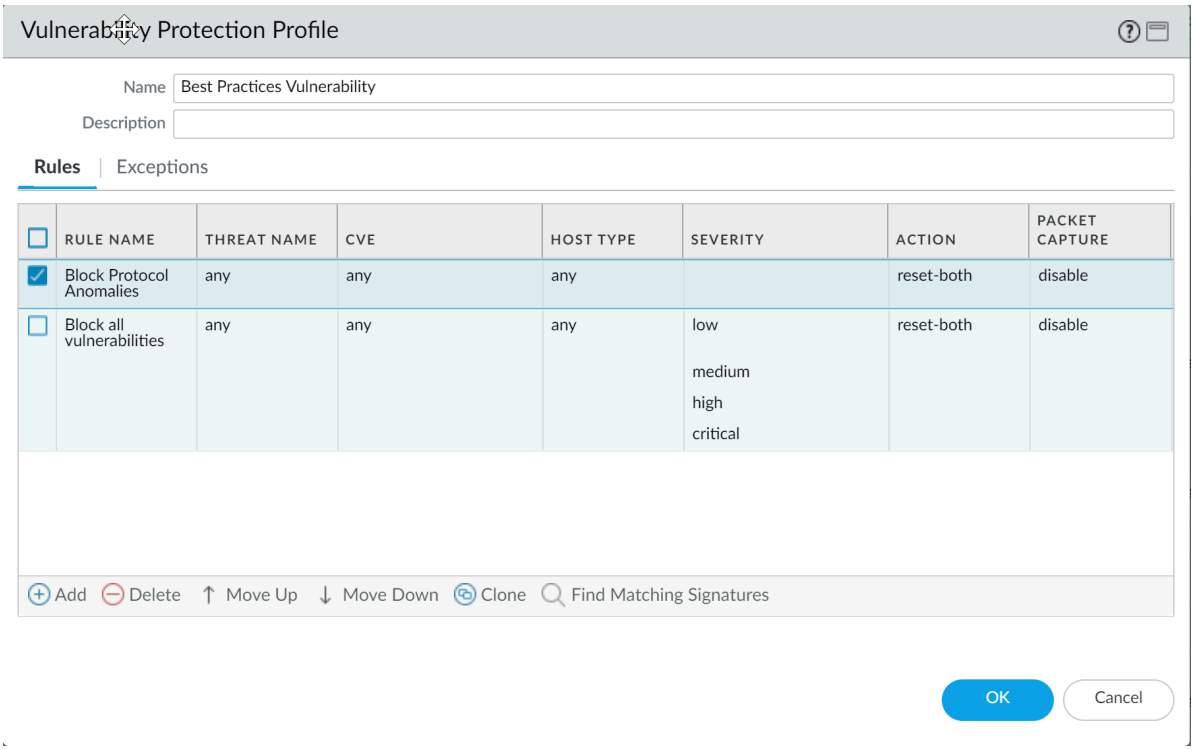
  建立漏洞保護設定檔規則，將 **Category**（類別）設定為 protocol-anomaly（通訊協定異常），規則 **Action**（動作）設定為 Reset Both（重設二者），**Severity**（嚴重性）設定為 Any（任何）。



- 可以允許以非標準方式使用所建立之通訊協定的關鍵應用程式的通訊協定異常。為此，建立漏洞保護設定檔規則，允許通訊協定異常：將 **Action**（動作）設定為 Allow（允許），**Category**（類別）設定為 protocol-anomaly（通訊協定異常），**Severity**（嚴重

性）設定為 Any（任何）。將漏洞保護設定檔規則附加於對傳送自/至關鍵應用程式執行的安全性原則規則。

- 向漏洞保護設定檔再新增一條規則，用於封鎖所有嚴重性層級為低及以上的漏洞。該規則必須列在用於封鎖通訊協定異常的規則之後。



- 繼續將下列安全性設定檔附加至安全性原則規則中，以提供特徵碼式保護：
  - 反間諜軟體設定檔，用於封鎖所有嚴重性層級為低及以上的間諜軟體。
  - 防毒軟體設定檔，用於封鎖所有符合防毒特徵碼的內容。

與 Palo Alto Networks 分享威脅情報

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

遙測是收集並傳輸資料以進行分析的程序。在防火牆上啟用遙測後，防火牆會定期收集並傳送資訊（包括應用程式、威脅和裝置健康狀態）到 Palo Alto Networks。分享威脅情報具有下列好處：

- 為您和全世界的其他用戶提供增強的漏洞及間諜軟體特徵碼。例如，當威脅事件觸發漏洞或間諜軟體特徵碼時，防火牆會將該威脅關聯的 URL 與 Palo Alto Networks 威脅研究團隊分享，以便他們能夠正確將這些 URL 分類為惡意。
- 快速測試和評估實驗性威脅特徵碼，而不影響您的網路，以便能夠更快地向所有 Palo Alto Networks 客戶發佈重要威脅防禦特徵碼。
- 改善 PAN-DB URL 篩選、DNS 型命令與控制項 (C2) 特徵碼及 WildFire 內部的準確性和惡意軟體偵測能力。

Palo Alto Networks 將使用從遙測裝置擷取的威脅情報，為您和其他 Palo Alto Networks 使用者提供這些福利。所有 Palo Alto Networks 使用者都能受益於每個使用者分享的遙測資料，讓遙測成為一種由社群驅動的威脅防禦方法。Palo Alto Networks 不會與其他客戶或第三方組織共用您的遙測資料。

若要閱讀有關遙測（包括其好處、使用方式和設定）的更多資訊，請參閱裝置遙測。

進階 Threat Prevention 資源

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

如需威脅防護最佳做法的更多資訊，請參閱下列資源：

- 建立自訂威脅特徵碼
- 保護網路發生 Layer 4 與 Layer 7 規避攻擊的最佳做法
- URL 篩選最佳做法
- 零信任的最佳做法
- DoS 和區域保護最佳做法

若要檢視 Palo Alto Networks 產品可識別的威脅及應用程式的清單，可使用下列連結：

- Applipedia—提供有關 Palo Alto Networks 可識別應用程式的詳細資訊。
- Threat Vault—列出 Palo Alto Networks 產品可識別的威脅。您可依漏洞、間諜軟體或病毒進行搜尋。按一下 ID 號碼旁的 (詳細資訊) 圖示就能瞭解有關威脅的詳細資訊。

設定 Threat Prevention

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

在啟用和設定內嵌雲端分析之前，您必須取得並安裝 Threat Prevention 或進階 Threat Prevention（以存取內嵌雲端分析功能）以及其運作的任何平台授權。授權是從 Palo Alto Networks 客戶支援入口網站啟動，且必須處於作用中狀態，才能啟用任何威脅防護功能。此外，Threat Prevention（類似於其他 Palo Alto Networks 安全性服務）是透過安全性設定檔進行管理的，而安全性設定檔又依賴透過安全性政策規則定義的網路強制執行政策設定。在啟用威脅防護之前，建議您先熟悉安全性訂閱已啟用的安全性平台核心元件。如需詳細資訊，請參閱產品文件。

若要啟用和設定威脅防護訂閱，以在網路安全性部署中發揮最佳功能，請參閱下列工作。雖然不一定要實作此處顯示的所有程序，但 Palo Alto Networks 建議檢閱所有工作，以熟悉成功部署的可用選項。此外，也建議您遵循 Palo Alto Networks 提供的最佳做法，以獲得最佳的可用性和安全性。

設定防毒、反間諜軟體及漏洞保護

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

每個 Palo Alto Networks 新世代防火牆皆隨附可附加至安全性原則規則的預先定義防毒、反間諜軟體和漏洞保護設定檔。有一個預先定義的防毒設定檔名為預設，它使用每個通訊協定的預設動作（封鎖 HTTP、FTP 與 SMB 流量，以及 SMTP、IMAP 及 POP3 流量上的動作）。有兩個預先定義的反間諜軟體與漏洞保護設定檔：

- 預設—將預設動作套用至用戶端與伺服器所有的重要、高與中等嚴重性間諜軟體/漏洞保護事件。它不會偵測低和資訊事件。
- 嚴格—將封鎖回應套用至所有用戶端與伺服器的重要、高與中等嚴重性間諜軟體/漏洞保護事件，並針對低和資訊事件使用預設動作。

若要確保進入網路的流量沒有威脅，請將預先定義的設定檔附加到您的基本 Web 存取原則。當您監控網路上的流量及展開原則規則庫時，您可以設計更精確的設定檔來因應特殊的安全性需求。

使用下列工作流程，設定預設防毒、反間諜軟體和漏洞保護安全性設定檔。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定防毒、反間諜軟體及弱點保護 (Cloud Management)

STEP 1 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager。

威脅防護訂閱搭售將防毒、反間諜軟體及弱點保護功能組合在同一授權中，而且是您 Prisma Access 訂閱的一部分。有關透過 Prisma Access 提供的應用程式和服務資訊，請參閱所有適用的應用程式和服務。若要驗證您目前擁有的作用中授權訂閱，請檢查您的授權支援哪些。

STEP 2 | （選用）為防毒、反間諜軟體和漏洞保護建立自訂安全性設定檔。

也可以使用預先定義的最佳做法設定檔。

安全轉換到最佳做法安全性設定檔，以確保最佳安全性。

- 若要建立自訂的 WildFire and Antivirus Profiles（WildFire 與防毒設定檔），請選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **WildFire and Antivirus**（**WildFire** 與防毒）以及 **Add Profile**（新增設定檔）。使用防毒設定檔轉換步驟，安全達成目標。
- 若要建立自訂的 Anti-Spyware Profiles（反間諜軟體設定檔），請選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Anti-Spyware**（反反間諜軟體）以及 **Add Profile**（新增設定檔）。使用反間碟軟體設定檔轉換步驟，安全達成目標。
- 若要建立自訂的 Vulnerability Protection Profiles（弱點保護設定檔），請選取**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Vulnerability Protection**（弱點保護）以及 **Add Profile**（新增設定檔）。使用漏洞保護設定檔轉換步驟，安全達成目標。

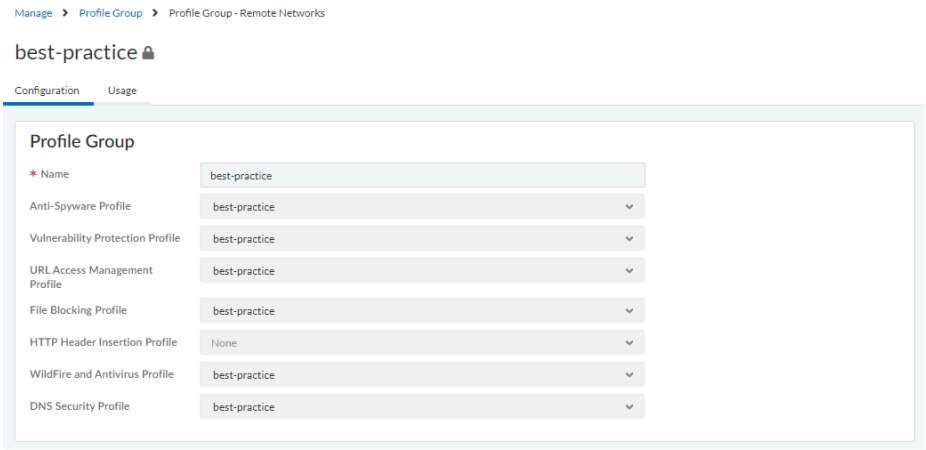
STEP 3 | 將安全性設定檔附加到您的 **Security Policy Rules**（安全性政策規則）。Prisma Access 預設會強制執行最佳做法安全性政策規則。

當您設定使用弱點保護設定檔的安全性政策規則，來在偵測到入侵或嘗試取得未經授權的存取時封鎖連線，*Prisma Access* 會自動封鎖該流量並記錄這些事件（請參閱 監控封鎖的 IP 位址）。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Security Policy**（安全性政策），並選取要修改的規則或 **Add Rule**（新增規則）。
2. 在 **Action and Advanced Inspection**（操作和進階檢查）中，選取 **Profile Group**（設定檔群組），其中包括以下安全性設定檔：**WildFire and Antivirus**（**WildFire** 和防毒）、**Anti-Spyware**（反間諜軟體）和 **Vulnerability Protection**（弱點保護）。

   您可以在 ***Manage***（管理） > ***Configuration***（設定） > ***NGFW and Prisma Access*** > ***Security Services***（安全服務） > ***Profile Groups***（設定檔群組）中建立新的設定檔群組。有關詳細資訊，請參閱啟用安全性設定檔。

   預設情況下，***best-practice***（最佳做法）設定檔群組會啟用所有可用安全性設定檔的最佳做法設定。



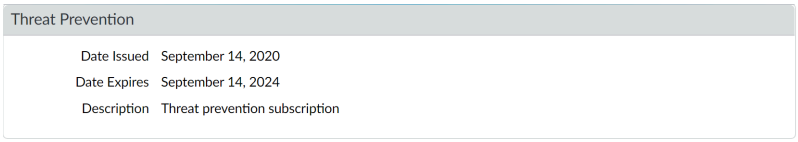
STEP 4 | Commit（提交）您的變更。

設定防毒、反間諜軟體及弱點保護 (NGFW (Managed by PAN-OS or Panorama))

Palo Alto Networks 針對所有反間諜軟體和漏洞保護定義了預設動作。若要檢視設定檔，可選取 ***Objects***（物件） > ***Security Profiles***（安全性設定檔） > ***Anti-Spyware***（反間諜軟體）或 ***Objects***（物件） > ***Security Profiles***（安全性設定檔） > ***Vulnerability Protection***（漏洞保護），然後選取設定檔。按一下 *Exceptions*（例外狀況）頁籤，然後按一下 *Show all signatures*（顯示所有特徵碼），即可檢視特徵碼清單和相應預設 ***Action***（動作）。若要變更預設動作，可建立新設定檔，指定 ***Action***（動作）及/或新增特徵碼例外到設定檔中的 ***Exceptions***（例外）。

STEP 1 | 確認您擁有 Threat Prevention（威脅防護）使用授權。

Threat Prevention（威脅防護）使用授權搭售將防毒、反間諜軟體及漏洞保護功能組合在同一授權中。若要確認您是否具備有效的 Threat Prevention（威脅防護）使用授權，可選取 **Device**（裝置） > **Licenses**（授權），然後確認 **Threat Prevention**（威脅防護）到期日期是否為未來日期。



STEP 2 | 下載最新的內容。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後按一下頁面底端的**Check Now**（立即檢查），擷取最新的特徵碼。
2. 在 **Actions**（動作）欄中，按一下 **Download**（下載），安裝最新的防毒更新，然後再下載並 **Install**（安裝）最新的應用程式和威脅更新。

STEP 3 | 排程內容更新。

有關部署更新的重要資訊，請參閱應用程式與威脅內容更新的最佳做法。

1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後按一下 **Schedule**（排程），以便為 **Antivirus**（防毒）及 **Applications and Threats**（應用程式和威脅）自動擷取特徵碼更新。
2. 指定更新頻率及時間：
   - 僅下載—防火牆將按您定義的排程自動下載最新更新，但您必須手動 **Install**（安裝）更新。
   - 下載並安裝—防火牆將按照您定義的排程自動下載並安裝更新。
3. 按一下 **OK**（確定）以儲存更新排程；無需提交。
4. （選用）定義一個 **Threshold**（臨界值），以指定防火牆將在可用更新出現至少多少小時之後再下載更新。例如，將 **Threshold**（臨界值）設定為 **10**，則表示無論排程設定為何，防火牆都將至少在 10 小時後再下載更新。
5. （僅限 HA）確定是否 **Sync To Peer**（同步到對等體），這將允許對等體在下載並安裝後同步內容更新（更新排程不會在各對等體之間同步；您必須在兩個對等體上手動設定排程）。

   關於確定是否以及如何 **Sync To Peer**（同步到對等體）的其他考量，視乎於您的 HA 部署：

   - 主動/被動 **HA** — 如果防火牆使用 MGT 連接埠進行內容更新，則排程單獨排程各防火牆下載並安裝更新。但是，如果防火牆使用資料連接埠進行內容更新，則被動防火牆在變為主動之前，將不會下載或安裝更新。若要在使用資料連接埠進行更新時，使兩個防火牆上的排程保持同步，則在兩個防火牆上排程更新，然後啟用 **Sync To Peer**（同步到對等體），以便讓主動防火牆下載並安裝更新，並將更新推送到被動防火牆。

- 主動/主動 **HA** — 如果防火牆使用 MGT 連接埠進行內容更新，則在兩個防火牆上選取 **download-and-install**（下載並安裝），但不啟用 **Sync To Peer**（同步到對等體）。但是，如果防火牆使用資料連接埠，則在兩個防火牆上選取 **download-and-install**（下載並安裝），並啟用 **Sync To Peer**（同步到對等體），以便當一個防火牆變為主動-次要狀態時，主動-主要防火牆將下載並安裝更新，並將更新推送主動-次要防火牆。

STEP 4 | （選用）為防毒、反間諜軟體和漏洞保護建立自訂安全性設定檔。

也可以使用預先定義的預設或嚴格設定檔。

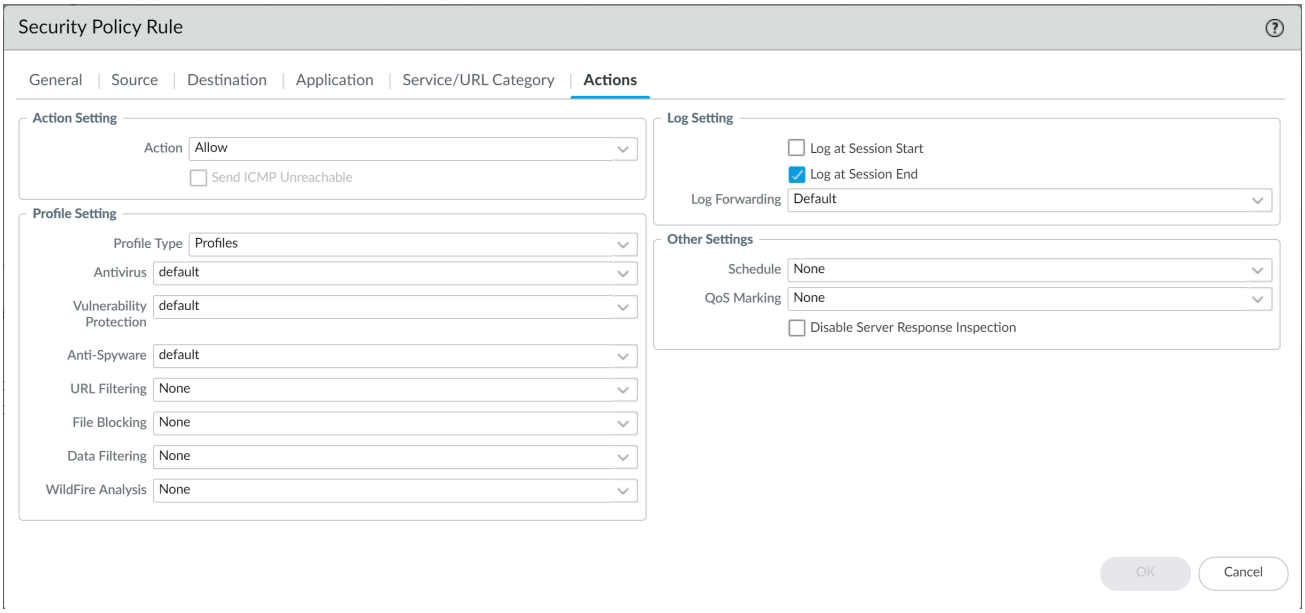
安全轉換到最佳做法安全性設定檔，以確保最佳安全性。

- 若要建立自訂 Antivirus Profiles（防毒設定檔），請選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Antivirus**（防毒），然後 **Add**（新增）設定檔。使用防毒設定檔轉換步驟，安全達成目標。
- 若要建立自訂反間諜軟體設定檔，可選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體），然後 **Add**（新增）設定檔。使用反間碟軟體設定檔轉換步驟，安全達成目標。
- 若要建立自訂弱點保護設定檔，請選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Vulnerability Protection**（弱點保護），然後 **Add**（新增）設定檔。使用漏洞保護設定檔轉換步驟，安全達成目標。

STEP 5 | 將安全性設定檔附加至安全性原則規則。

若您為防火牆設定了使用漏洞保護設定檔封鎖連線的安全性原則規則，防火牆將自動封鎖硬體中的此類流量（請參閱監控封鎖的 IP 位址）。

1. 選取**Policies**（原則） > **Security**（安全性），然後選取您要修改的規則。
2. 在 **Actions**（動作）頁籤中，選取 **Profiles**（設定檔）作為 **Profile Type**（設定類型）。
3. 選取為 **Antivirus**（防毒）、**Anti-Spyware**（反間諜）和 **Vulnerability Protection**（漏洞保護）建立的安全性設定檔。



STEP 6 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

設定內嵌雲端分析

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階威脅防護（支援增強功能）

內嵌雲端分析是一項進階 Threat Prevention 功能，可透過查詢進階 Threat Prevention 雲端服務來即時偵測進階、高度規避的零時差命令與控制 (C2) 威脅，以及命令注入和 SQL 注入弱點。內嵌雲端分析防護是透過反間諜軟體和弱點保護安全性設定檔提供的，前者會處理進階 C2（命令與控制）和間諜軟體威脅，後者處理命令注入和 SQL 注入弱點。

運行 PAN-OS 11.2 及更高版本部署的受支援防火牆還可以存取進階 Threat Prevention 的本機深度學習。本機深度學習透過提供一種機制來對零時差威脅和其他規避性威脅執行基於本機深度學習的快速分析，從而補充了進階 Threat Prevention 的內嵌雲端分析元件。本機深度學習模型的更新是透過內容更新來提供的。由於執行本機深度學習偵測模組需要額外的系統資源，因此本機深度學習僅在以下平台上可用：

- PA-5400 系列，不含 PA-5450 設備。
- VM-Series（必須分配至少總記憶體的 16GB）
- VM-Series 公有雲
- VM-Series 私有雲

若要啟用和設定內嵌雲端分析和本機深度學習，您必須啟動進階 Threat Prevention 授權，並建立（或修改）反間諜軟體和弱點保護安全性設定檔。然後為每個類別分析引擎配置政策設定，並將設定檔附加到安全性政策規則。

有關建立安全性政策規則的詳細資訊，請參閱 PAN-OS® 管理員指南的政策章節。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定內嵌雲端分析（PAN-OS 和 Panorama）

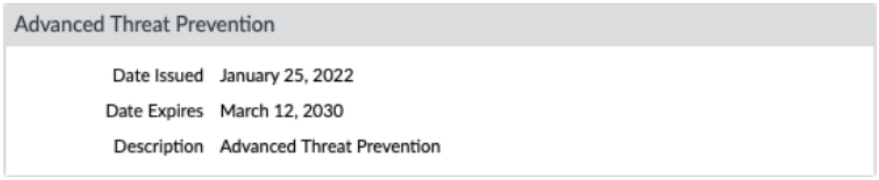
進階 *Threat Prevention* 內嵌雲端分析支援多個偵測引擎，這些引擎需要不同的最低 *PAN-OS* 版本才能啟用：

- 偵測進階 *C2*（命令和控制）和間諜軟體威脅需要 *PAN-OS 10.2* 及更高版本。
- 偵測零時差入侵威脅需要 *PAN-OS 11.0* 及更高版本。
- 支援 *LDL*（本機深度學習）需要 *PAN-OS 11.2* 及更高版本。

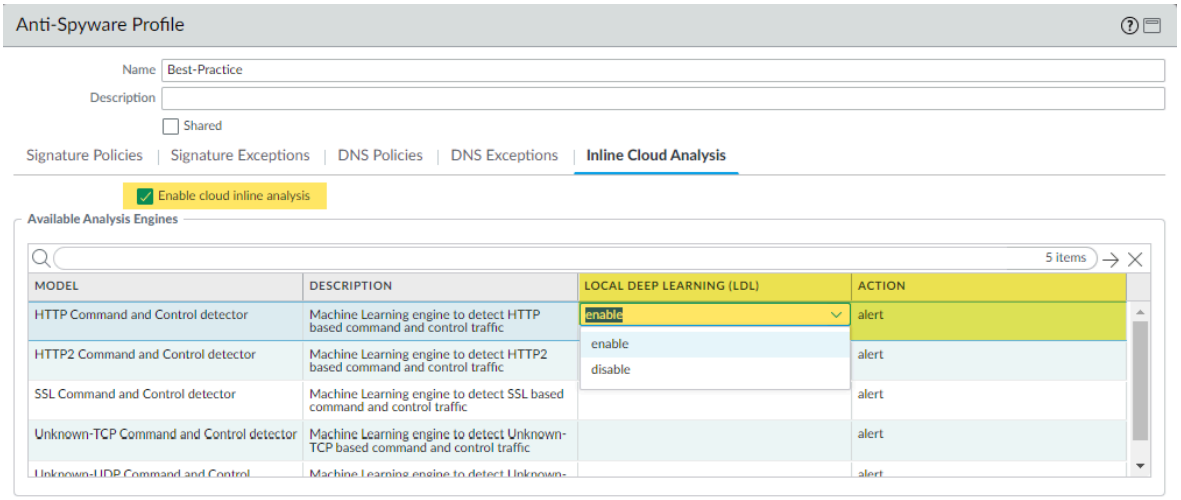
STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 若要利用內嵌雲端分析，您必須具有作用中的進階 Threat Prevention 訂閱。

若要確認當前哪些訂閱具有作用中的授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認有適當的授權可供使用並且該授權沒有過期。



STEP 3 | 更新或建立新的反間諜軟體安全性設定檔以啟用內嵌雲端分析（即時分析進階 C2（命令和控制）和間諜軟體威脅的流量）。



1. 選取現有的 **Anti-Spyware Profile**（反間諜軟體設定檔）或 **Add**（新增）新的設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體））。
2. 選取反間諜軟體設定檔，然後移至 **Inline Cloud Analysis**（內嵌雲端分析）及 **Enable inline cloud analysis**（啟用內嵌雲端分析）。
3. （本機深度學習 [在 PAN-OS 11.2 及更高版本中受支援]）為具有 **Local Deep Learning (LDL)**（本機深度學習 **(LDL)**）選項的每個可用分析引擎選取 **enable**（啟用）。目前有兩種分

析引擎可搭配選用的 LDL 模式：**HTTP Command and Control detector**（**HTTP** 命令和控制偵測器）和 **HTTP2 Command and Control detector**（**HTTP2** 命令和控制偵測器）。

4. 指定在使用相應的分析引擎偵測到威脅時要執行的 **Action**（動作）。

   每個分析引擎的預設動作是 ***alert***（警示），不過，*Palo Alto Networks* 建議將所有動作都設定為 ***Reset-Both***（重設兩者）以取得最佳安全狀況。

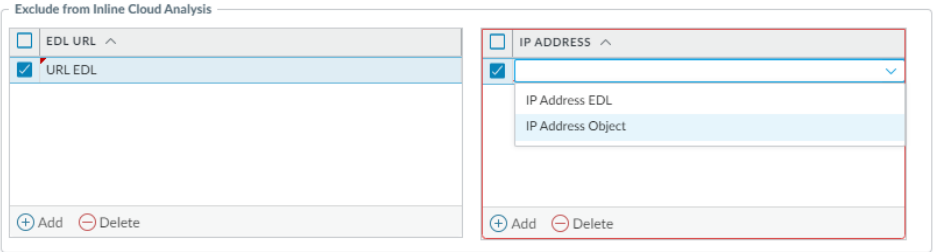
   - **Allow**（允許）—允許要求，不產生日誌項目。
   - **Alert**（警示）—允許要求並產生威脅日誌項目。
   - **Drop**（丟棄）—丟棄要求；重設動作不會傳送至主機/應用程式。
   - **Reset-Client**（重設用戶端）—重設用戶端連線。
   - **Reset-Server**（重設伺服器）—重設伺服器端連線。
   - **Reset-Both**（重設兩者）—重設用戶端及伺服器端的連線。

5. 按一下 **OK**（確定）以結束反間諜軟體設定檔設定對話方塊並 **Commit**（提交）您的變更。

STEP 4 | （選用）如果內嵌雲端分析產生誤判，則向反間諜軟體設定檔新增 URL 和/或 IP 位址例外。可以透過指定外部動態清單（URL 或 IP 位址清單類型）或 **Addresses**（位址）物件來新增例外。

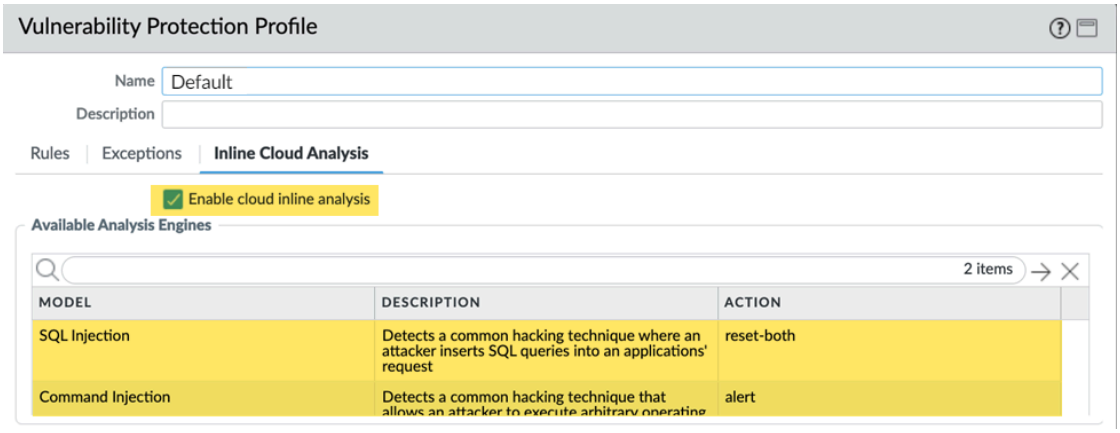
1. 新增 **External Dynamic Lists**（外部動態清單） 或 [IP] **Addresses**（位址）物件例外。
2. 選取 **Objects > Security Profiles > Anti-Spyware**（物件 > 安全性設定檔 > 反間諜軟體）。
3. 選取要為其排除特定 URL 和/或 IP 位址的反間諜軟體設定檔，然後選取 **Inline Cloud Analysis**（內嵌雲端分析）。
4. 根據要新增的例外類型，**Add**（新增）**EDL URL** 或 **IP Address**（**IP** 位址），然後選取預先存在的 URL 或 IP 位址外部動態清單。如果沒有可用清單，則建立一個新的外部動態清單。對於 IP 位址例外，可以選取 **Addresses**（位址）物件清單。

   在 *Panorama* 管理的防火牆上設定為 ***Shared***（共用）的反間諜軟體設定檔無法將 *IP* 位址物件新增至內嵌雲端分析例外清單。



5. 按一下 **OK**（確定）以儲存反間諜軟體設定檔並 **Commit**（提交）您的變更。

STEP 5 | （在 PAN-OS 11.0 及更高版本中支援）更新或建立新的弱點保護安全性設定檔，以啟用內嵌雲端分析（即時分析命令注入和 SQL 注入弱點的流量）。

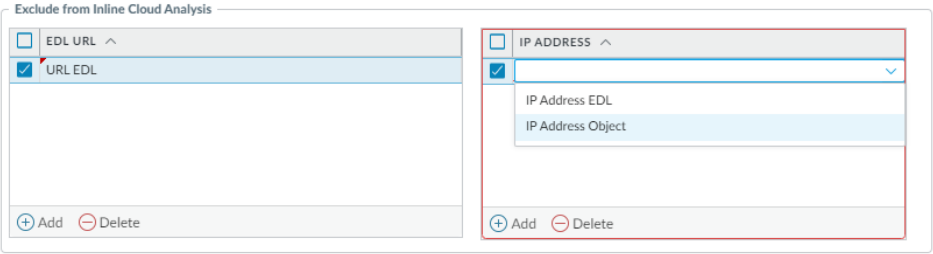


1. 選取現有的弱點保護安全性設定檔 或 **Add**（新增）（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Vulnerability Protection**（弱點保護））。
2. 選取您的弱點保護設定檔，然後前往 **Inline Cloud Analysis**（內嵌雲端分析）和 **Enable cloud inline analysis**（啟用雲端內嵌分析）。
3. 指定使用對應的分析引擎偵測到弱點入侵時要採取的 **Action**（動作）。目前有兩種可用的分析引擎：**SQL Injection**（**SQL** 注入）和 **Command Injection**（命令注入）。
   - **Allow**（允許）—允許要求，不產生日誌項目。
   - **Alert**（警示）—允許要求並產生威脅日誌項目。
   - **Reset-Client**（重設用戶端）—重設用戶端連線。
   - **Reset-Server**（重設伺服器）—重設伺服器端連線。
   - **Reset-Both**（重設兩者）—重設用戶端及伺服器端的連線。
4. 按一下 **OK**（確定）以退出弱點保護設定檔的設定對話，並且 **Commit**（提交）變更。

STEP 6 | （選用）如果內嵌雲端分析產生誤判，則向弱點保護設定檔新增 URL 和/或 IP 位址例外。可以透過指定外部動態清單（URL 或 IP 位址清單類型）或 **Addresses**（位址）物件來新增例外。

1. 新增 **External Dynamic Lists**（外部動態清單） 或 [IP] **Addresses**（位址）物件例外。
2. 選取 **Objects > Security Profiles > Vulnerability**（物件 > 安全性設定檔 > 弱點），以返回您的弱點保護設定檔。
3. 選取您要排除特定 URL 和/或 IP 位址的弱點設定檔，然後選取 **Inline Cloud Analysis**（內嵌雲端分析）。
4. 根據要新增的例外類型，**Add**（新增）**EDL URL** 或 **IP Address**（**IP** 位址），然後選取預先存在的 URL 或 IP 位址外部動態清單。如果沒有可用清單，則建立一個新的外部動態清單。對於 IP 位址例外，可以選取 **Addresses**（位址）物件清單。

   在 *Panorama* 管理的防火牆上設定為 ***Shared***（共用）的弱點設定檔無法將 *IP* 位址物件新增至內嵌雲端分析例外清單。



5. 按一下 **OK**（確定）以儲存弱點保護設定檔，並 **Commit**（提交）變更。

STEP 7 | 設定逾時延遲，以及要求超過延遲上限時要採取的動作。

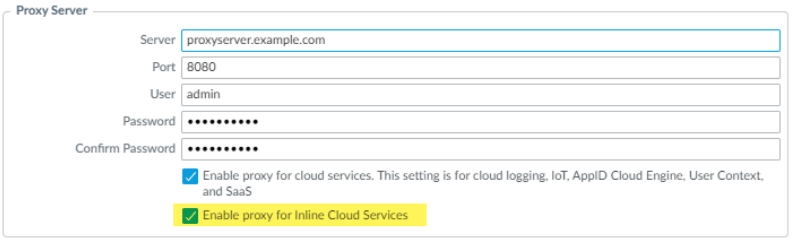
1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Threat Prevention Inline Cloud Analysis**（**Threat Prevention** 內嵌雲端分析）。
2. 指定逾時值，以及達到內嵌雲端分析要求的延遲上限時，要採取的相關動作：
   - 最大延遲（毫秒）—指定內嵌雲端分析回傳結果的最大可接受處理時間（以秒為單位）。
   - 達到最大延遲時允許—使防火牆能夠在達到最大延遲時執行允許動作。取消選取此選項可將防火牆動作設定為封鎖。
   - 未掃描日誌流量—使防火牆能夠記錄表現出異常特徵的流量要求，這些異常特徵指示存在進階和規避命令和控制 (C2) 威脅，但尚未由 Threat Prevention 內嵌雲端分析器處理。
3. 按一下 **OK**（確定）確認您的變更。

STEP 8 | 安裝裝置憑證對所有啟用內嵌雲端分析的防火牆重複此操作。

STEP 9 | （使用明確 Proxy 伺服器部署防火牆時為必要項目）設定代理伺服器，以用於存取有助於所有已設定內嵌雲端分析功能所產生要求的伺服器。可以指定單一 Proxu 伺服器並將其套用至所有 Palo Alto Networks 更新服務，包括所有已設定的內嵌雲端和記錄日誌服務。

1. （PAN-OS 11.2.3 及更新版本）透過 PAN-OS 設定 Proxy 伺服器。
   1. 選取 **Device**（裝置） > **Setup**（設定） > **Services**（服務），並編輯 **Services**（服務）詳細資料。
   2. 指定 **Proxy Server**（**Proxy** 伺服器）設定並 **Enable proxy for Inline Cloud Services**（啟用內嵌運端服務的 **Proxy** 存取）。您可以在 **Server**（伺服器）欄位中提供 IP 位址或 FQDN。

      Proxy 伺服器密碼必須包含至少六個字元。

   3. 按一下 **OK**（確定）。
2. （僅適用於以下版本：（PAN-OS 10.2.11 及更新版本，以及 PAN-OS 11.1.5 及更新版本）透過防火牆 CLI 設定 Proxy 伺服器。
   1. 存取防火牆 CLI。
   2. 使用下列 CLI 命令設定基本 Proxy 伺服器設定：

      ```
      set deviceconfig system secure-proxy-server <FQDN_or_IP>
       set deviceconfig system secure-proxy-port <1-65535>
       set deviceconfig system secure-proxy-user <value> set
       deviceconfig system secure-proxy-password <value>
      ```

      Proxy 伺服器密碼必須包含至少六個字元。

   3. 使用下列 CLI 命令啟用 Proxy 伺服器，以向內嵌雲端服務伺服器傳送請求：

      ```
      debug dataplane mica set inline-cloud-proxy enable
      ```

   4. 使用下列 CLI 命令檢視內嵌雲端服務 Proxy 支援的目前運作狀態：

      ```
      debug dataplane mica show inline-cloud-proxy
      ```

      例如：

      ```
      debug dataplane mica show inline-cloud-proxy 適用於已停用進階服務的 Proxy
      ```

STEP 10 | （選用）設定防火牆用於處理內嵌雲端分析服務要求的雲端內容完全合格網域名稱 (FQDN)。預設 FQDN 連接至 hawkeye.services-edge.paloaltonetworks.com，然後解析為最近的雲端服務伺服器。您可以透過指定最能滿足資料落地和效能需求的區域雲端內容伺服器來取代自動伺服器選取。

雲端內容 *FQDN* 是全球使用的資源，會影響依賴於此連線的其他服務傳送流量有效負載的方式。

確認防火牆使用適用於您所在區域的正確內容雲端 FQDN（**Device**（裝置） > **Setup**（設定） > **Content-ID**（內容 **ID**） > **Content Cloud Setting**（內容雲端設定）），並視需要變更 FQDN：

如果您的 *NGFW* 已內嵌設定為促進 *SaaS* 安全性部署，請注意，位於法國和日本的 *FQDN* 目前不支援 *SaaS* 安全性功能。

- 美國中部（美國愛荷華州）—**us.hawkeye.services-edge.paloaltonetworks.com**
- 歐洲（德國法蘭克福）—**eu.hawkeye.services-edge.paloaltonetworks.com**
- 亞太地區（新加坡）—**apac.hawkeye.services-edge.paloaltonetworks.com**
- 印度（孟買）—**in.hawkeye.services-edge.paloaltonetworks.com**
- 英國（英國倫敦）—**uk.hawkeye.services-edge.paloaltonetworks.com**
- 法國（法國巴黎）—**fr.hawkeye.services-edge.paloaltonetworks.com**
- 日本（日本東京）—**jp.hawkeye.services-edge.paloaltonetworks.com**
- 澳洲（澳洲雪梨）—**au.hawkeye.services-edge.paloaltonetworks.com**
- 加拿大（加拿大蒙特婁）—**ca.hawkeye.services-edge.paloaltonetworks.com**
- 瑞士（瑞士蘇黎世）—**ch.hawkeye.services-edge.paloaltonetworks.com**

STEP 11 | （選用）驗證防火牆到進階 Threat Prevention 雲端服務的連線狀態。

在防火牆上使用以下 CLI 命令檢視連線狀態。

```
show ctd-agent status security-client
```

例如：

```
show ctd-agent status security-client ...Security Client AceMlc2(1)
 Current cloud server: hawkeye.services-edge.paloaltonetworks.com
 Cloud connection: connected ...
```

為簡潔起見，縮短了 *CLI* 輸出。

如果無法連接至進階 Threat Prevention 雲端服務，請驗證以下網域是否未被封鎖：hawkeye.services-edge.paloaltonetworks.com。

STEP 12 | （選用） 監控進階 Threat Prevention

設定內嵌雲端分析Strata Cloud Manager

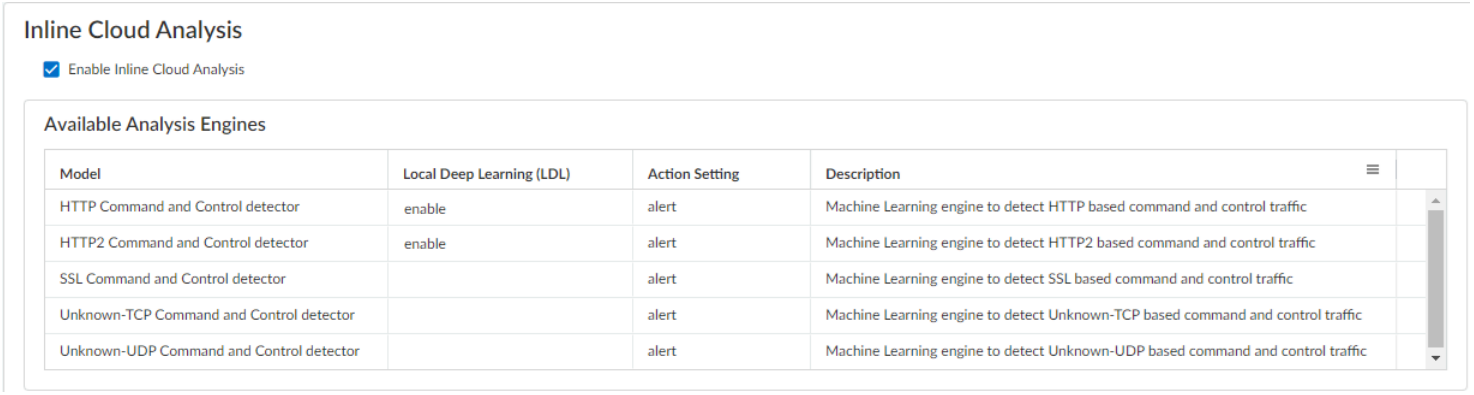
STEP 1 | 若要運用內嵌雲端分析，您必須擁有作用中的 Prisma Access 訂閱，提供對進階 Threat Prevention 功能的存取權。有關透過 Prisma Access 提供的應用程式和服務資訊，請參閱所有適用的應用程式和服務。

若要驗證您目前擁有的作用中授權訂閱，請檢查您的授權支援哪些。

STEP 2 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager。

STEP 3 | 更新或建立新的反間諜軟體安全性設定檔以啟用內嵌雲端分析（即時分析進階 C2 [命令和控制] 和間諜軟體威脅的流量）。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Anti-Spyware**（反間諜軟體）。
2. 選取您的反間諜軟體安全性設定檔，然後導覽至 **Inline Cloud Analysis**（內嵌雲端分析）面板，並 **Enable Inline Cloud Analysis**（啟用內嵌雲端分析）。



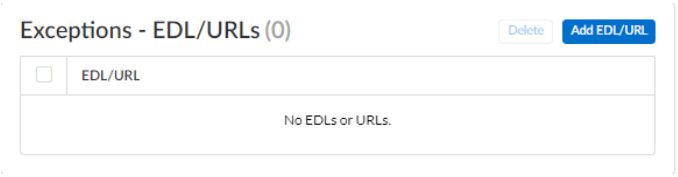
3. 為具有 **Local Deep Learning (LDL)**（本機深度學習 **(LDL)**）選項的每個可用分析引擎選取 **enable**（啟用）。目前有兩種分析引擎可搭配選用的 LDL 模式：**HTTP Command and Control detector**（**HTTP** 命令和控制偵測器）和 **HTTP2 Command and Control detector**（**HTTP2** 命令和控制偵測器）。
4. 指定在使用相應的分析引擎偵測到威脅時要執行的 **Action**（動作）。

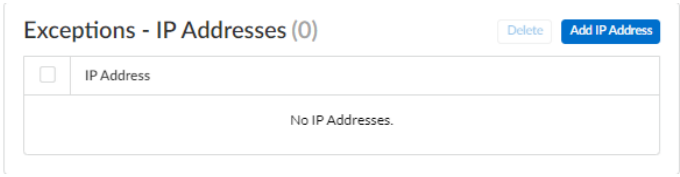
   每個分析引擎的預設動作是 ***alert***（警示），不過，*Palo Alto Networks* 建議將所有動作都設定為 ***Reset-Both***（重設兩者）以取得最佳安全狀況。

   - **Allow**（允許）—允許要求，不產生日誌項目。
   - **Alert**（警示）—允許要求並產生威脅日誌項目。
   - **Drop**（丟棄）—丟棄要求；重設動作不會傳送至主機/應用程式。
   - **Reset-Client**（重設用戶端）—重設用戶端連線。
   - **Reset-Server**（重設伺服器）—重設伺服器端連線。
   - **Reset-Both**（重設兩者）—重設用戶端及伺服器端的連線。
5. 按一下 **OK**（確定）以退出反間諜軟體安全性設定檔設定對話，並 **Commit**（提交）變更。

STEP 4 | （選用）如果內嵌雲端分析產生誤判，則向反間諜軟體設定檔新增 URL 和/或 IP 位址例外。可以透過指定外部動態清單（URL 或 IP 位址清單類型）或 **Addresses**（位址）政策物件來新增例外。

1. 新增 **External Dynamic Lists**（外部動態清單） 或 [IP] **Addresses**（位址）物件例外。
2. 選取 **Manage**（管理） > **Configuration**（設定） > **Anti-Spyware**（反間諜軟體）。
3. 選取要排除特定 URL 或 IP 位址的反間諜軟體設定檔，然後前往 **Inline Cloud Analysis**（內嵌雲端分析）窗格。
4. 根據要新增的例外類型，**Add EDL/URL**（新增 **EDL/URL**）或 **Add IP Address**（新增 **IP** 位址），然後選取預先存在的 URL 或 IP 位址外部動態清單。如果沒有可用清單，則建立一個新的外部動態清單政策物件。對於 IP 位址例外，可以選取 **Addresses**（位址）物件清單。





5. 按一下 **OK**（確定）以儲存反間諜軟體設定檔並 **Commit**（提交）您的變更。

STEP 5 | （選用） 監控進階 Threat Prevention

防止暴力密碼破解攻擊

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

暴力密碼破解攻擊使用大量來自相同來源或目的地 IP 位址的要求/回應來入侵系統。攻擊者運用試誤法來猜測挑戰或要求的回應。

弱點保護設定檔包含特徵碼以防禦暴力密碼破解攻擊。每個特徵碼都有 ID、威脅名稱及嚴重性，當模式被記錄下來時就會觸發特徵碼。模式會指定將流量視為暴力密碼破解攻擊的條件與間隔；有些特徵碼會與另一個子特徵碼相關聯，子特徵碼的嚴重性較低，並會指定要比對的模式。當模式比對特徵碼或子特徵碼時，會觸發特徵碼的預設動作。

若要執行保護：

- 將漏洞保護設定檔附加至安全性原則規則。請參閱 設定防毒、反間諜軟體及漏洞保護。
- 安裝內容更新，其中包含可防禦防火牆新興威脅的新特徵碼。請參閱安裝內容及軟體更新。

自訂暴力密碼破解特徵碼的動作與觸發條件

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

防火牆包含兩種預先定義的暴力密碼破解特徵碼—父特徵碼與子特徵碼。子特徵碼是符合特徵碼且只發生一次的流量模式。父特徵碼與子特徵碼有關聯，當在特定時間間隔內發生多個事件且事件符合在子特徵碼中定義的流量模式時，便會觸發父特徵碼。

一般而言，子特徵碼的預設動作是允許，因為單一事件並非表示攻擊會發生。這可以確保合法流量不會被封鎖，避免為不值得注意的事件產生威脅日誌。Palo Alto Networks 建議您務必在深思熟慮後才變更預設值。

在大多數的狀況中，暴力密碼破解特徵碼是值得注意的事件，因為它有重複發生的模式。若有必要，執行下列任何操作，來自訂針對暴力密碼破解特徵碼的動作：

- 建立規則以修改暴力密碼破解類別中所有特徵碼的預設動作。您可以選擇允許、警示、封鎖、重設或丟棄流量。
- 定義特定特徵碼的例外狀況。例如，您可以搜尋 CVE 並定義例外。

對於父特徵碼，您可以修改觸發條件與動作；對於子特徵碼，您只能修改動作。

為了有效減輕攻擊危害，可為大多數暴力密碼破解特徵碼指定封鎖 *IP* 位址動作而非丟棄或重設動作。

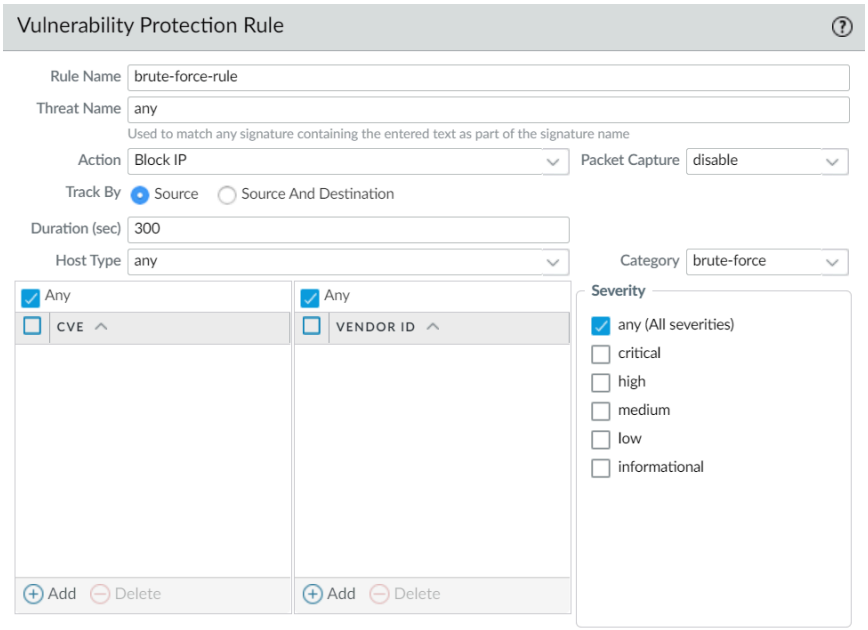
STEP 1 | 建立新漏洞保護設定檔。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Vulnerability Protection**（漏洞保護），然後 **Add**（新增） 設定檔。
2. 輸入漏洞保護設定檔的 **Name**（名稱）。
3. （選用）輸入 **Description**（說明）。
4. （選用）指定與下列項 **Shared**（共用）設定檔：
   - 多虛擬系統防火牆上的每個虛擬系統 **(vsys)**—如果清除（停用），設定檔將僅供 **Objects**（物件）頁籤上選定的虛擬系統使用。
   - **Panorama** 上的每個裝置群組—如果清除（停用），設定檔將僅供 **Objects**（物件）頁籤上選定的裝置群組使用。
5. （選用—僅限 Panorama）選取 **Disable override**（停用覆寫），可防止管理員在繼承此漏洞保護設定檔的裝置群組中取代該設定檔的設定。預設會清除此選取項目，這表示管理員可以覆寫繼承此設定檔之任何設備群組的設定。

STEP 2 | 建立可為類別中所有特徵碼定義動作的規則。

1. 在 **Rules**（規則）頁籤上，**Add**（新增）規則並輸入 **Rule Name**（規則名稱）。
2. （選用）指定特定的威脅名稱（預設為 **any**（任何））。
3. 設定 **Action**（動作）。在此範例中，動作設為 **Block IP**（封鎖 IP）。

   如果您設定了漏洞保護設定檔以封鎖 *IP*，防火牆將首先使用硬體來封鎖 *IP* 位址。如果攻擊流量超過硬體的封鎖能力，則防火牆會使用軟體封鎖機制來封鎖剩餘的 *IP* 位址。
4. 將 **Category**（類別）設為 **brute-force**。
5. （選用）如果封鎖，則指定針對哪種 **Host Type**（主機類型）執行封鎖：**server**（伺服器） 或 **client**（用戶端）（預設為 **any**（任何））。
6. 若要自訂特定特徵碼的動作，請參閱步驟 3。
7. 若要自訂上層特徵碼的觸發閾值，請參閱步驟 4。



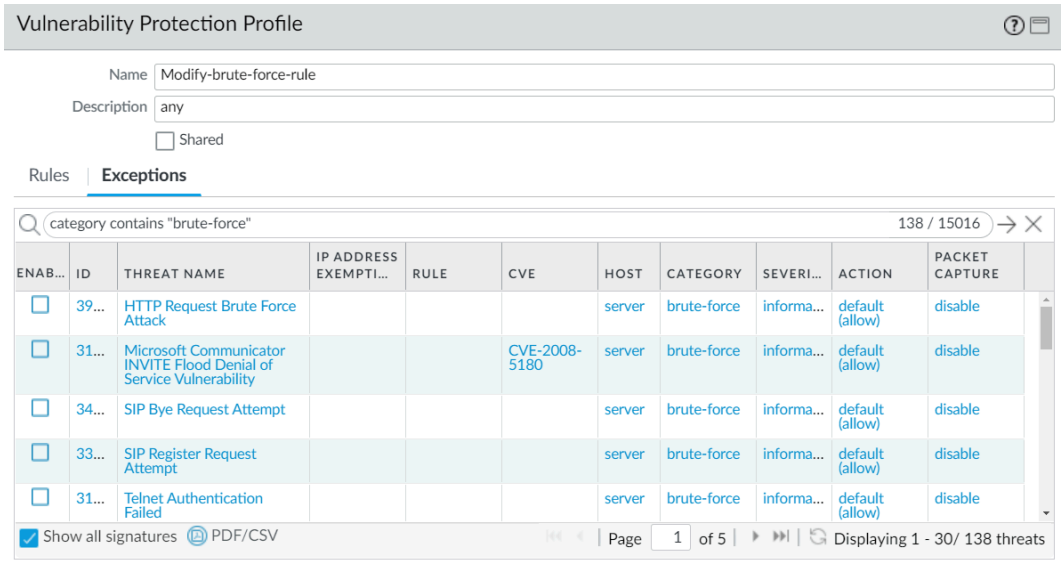
8. 按一下 **OK**（確定）儲存規則與設定檔。

STEP 3 | （選用）自訂特定特徵碼的動作。

1. 在 **Exceptions**（例外）頁籤上，**Show all signatures**（顯示所有特徵碼），以尋找您要修改的特徵碼。

   若要檢視暴力密碼破解類別中所有的特徵碼，可搜尋 `category contains 'brute-force'`。

2. 若要編輯特定特徵碼，請按一下動作欄中的預設動作。



3. 設定動作：**Allow**（允許）、**Alert**（警示）、**Block Ip**（封鎖 IP）或 **Drop**（丟棄）。如果您選取 **Block Ip**（封鎖 IP），則完成下列額外的工作：

   1. 指定經過多長 **Time**（時間）（單位為秒）後觸發動作。
   2. 指定是使用 **IP source**（IP 來源）還是 **IP source and destination**（IP 來源和目的地）來 **Track By**（追蹤）和封鎖 IP 位址。

4. 按一下 **OK**（確定）。
5. 對於每個修改過的特徵碼，選取 **Enable**（啟用）欄中的核取方塊。
6. 按一下 **OK**（確定）。

STEP 4 | 自訂父特徵碼觸發條件。

可以編輯的父特徵碼會標示此圖示：.

在此範例中，搜尋準則是暴力密碼破解類別與 CVE-2008-1447。

1. 編輯 ( ) 特徵碼的時間屬性與彙總準則。
2. 若要修改觸發臨界值，請指定**Number of Hits**（叫用次數）x **seconds**（秒數）。
3. 指定是依據 **source**（來源）、**destination**（目的地）還是 **source-and-destination**（來源和目的地）彙總叫用次數（**Aggregation Criteria**（彙總準則））。
4. 按一下 **OK**（確定）。

STEP 5 | 將此新設定檔附加至安全性原則規則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後 **Add**（新增） 或修改安全性原則規則。
2. 在 **Actions**（動作）頁籤上，選取 **Profiles**（設定檔）作為設定檔組態的 **Profile Type**（設定類型）。
3. 選取 **Vulnerability Protection**（漏洞保護）設定檔。
4. 按一下 **OK**（確定）。

STEP 6 | Commit（提交）您的變更。

1. 按一下 **Commit**（交付）。

啟用規避特徵碼

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

Palo Alto Networks 用於偵測所產生的 HTTP 或 TLS 要求，可向用戶端連接至非 DNS 查詢中指定網域的實例發出警示。只有在防火牆已用作 DNS Proxy 並解析網域名稱查詢的情況下，規避特徵碼才能發揮作用。最佳做法是，按照下列步驟啟用規避特徵碼。

STEP 1 | 啟用用戶端與伺服器之間的防火，以用作 DNS Proxy。

設定 DNS Proxy 物件，包括：

- 指定您要防火牆在其上方接聽 DNS 查詢的介面。
- 定義防火牆將與之通訊以解析 DNS 要求的 DNS 伺服器。
- 設定防火牆可以本機解析（無需連線 DNS 伺服器）的靜態 FQDN 至 IP 位址項目。
- 允許快取已解析之主機名稱到 IP 位址對應。

STEP 2 | 獲取最新的應用程式與威脅內容版本（至少為 579 或更新的內容版本）。

1. 請選取 **Device**（裝置） > **Dynamic Updates**（動態更新）。（裝置 > 動態更新）.
2. **Check Now**（立即檢查）以獲得最新應用程式與威脅內容更新。
3. 下載並安裝應用程式與威脅內容版本 579（或更新版本）。

STEP 3 | 定義防火牆應對與規避特徵碼相符的流量強制執行何種動作。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）並 **Add**（新增） 或修改 反間諜軟體設定檔 。
2. 選取 **Exceptions**（例外），然後選取 **Show all signatures**（顯示所有特徵碼）。
3. 根據關鍵字 `evasion` 篩選特徵碼。
4. 對於所有規避特徵碼，請將 **Action**（動作）設定為允許或預設動作（對規避特徵碼的預設動作是允許）以外的任何設定。例如針對特徵碼 ID 14978 和 14984，將 **Action**（動作）設定為 **alert**（警示）或 **drop**（丟棄）。
5. 按一下 **OK**（確定），儲存更新的反間諜軟體設定檔。
6. 將反間諜軟體設定檔附加至安全性原則規則：選取 **Policies**（原則） > **Security**（安全性），選取要修改的原則，然後按一下 **Actions**（動作）頁籤。在設定檔組態中，按一下 **Anti-Spyware**（反間諜軟體）旁邊的下拉式清單，然後選取您要修改的反間諜軟體設定檔以強制執行規避特徵碼。

STEP 4 | Commit（提交）您的變更。

按一下 **Commit**（交付）。

建立威脅例外

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

Palo Alto Networks 定義了針對威脅特徵碼的建議預設動作（例如封鎖或警示）。您可以使用威脅 ID 將威脅特徵碼從強制執行中排除，或者修改針對該威脅特徵碼強制執行的動作。例如，您可以修改針對在網路上觸發誤報的威脅特徵碼的動作。

針對防毒、弱點、間諜軟體和 DNS 特徵碼設定威脅例外，以變更針對威脅強制執行的動作。但是，在開始之前，請確保已根據預設或最佳做法特徵碼設定，正確偵測威脅和強制執行，以獲得最佳安全狀態：

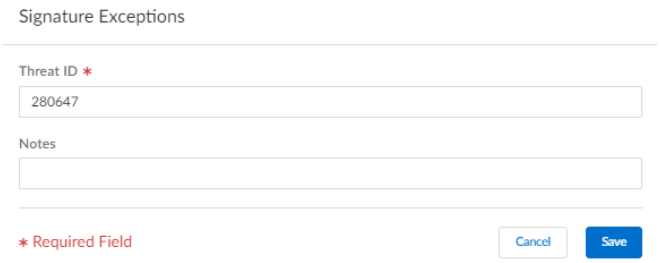
- 取得最新的防毒、威脅和應用程式以及 WildFire 特徵碼更新（適用於防火牆）。
- 設定防毒、反間諜軟體及漏洞保護並將這些安全性設定檔套用到您的安全性政策中。
- Strata Cloud Manager
- PAN-OS 和 Panorama

建立威脅例外 (Strata Cloud Manager)

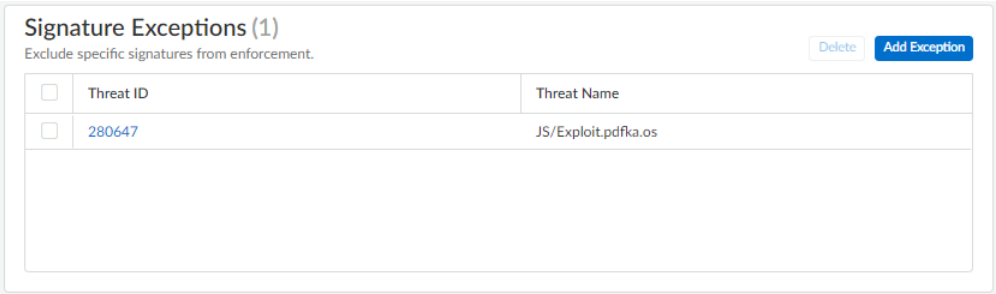
STEP 1 | 將防毒特徵碼從強制執行中排除。

雖然您可以使用 *WildFire* 和防毒設定檔將防毒特徵碼從強制執行中排除，但您不能變更將對特定防毒特徵碼強制執行的動作。但是，您可以透過編輯安全性設定檔 ***Enforcement Actions***（強制執行動作），來定義在不同類型的流量中發現病毒時可強制執行的動作。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **WildFire and Antivirus**（**WildFire** 和防毒）。
2. **Add Profile**（新增設定檔），或是從您要排除威脅特徵碼的位置選取現有 WildFire 和防毒設定檔，然後前往 **Advanced Settings**（進階設定）分頁。
3. 從 **Signature Exceptions**（特徵碼例外）功能表中 **Add Exception**（新增例外），並針對您要從強制執行中排除的威脅特徵碼提供 **Threat ID**（威脅 **ID**）。您可以選擇在特徵碼例外中新增註解。



4. 完成後請 **Save**（儲存）特徵碼例外。
5. 有效的威脅特徵碼 ID 會自動填入威脅名稱欄位。您可以檢視作用中的特徵碼例外完整清單，並且 **Delete**（刪除）不再需要的項目。

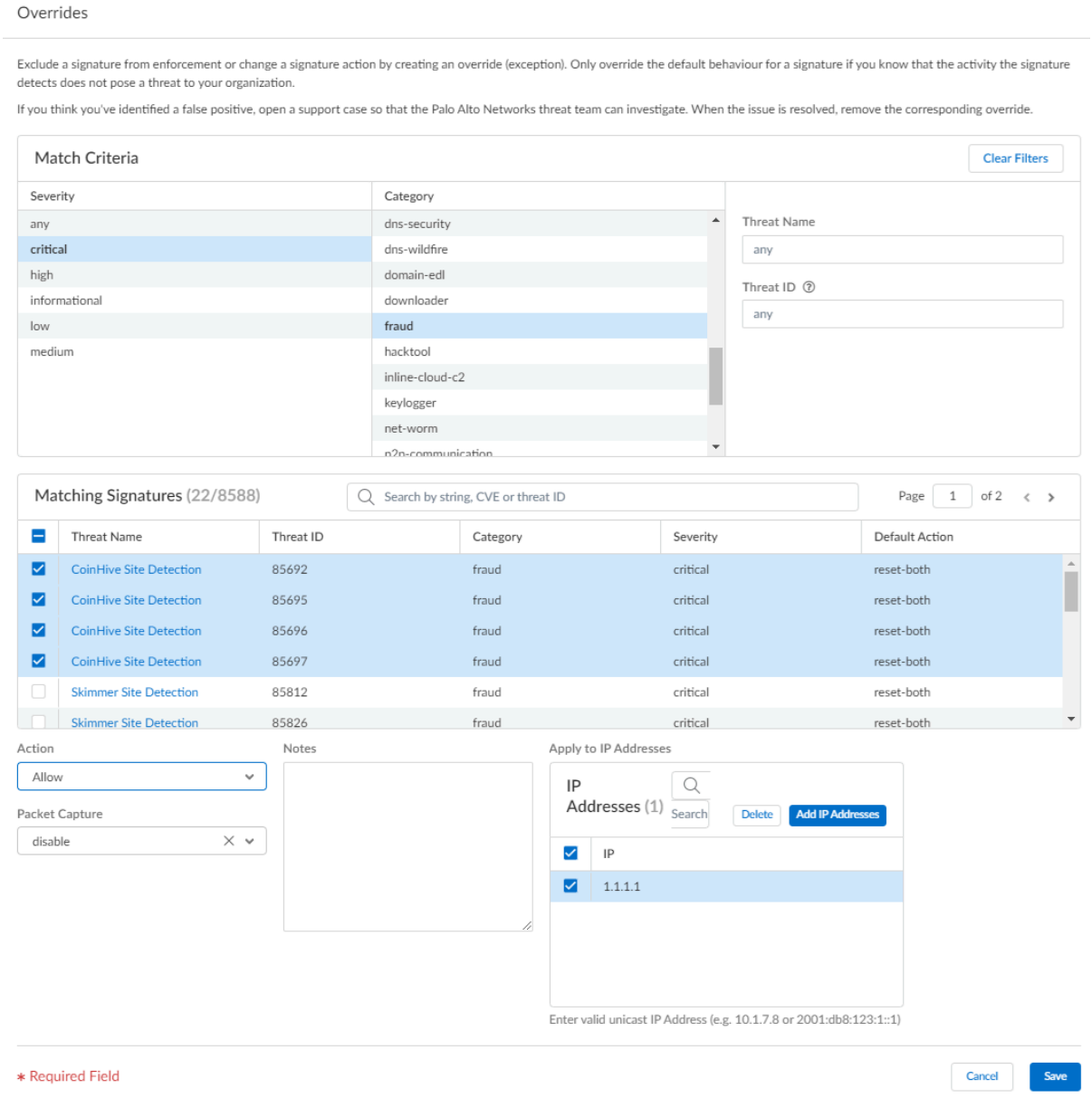


6. 重複新增其他例外，或在新增所有威脅例外後按一下 **Save**（儲存）。

STEP 2 | 修改弱點和間諜軟體特徵碼的強制執行（DNS 特徵碼除外；雖然是間諜軟體特徵碼的一種，但 DNS 特徵碼是透過 Prisma Access 中的 DNS 安全訂閱來處理的）。

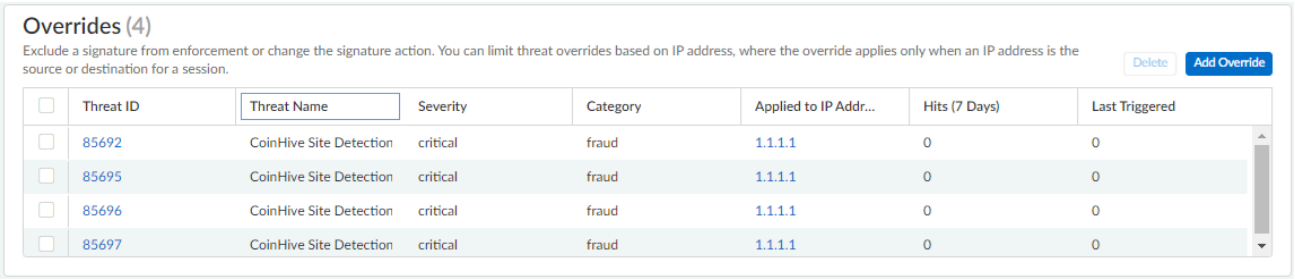
1. 根據特徵碼類型，選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Anti-Spyware**（反間諜軟體）或 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access** > **Security Services**（安全服務） > **Vulnerability Protection**（弱點保護）。
2. **Add Profile**（新增設定檔）或從您要修改特徵碼強制執行的位置，選取現有反間諜軟體或弱點保護設定檔，然後選取 **Add Override**（新增取代）。

3. 透過提供相關的 **Match Criteria**（比對規則）來搜尋間諜軟體或弱點特徵碼。這會自動過濾可用的特徵碼，並在 **Matching Signatures**（比對特徵碼）部分中顯示結果。
4. 選取要修改強制執行的特徵碼核取方塊。
5. 針對已選取的特徵碼，提供更新的 **Action**（動作）、**Packet Capture**（封包擷取）以及 **IP Addresses**（IP 位址），以便套用修改後的強制執行規則。



6. **Save**（儲存）更新的特徵碼強制執行設定。

7. 您可以檢視 **Overrides**（取代）的完整列表，包括各種統計資料，並且 **Delete**（刪除）不再需要的項目。

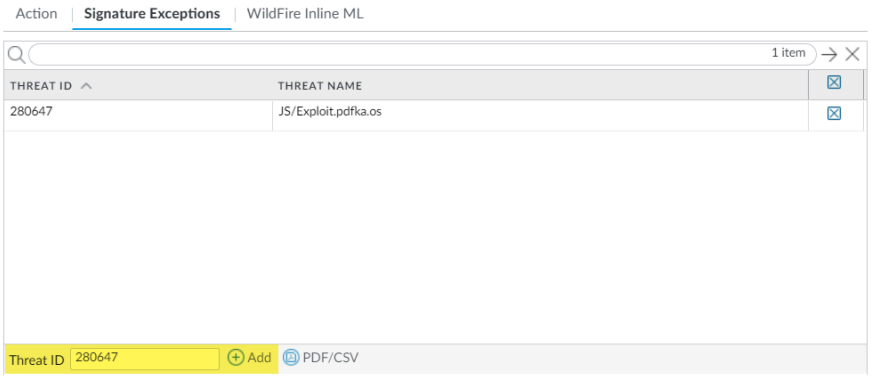


建立威脅例外 (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | 將防毒特徵碼從強制執行中排除。

雖然您可以使用防毒設定檔將防毒特徵碼從強制執行中排除，但您不能變更防火牆將對特定防毒特徵碼強制執行的動作。然而，您可以透過編輯解碼器，定義防火牆將針對在不同類型流量中找到的病毒強制執行的動作（***Objects***（物件）**>** ***Security Profiles***（安全性設定檔）**>** ***Antivirus***（防毒）**>** ***<antivirus-profile>*** **>** ***Antivirus***（防毒））。

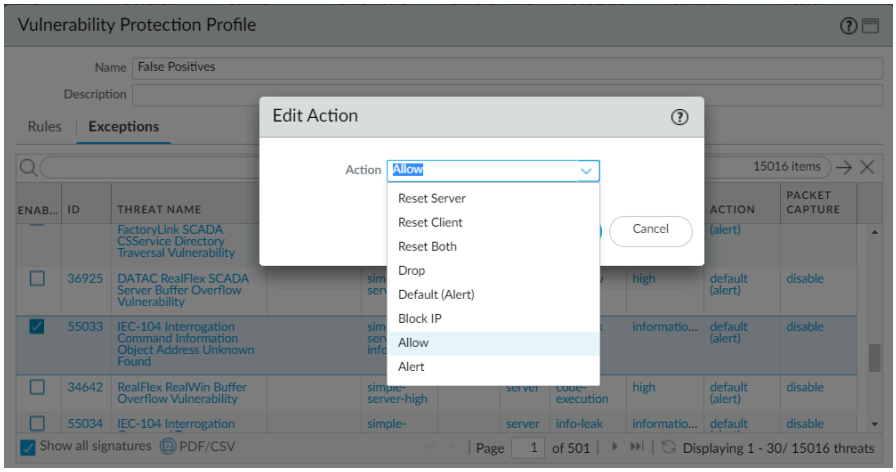
1. 選取 **Objects**（物件）**>** **Security Profiles**（安全性設定檔）**>** **Antivirus**（防毒）。
2. **Add**（新增）您希望從中排除威脅特徵碼的防毒設定檔或修改現有設定檔，然後選取 **Signature Exception**（特徵碼例外）。
3. 為您要從強制執行中排除的威脅特徵碼 **Add**（新增）**Threat ID**（威脅 **ID**）。



4. 按一下 **OK**（確定）以儲存防毒設定檔。

STEP 2 | 修改針對漏洞和間諜軟體特徵碼的強制執行規則（DNS 特徵碼除外；跳至下一選項，為 DNS 特徵碼修改強制執行；DNS 特徵碼屬於間諜軟體特徵碼）。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體） 或 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Vulnerability Protection**（漏洞保護）。
2. **Add**（新增）您想要從中排除威脅特徵碼的反間諜軟體或漏洞保護設定檔或修改現有設定檔，然後為反間諜軟體保護設定檔選取 **Signature Exceptions**（特徵碼例外），或為漏洞保護設定檔選取 **Exceptions**（例外）。
3. **Show all signatures**（顯示所有特徵碼），然後進行篩選，以選取要修改強制執行規則的特徵碼。
4. 核取 **Enable**（啟用）欄下的方塊，獲得要修改其執行規則的特徵碼。
5. 選取您希望防火牆對此威脅特徵碼強制執行的 **Action**（動作）。



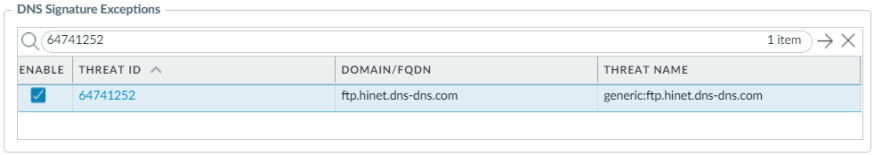
對於您希望從強制執行中排除的特徵碼（因為會觸發誤報），將 **Action**（動作）設定為 **Allow**（允許）。

6. 按一下 **OK**（確定）以儲存新的或修改後的反間諜軟體或漏洞保護設定檔。

STEP 3 | 為 DNS 特徵碼修改強制執行規則。

依預設，對於已偵測到 DNS 特徵碼的惡意主機名稱，其 DNS 查閱將被 sinkhole。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. **Add**（新增）或修改您希望從中排除威脅特徵碼的反間諜軟體設定檔，然後選取 **DNS Exceptions**（**DNS** 例外）。
3. 搜尋您要從強制執行中排除的 DNS 特徵碼的 DNS 威脅 ID，然後選取適用特徵碼的方塊：



4. 按一下 **OK**（確定）以儲存新的或修改後的反間諜軟體設定檔。

使用 DNS 查詢識別網路上受感染的主機

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

反間諜軟體設定檔中的 DNS Sinkhole 動作能讓防火牆偽造對 DNS 查詢之有關已知惡意網域的回應，或偽造對自訂網域的回應，以便您可以識別網路上感染惡意軟體的主機。遭入侵的主機可能會啟動與命令和控制 (C2) 伺服器的通訊—一旦建立連線，攻擊者即可遠端控制受感染主機，以進一步滲入網路或洩漏資料。

針對 Palo Alto Networks DNS 特徵碼清單中包括的任何網域的 DNS 查詢，會導向至 Palo Alto Networks 伺服器 IP 位址，因此遭到 sinkhole 攻擊。

防火牆有兩個 DNS 特徵碼來源，可用於識別惡意和 C2 網域：

- （需要進階 | Threat Prevention 訂閱）本機 DNS 特徵碼—這是一組有限的盒上 DNS 特徵碼，防火牆可用於識別惡意網域。防火牆取得新的 DNS 特徵碼作為日常防毒軟體更新的一部分。
- （需要 DNS 安全性訂閱）DNS 安全性特徵碼—防火牆存取 Palo Alto Networks DNS 安全性雲端服務，以根據完整的 DNS 特徵碼資料庫來識別惡意網域。某些特徵碼（僅 DNS 安全性提供）可以唯一地偵測使用網域產生演算法 (DGA) 和 DNS 通道等機器學習技術的 C2 攻擊。有關 DNS 安全訂閱的更多資訊，請參閱 DNS 安全指南。

  如果您想要為 DNS 安全特徵碼指定 sinkhole 操作，您可以將這些設定配置為 DNS 安全性設定檔的一部分。

針對本機 DNS 特徵碼集或 DNS 安全性特徵碼集中網域的 DNS 查詢，將重新導向至 Palo Alto Networks 伺服器，且主機無法存取惡意網域。下列主題提供有關如何啟用 DNS sinkholing 以識別受感染主機的詳細資訊。

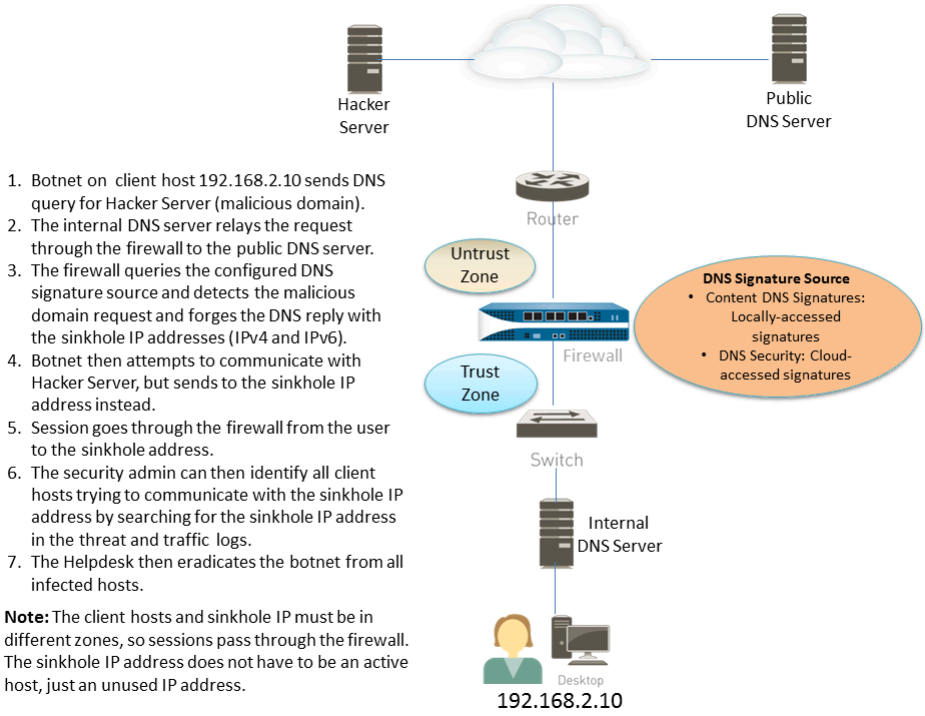
- DNS Sinkholing 的運作原理
- 設定 DNS Sinkholing
- 為自訂網域清單設定 DNS Sinkholing
- 將 Sinkhole IP 位址設定為網路上的本機伺服器
- 查看嘗試連線至惡意網域的受感染主機

DNS Sinkholing 的運作原理

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

我可以在哪裡使用這個？	我需要哪些內容？
• CN-Series	

DNS Sinkholing 可幫助您在防火牆看不到受感染用戶端的 DNS 查詢 (亦即防火牆看不到 DNS 查詢的發送者) 狀況下，使用 DNS 流量來識別受保護網路上的遭感染主機。在防火牆位於本機 DNS 伺服器北方的一般部署中，威脅日誌會將本機 DNS 解析程式識別成流量來源，而非實際的受感染主機。Sinkholing 惡意軟體 DNS 查詢可解決此可見性問題，方法是偽裝回應惡意網域上導向的用戶端主機查詢，使得嘗試連線至惡意網域（例如，命令與控制項）的用戶端轉而嘗試連線到預設 Palo Alto Networks sinkhole IP 位址（如果您選擇為自訂網域清單設定 DNS Sinkholing，則連線至所定義 IP 位址）。接著可在流量日誌中輕易識別受感染的主機。



設定 DNS Sinkholing

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

若要啟用 DNS sinkholing，請將預設的反間諜軟體設定檔附加至防火牆安全性政策規則（請參閱設定防毒、反間諜軟體及漏洞保護）。針對所指定 Palo Alto Networks DNS 特徵碼來源中包括的任何網域的 DNS 查詢，會解析至預設 Palo Alto Networks sinkhole IP 位址。IP 位址目前為 IPv4—sinkhole.paloaltonetworks.com 和回送位址 IPv6 位址—::1。這些位址可能隨時變更並可使用內容更新來進行更新。

STEP 1 | 為外部動態清單中的自訂網域清單啟用 DNS sinkholing。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 修改現有的設定檔，或選取一個現有的預設設定檔並加以複製。
3. 輸入設定檔的 **Name**（名稱），然後選取 **DNS Policies**（**DNS** 原則）頁籤。
4. 確認 **default-paloalto-dns** 存在於 **Signature Source**（特徵碼來源）中。
5. （選用）在 **Packet Capture**（封包擷取）下拉式清單中，選取 **single-packet**（單一封包）以擷取工作階段的第一個封包；或選取 **extended-capture**（單一封包）以設定 1-50 個封包。接著您可以使用封包擷取用於進一步分析。

STEP 2 | 確認反間諜軟體設定檔上的 sinkholing 設定。

1. 在 **DNS Policies**（**DNS** 原則）頁籤上，確認 DNS 查詢上的 **Policy Action**（原則動作）為 **sinkhole**。
2. 在「DNS Sinkhole 設定」區段，確認已啟用 **Sinkhole**。為了方便您，預設 Sinkhole IP 位址設定為可以存取 Palo Alto Networks 伺服器。Palo Alto Networks 可透過內容更新來自動重新整理此 IP 位址。

   如果您要將 **Sinkhole IPv4** 或 **Sinkhole IPv6** 位址修改成網路上的本機伺服器或回送位址，請參閱將 Sinkhole IP 位址設定為網路上的本機伺服器。
3. 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

STEP 3 | 將反間諜軟體設定檔附加至安全性原則規則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後選取安全性原則規則。
2. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段啟動時記錄）核取方塊以啟用記錄。
3. 在設定檔組態區段，按一下 **Profile Type**（設定檔類型）以檢視所有的 **Profiles**（設定檔）。在 **Anti-Spyware**（反間諜軟體）下拉式清單中選取新的設定檔。
4. 按一下 **OK**（確定）來儲存原則規則。

STEP 4 | 透過監控防火牆上的活動測試是否已強制執行該原則動作。

1. 選取 **ACC** 並新增 URL 網域作為全域篩選器，以檢視您存取的網域上的威脅活動和封鎖活動。
2. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後依 `(action eq sinkhole)` 篩選以檢視有關遭到 sinkhole 攻擊的日誌。

為自訂網域清單設定 DNS Sinkholing

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

若要為自訂網域清單啟用 DNS Sinkholing，必須建立一個包含網域的外部動態清單、在反間諜軟體設定檔中啟用 sinkhole 動作以及將設定檔附加至安全性原則規則。當用戶端嘗試存取清單中的惡意網域時，防火牆會將封包中的目的地 IP 位址偽造成預設 Palo Alto Networks 伺服器或使用者定義的 IP 位址以實施 sinkholing 攻擊。

對於外部動態清單中包括的每個自訂網域，防火牆會產生以 DNS 為基礎的間諜軟體特徵碼。此特徵碼名稱為 Custom Malicious DNS Query <domain name>，是中度嚴重性類型的間諜軟體；每個特徵碼是網域名稱的 24 位元組雜湊。

如需網域清單項目限制的資訊，請參閱外部動態清單。

STEP 1 | 為外部動態清單中的自訂網域清單啟用 DNS sinkholing。

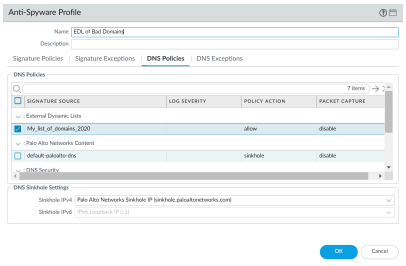
1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 修改現有的設定檔，或選取一個現有的預設設定檔並加以複製。
3. 輸入設定檔的 **Name**（名稱），然後選取 **DNS Policies**（**DNS** 原則）頁籤。
4. 從 **External Dynamic Lists**（外部動態清單）特徵碼來源選取一個 EDL。

   若您已建立以下類型的外部動態清單：***Domain List***（網域清單），您可以在此選取。清單不會顯示可能已建立的 *URL* 或 *IP* 位址類型的外部動態位址。
5. 從反間諜軟體設定檔組態外部動態清單（請參閱將防火牆設定為存取外部動態清單）。**Type**（類型）預設為 **Domain List**（網域清單）。
6. （選用）在 **Packet Capture**（封包擷取）下拉式清單中，選取 **single-packet**（單一封包）以擷取工作階段的第一個封包；或選取 **extended-capture**（單一封包）以設定 1-50 個封包。接著您可以使用封包擷取用於進一步分析。

STEP 2 | 確認反間諜軟體設定檔上的 sinkholing 設定。

1. 在 **DNS Policies**（**DNS** 原則）頁籤上，確認 DNS 查詢上的 **Policy Action**（原則動作）為 **sinkhole**。
2. 在「DNS Sinkhole 設定」區段，確認已啟用 **Sinkhole**。為了方便您，預設 Sinkhole IP 位址設定為可以存取 Palo Alto Networks 伺服器。Palo Alto Networks 可透過內容更新來自動重新整理此 IP 位址。

   如果您要將 **Sinkhole IPv4** 或 **Sinkhole IPv6** 位址修改成網路上的本機伺服器或回送位址，請參閱將 Sinkhole IP 位址設定為網路上的本機伺服器。



3. 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

STEP 3 | 將反間諜軟體設定檔附加至安全性原則規則。

1. 選取 **Policies**（原則） > **Security**（安全性），然後選取安全性原則規則。
2. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段啟動時記錄）核取方塊以啟用記錄。
3. 在設定檔組態區段，按一下 **Profile Type**（設定檔類型）以檢視所有的 **Profiles**（設定檔）。在 **Anti-Spyware**（反間諜軟體）下拉式清單中選取新的設定檔。
4. 按一下 **OK**（確定）來儲存原則規則。

STEP 4 | 測試已強制執行該原則動作。

1. 檢視外部動態清單項目（屬於網域清單），然後存取清單中的網域。
2. 若要監控防火牆上的活動：
   1. 選取 **ACC** 並新增 URL 網域作為全域篩選器，以檢視您存取的網域上的威脅活動和封鎖活動。
   2. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後依 `(action eq sinkhole)` 篩選以檢視有關遭到 sinkhole 攻擊的日誌。

STEP 5 | 確認是否忽略或跳過外部動態清單中的項目。

在防火牆上使用以下 CLI 命令以檢閱清單詳情。

```
request system external-list show type domain name <list_name>
```

例如：

```
request system external-list show type domain name
 My_List_of_Domains_2015 vsys1/EBLDomain:Next update
 at :Thu May 21 10:15:39 2015 Source : https://1.2.3.4/
My_List_of_Domains_2015 Referenced :Yes Valid :Yes Number of
 entries :3 domains:www.example.com baddomain.com qqq.abcedfg.com
```

STEP 6 | （選用）依需要擷取外部動態清單。

若要強制防火牆依需要（而非在下一個重新整理間隔）擷取更新清單（您為外部動態清單定義的 **Repeat**（重複）頻率），請使用以下 CLI 命令：

```
request system external-list refresh type domain name  <list_name>
```

您還可以使用防火牆介面來從 Web 伺服器擷取外部動態清單。

將 Sinkhole IP 位址設定為網路上的本機伺服器

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

依預設，為所有 Palo Alto Networks DNS 特徵碼啟用 sinkholing，sinkhole IP 位址將設為可存取 Palo Alto Networks 伺服器。若您希望將 sinkhole IP 位址設成網路上的本機伺服器，請使用本節中的指示。

您必須獲得 IPv4 與 IPv6 位址，以用作 sinkhole IP 位址，因為惡意軟體在執行 DNS 查詢時，會使用一個或同時使用這兩個通訊協定。DNS Sinkhole 位址必須位於與用戶端主機不同的區域中，以確保當受感染的主機嘗試以 Sinkhole IP 位址啟動工作階段時，系統會將該工作階段路由通過防火牆。

為此，必須保留這個 *Sinkhole* 位址而不需指派給實體主機。您可以選擇性地使用 *honey-pot* 伺服器作為實體主機，以進一步分析惡意流量。

之後的設定步驟會使用下列的範例 *DNS Sinkhole* 位址：

IPv4 DNS sinkhole 位址—*10.15.0.20*

IPv6 DNS sinkhole 位址—*fd97:3dec:4d27:e37c:5:5:5:5*

STEP 1 | 設定 Sinkhole 介面與區域。

來自用戶端主機所在區域的流量必須路由至定義 Sinkhole IP 位址所在的區域，如此便能記錄流量。

為 *Sinkhole* 流量使用專屬區域，因為受感染的主機將會傳送流量至此區域。

1. 選取 **Network**（網路） > **Interfaces**（介面），然後選取要設定成為 Sinkhole 介面的介面。
2. 在 **Interface Type**（介面類型）下拉式清單中選取 **Layer3**。
3. 若要新增 IPv4 位址，請選取 **IPv4** 頁籤，選取 **Static**（靜態），然後按一下 **Add**（新增）。在此範例中，新增 10.15.0.20 作為 IPv4 DNS Sinkhole 位址。
4. 選取 **IPv6** 頁籤，按一下 **Static**（靜態），然後按一下 **Add**（新增）並輸入 IPv6 位址與子網路遮罩。在此範例中，輸入 fd97:3dec:4d27:e37c::/64 作為 IPv6 Sinkhole 位址。
5. 按一下 **OK**（確定）儲存。
6. 若要為 Sinkhole 新增區域，可選取 **Network**（網路） > **Zones**（區域），然後按一下 **Add**（新增）。
7. 輸入區域 **Name**（新增）。

8. 在 **Type**（新增）下拉式清單中選取 **Layer3**。
9. 在 **Interfaces**（介面）區段中，按一下 **Add**（新增），然後新增您剛剛設定的介面。
10. 按一下 **OK**（確定）。

STEP 2 | 啟用 DNS sinkholing。

依預設，會針對所有 Palo Alto Networks DNS 特徵碼啟用 sinkholing。若要變更本機伺服器的 sinkhole 位址，請參閱為自訂網域清單設定 DNS Sinkholing 中的步驟2。

STEP 3 | 編輯安全性原則規則以允許流量從信任區域中的用戶端主機流到不信任區域，藉此包含 Sinkhole 區域作為目的地，並附加反間諜軟體設定檔。

編輯允許流量從信任區域中的用戶端主機流向不信任區域的安全性原則規則，確保識別來自受感染主機的流量。透過在規則上新增 Sinkhole 區域作為目的地，便可允許受感染的用戶端將假的 DNS 查詢傳送至 DNS Sinkhole。

1. 選取 **Policies**（原則） > **Security**（安全性）。
2. 選取允許流量從用戶端主機區域流向不信任區域的現有規則。
3. 在 **Destination**（目的地）頁籤中 **Add**（新增）Sinkhole 區域。這允許用戶端主機流量流向 Sinkhole 區域。
4. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段啟動時記錄）核取方塊以啟用記錄。這會確保當存取不信任或 Sinkhole 區域時，會記錄來自信任區域中用戶端主機的流量。
5. 在設定檔組態區段中，選取您要啟用其 DNS Sinkholing 的反間諜軟體設定檔。
6. 按一下 **OK**（確定）以儲存安全性原則規則，然後按一下 **Commit**（提交）。

STEP 4 | 若要確認您能夠識別受感染的主機，請確認會記錄從信任區域中用戶端主機流向新 Sinkhole 區域的流量。

在此範例中，受感染的用戶端主機是 192.168.2.10，Sinkhole IPv4 位址是 10.15.0.20。

1. 從信任區域中的用戶端主機，開啟命令提示提示，然後執行下列命令：

```
C:\>ping <sinkhole address>
```

下列範例輸出顯示對 10.15.0.2 的 DNS Sinkhole 位址的 ping 請求，並顯示結果，亦即 `Request timed out`，因為在此範例中，未將 Sinkhole IP 位址指派給實體主機：

```
C:\>ping 10.15.0.20 Pinging 10.15.0.20 with 32 bytes of
 data:Request timed out.Request timed out.Ping statistics for
```

```
10.15.0.20:Packets:Sent = 4, Received = 0, Lost = 4 (100%
loss)
```

2. 在防火牆上，選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），然後尋找來源為 192.168.2.10 且目的地為 10.15.0.20 的日誌項目。這將確保流向 Sinkhole IP 位址的流量會周遊防火牆區域。

您可以搜尋和/或篩選日誌，並僅顯示目的地為 *10.15.0.20* 的日誌。做法是按一下 ***Destination***（目的地）欄中的 *IP* 位址 *(10.15.0.20)*，這會將過濾器（*10.15.0.20* 中的 *addr.dst*）新增至搜尋欄位。按一下搜尋欄位右側的套用篩選器圖示來套用篩選器。

STEP 5 | 測試 DNS sinkholing 是否已正確設定。

您正在模擬受感染用戶端主機會在惡意應用程式嘗試自動通報時執行的動作。

1. 尋找防火牆目前的防毒軟體特徵碼資料庫中包括的惡意網域，以測試 sinkholing。
   1. 選取 **Device**（裝置） > **Dynamic Updates**（動態更新），然後在 **Antivirus**（防毒）區段中按一下目前所安裝防毒資料庫的 **Release Notes**（版本資訊） 連結。您也可以尋找防毒版本資訊，其中列有 Palo Alto Networks 支援網站上的 Dynamic Updates（動態更新）下的增量特徵碼更新。
   2. 在版本資訊的第二欄中，找到有網域延伸的行項目（例如 .com、.edu 或 .net）。左欄將顯示網域名稱。例如在 1117-1560 版的防毒軟體中，左欄中包括名為 「tbsbana」的項目，右欄則列出「net」。

      以下顯示版本資訊中此行項目的內容：

      ```
      conficker:tbsbana 1 variants: net
      ```
2. 從用戶端主機開啟命令提示。
3. 對您識別為已知惡意網域的 URL 執行 NSLOOKUP。

   例如，使用 URL `track.bidtrk.com`：

   ```
   C:\>nslookup track.bidtrk.com Server: my-local-
   dns.local Address:10.0.0.222 Non-authoritative
    answer:Name: track.bidtrk.com.org Addresses:
    fd97:3dec:4d27:e37c:5:5:5:510.15.0.20
   ```

   在輸出中，請注意系統已使用我們設定的 Sinkhole IP 位址 (10.15.0.20) 來偽造對惡意網域的 NSLOOKUP。因為網域符合惡意的 DNS 特徵碼，所以已執行 Sinkhole 動作。
4. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後尋找對應的威脅日誌項目，以確認在 NSLOOKUP 要求上執行了正確的動作。
5. 對 **`track.bidtrk.com`** 執行 ping，這將對 Sinkhole 位址產生網路流量。

查看嘗試連線至惡意網域的受感染主機

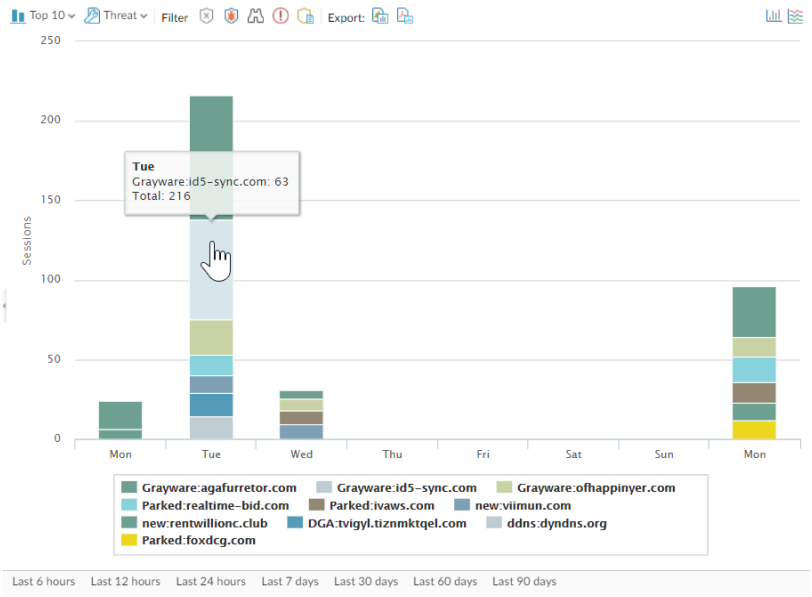
我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

在您設定 DNS Sinkholing 並確認流向惡意網域的流量會前往 Sinkhole 位址後，您應定期監控前往 Sinkhole 位址的流量，藉此追蹤受感染的主機並消除威脅。

使用 App Scope 識別受感染的用戶端主機。

1. 選取 **Monitor**（監控） > **App Scope**，然後選取 **Threat Monitor**（威脅監控）。
2. 按一下顯示頁面頂端的 **Show spyware**（顯示間諜軟體）按鈕。
3. 選取時間範圍。

   下列螢幕擷取畫面顯示三個可疑 DNS 查詢的實例，這些實例是在測試用戶端主機在已知惡意網域上執行 NSLOOKUP 時產生的。按一下圖表可看到事件的詳細資料。



設定自訂報告以識別所有已傳送流量至 Sinkhole IP 位址 (在此範例中為 10.15.0.20) 的用戶端主機。

轉送至 *SNMP* 管理員、*Syslog* 伺服器和/或 *Panorama*，以對這些事件啟用警示。

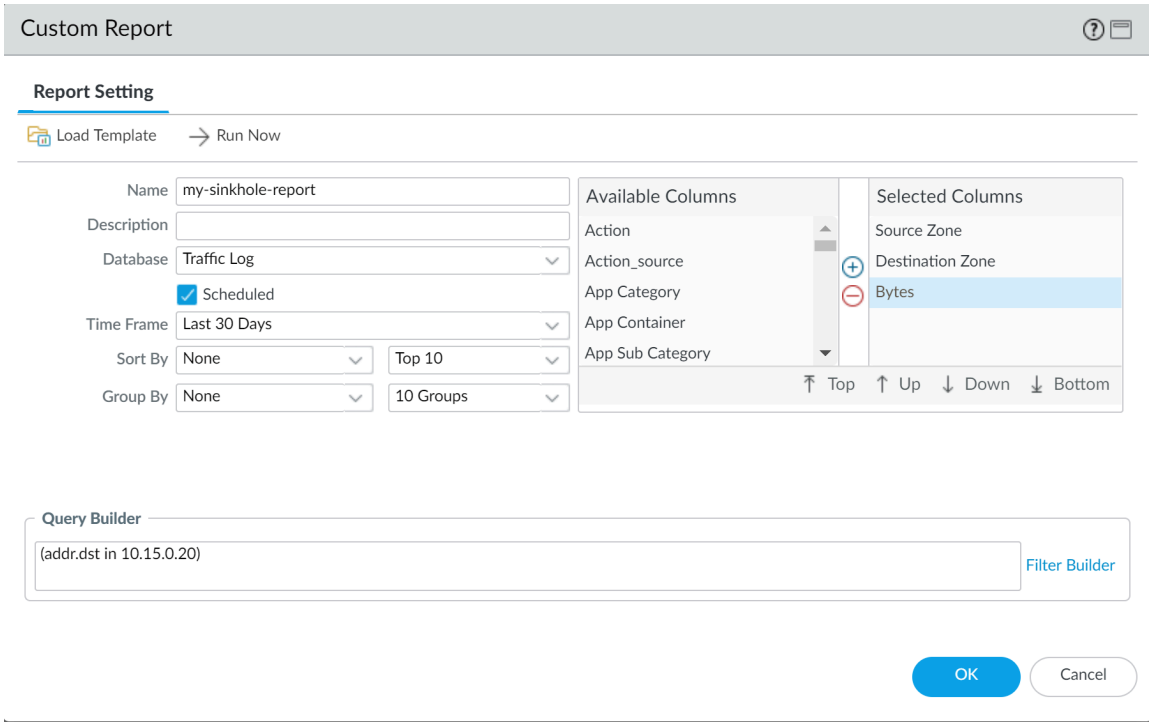
在此範例中，受感染的用戶端主機對列在 Palo Alto Networks DNS 特徵碼資料庫中的已知惡意網域執行 NSLOOKUP。發生此狀況時，系統會將查詢傳送至本機 DNS 伺服器，然後轉送要求經過防火牆到外部 DNS 伺服器。設有反間諜軟體設定檔的防火牆安全性原則會比對 DNS 特徵碼資料庫的查詢，然後使用 Sinkhole 位址 10.15.0.20 與 fd97:3dec:4d27:e37c:5:5:5:5 來偽造

回覆。用戶端會嘗試啟動工作階段，且流量日誌會記錄活動及來源主機和目的地位址，現在會將工作階段導向至偽造的 Sinkhole 位址。

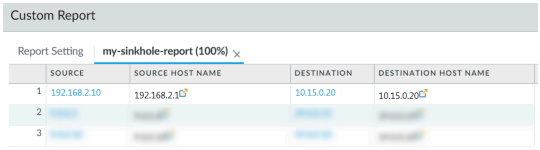
檢視防火牆上的流量日誌可讓您識別任何正將流量傳送至 Sinkhole 位址的用戶端主機。在此範例中，日誌會顯示來源位址 192.168.2.10 傳送了惡意 DNS 查詢。接著會尋找主機並予以清除。若沒有 DNS Sinkhole 選項，管理員只會將本機 DNS 伺服器視為執行查詢的系統，且看不到受感染的用戶端主機。如果您嘗試使用「Sinkhole」動作執行威脅日誌報告，則日誌會顯示本機 DNS 伺服器，而非受感染的主機。

1. 選取 **Monitor**（監控） > **Manage Custom Reports**（管理自訂報告）.
2. 按一下 **Add**（新增），並設定報告的 **Name**（名稱）。
3. 定義自訂報告以將流量擷取至 Sinkhole 位址，如下所示：
   - 資料庫—選取 **Traffic Log**（流量日誌）。
   - 已排程—啟用 **Scheduled**（已排程），報告將每晚執行。
   - **Time Frame**（時間範圍）—30 天
   - 選取的欄—選取**Source address**（來源位址）或 **Source User**（來源使用者）（如果您已設定 User-ID），這將識別報告中受感染的用戶端主機，並選取 **Destination address**（目的地位址），這將會是 #inkhole 位址。
   - 在畫面底端的區段中，為前往 Sinkhole 位址 (在此範例中為 10.15.0.20) 的流量建立自訂查詢。您可以在 **Query Builder**（查詢建立器）視窗 (**addr.dst in 10.15.0.20**) 中輸入目的地位址，或在每一欄中選取下列項目，然後按一下 **Add**（新增）：Connector =

and，Attribute = Destination Address，Operator = in，Value = 10.15.0.20。按一下 **Add**（新增）以新增查詢。



4. 按一下 **Run Now**（立即執行）以執行報告。報告會顯示將流量傳送至 Sinkhole 位址的所有用戶端主機，這表示這些主機最有可能受到感染。現在您可以追蹤主機，並檢查主機是否有間諜軟體。



5. 若要檢視已執行的已排程報告，請選取 **Monitor**（監控） > **Reports**（報告）。

自訂特徵碼

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

您可建立自訂威脅特徵碼以偵測和封鎖特定流量。當防火牆由 Panorama 管理伺服器管理時，ThreatID 會對應到防火牆上相應的自訂威脅，以使防火牆能夠產生填充了已設定自訂 ThreatID 的威脅日誌。瀏覽我們的自訂應用程式和威脅特徵碼指南，瞭解更多資訊。

監控進階 Threat Prevention

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

Palo Alto Networks 提供了多種選項來監控進階 Threat Preventio 處理的活動，以適應依賴進階 Threat Prevention 和相關資料的一系列產品情報擷取。根據產品平台，您可以存取高階儀表板，這些儀表板也提供 DNS 要求統計資料和使用趨勢，其中包括網路活動脈絡，以及特定使用者的 DNS 要求詳細資料。

您也可以檢視進階 Threat Prevention 如何與其他 Palo Alto Networks 應用程式和安全服務整合來保護貴組織免受威脅，並同時透過 Strata Cloud Manager 控管中心取得高階檢視，以掌握您部署的整體運作健康情況。控管中心可作為您的 NetSec 首頁，並透過具有多個資料面向的互動式視覺化儀表板提供網路運作健康情況、安全性及效率的全面摘要，以便您輕鬆快速地進行評估。

若要取得網路活動的概觀檢視，您可以查看儀表板，以便掌握網路整體威脅管理資料以及各種 DNS 趨勢。每個儀表板卡片都以圖形報告格式，提供了威脅如何影響網路的獨特檢視。這樣可以根據應用程式、使用者以及強制執行組織政策的安全規則，快速了解受威脅影響最大的實體。

Palo Alto Networks 提供了多種監控威脅活動的方法：

- Strata Cloud Manager 控管中心
- 檢閱威脅日誌
- 檢視進階 Threat Prevention 報告
- 監控封鎖的 IP 位址
- 進一步瞭解威脅特徵碼
- 根據威脅類別建立自訂報告

檢閱威脅日誌

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

威脅類別將不同類型的威脅特徵碼進行了分類，以幫助您瞭解威脅特徵碼偵測到的事件，並在事件之間建立連線。威脅類別是更廣泛威脅特徵碼類型的子集：間諜軟體、弱點、防毒。威脅日誌項目顯示了所記錄的每個事件的 **Threat Category**（威脅類別）。

您可以瀏覽、搜尋和查看偵測到威脅時自動產生的進階 Threat Prevention 日誌。通常，這包括 Threat Prevention 功能（包括內嵌 ML）分析的任何合格威脅特徵碼匹配，除非專門設定為無日誌嚴重性等級。日誌項目提供有關事件的許多詳細資訊，包括威脅層級及威脅性質（如果適用的話）。

- Strata Cloud Manager
- PAN-OS 和 Panorama

檢閱威脅日誌 (Cloud Management)

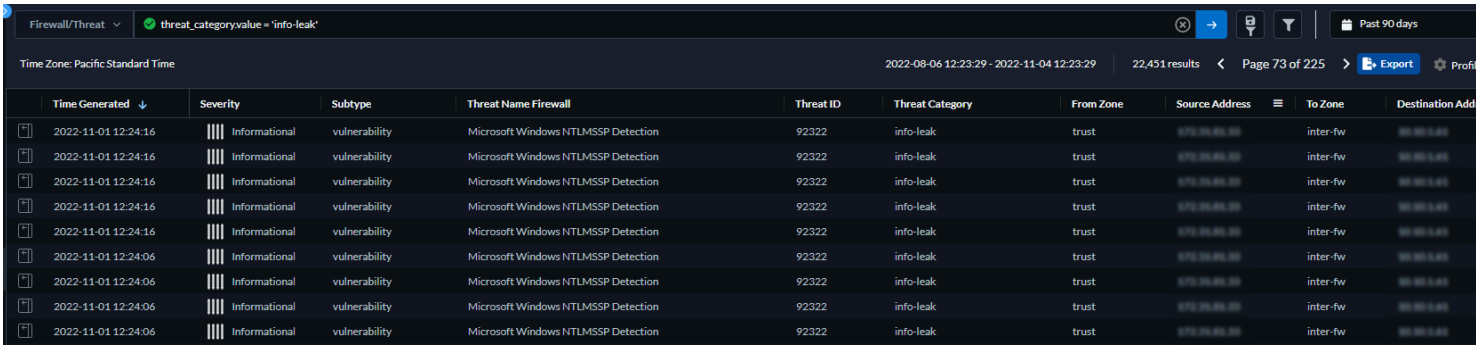
STEP 1 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager。

如需詳細瞭解如何使用活動儀表板，請參閱日誌檢視器。

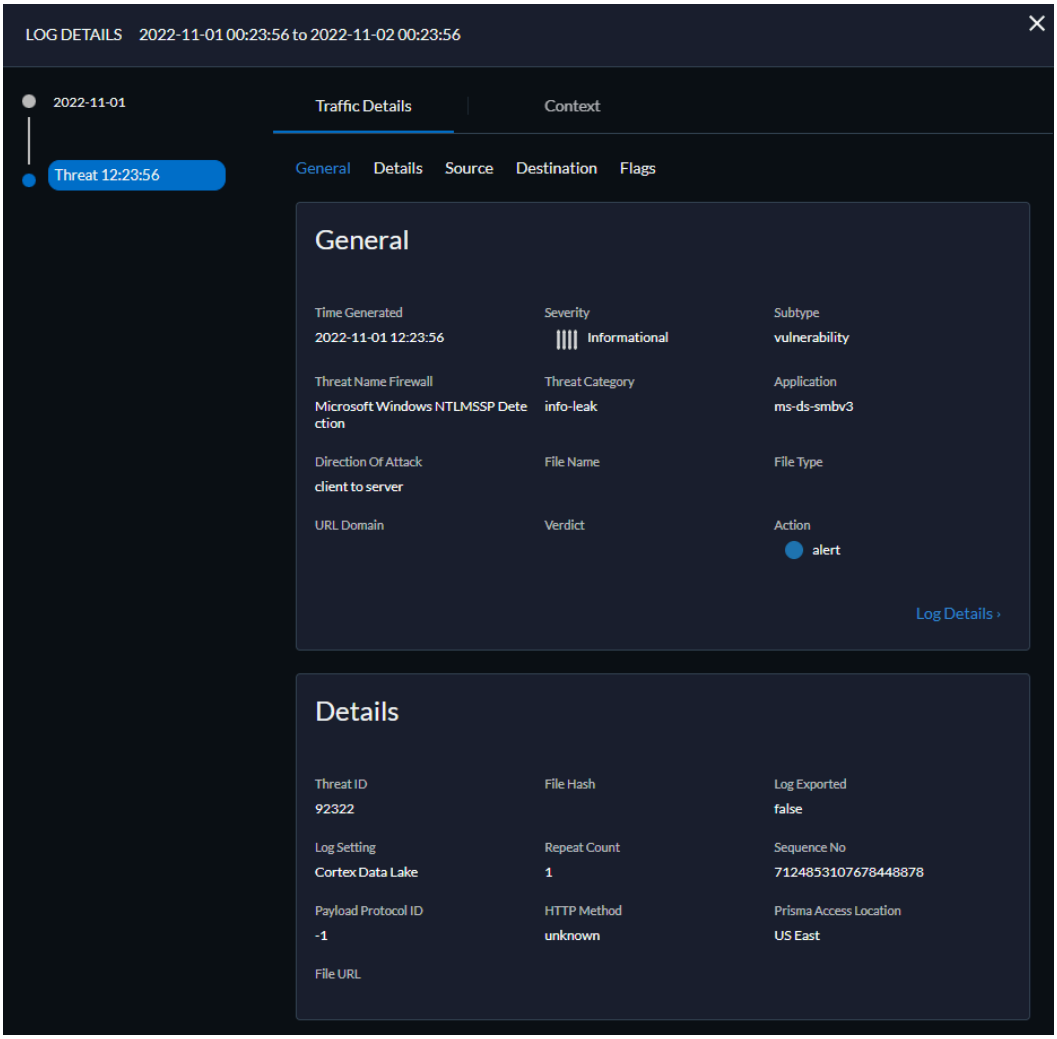
STEP 2 | 根據 Prisma Access 中的 **Threat Category**（威脅類別）或 **Subtype**（子類別）篩選威脅日誌。

1. 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。
2. 將要搜尋的日誌類型變更為 **Threat**（威脅）。
3. 依照「防毒」、「反間諜軟體」或「弱點保護」設定檔（分別是**antivirus**（防毒）、**spyware**（反間諜軟體）和 **vulnerability**（弱點）），使用威脅特徵碼子類型，或根據使用查詢建置器的威脅類別，來建立搜尋篩選器。例如，您可以使用 `sub_type.value = 'spyware'` 來檢視已判定為間諜軟體的威脅日誌。若要搜尋其他子類型，請將上述範例中的間諜軟體取代為其他支援的子類型（**vulnerability**（弱點）或 **spyware**（間諜軟體））。您也可以使用下列查詢 `threat_category.value = 'info-leak'`，根據特定 **Threat Category**（威脅類別）進行搜尋，例如資訊洩漏弱

點。如需您可以使用的有效類別清單，請參閱威脅特徵碼類別。根據需要調整搜尋條件，包括其他查詢參數（例如嚴重性級別和動作）以及日期範圍。



4. 篩選器設定完成後執行查詢。
5. 從結果選擇一個日誌項目，查看日誌詳細資訊。



6. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資料）窗格中。威脅的其他相關詳細資訊會顯示在相應視窗。

STEP 3 | 依使用內嵌雲端分析（間諜軟體）偵測到的威脅 [類別] 篩選威脅日誌。

以 *HTTP* 為基礎的 *C2* 流量，最初以威脅名稱內嵌雲端分析的 *HTTP* 命令和控制流量偵測分類，並且與多個威脅 *ID* 相關聯，現在分為三個唯一的威脅名稱，以對應唯一的威脅 *ID*，並更準確地描述進階 *Threat Prevention* 所做的偵測：***Evasive HTTP C2 Traffic Detection***（規避性 ***HTTP C2*** 流量偵測）（特徵碼 *ID*：*89950*），***Evasive Cobalt Strike C2 Traffic Detection***（規避性 ***Cobalt Strike C2*** 流量偵測）（特徵碼 *ID*：*89955*、*89956* 和 *89957*）和***Evasive Empire C2 Traffic Detection***（規避性 ***Empire C2*** 流量偵測）（威脅 *ID*：*89958*）。

2023 年 *12* 月 *11* 日之前產生的 *HTTP* 型 *C2* 流量日誌將繼續以威脅名稱內嵌雲端分析 *HTTP* 命令和控制流量偵測分類。

1. 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。
2. 將要搜尋的日誌類型變更為 **Threat**（威脅）。
3. 使用內嵌雲端分析專用的威脅類別建立搜尋篩選器（間諜軟體）：`threat_category.value = 'inline-cloud-c2'`。您可以透過交互參照與特定 C2 類型對應的威脅 ID 值，進一步限制搜尋。例如 `threat_category.value = 'inline-cloud-c2' AND Threat ID = 89958`，其中 89958 表示規避性 empire C2 流量的威脅 ID。
4. 選取日誌項目以檢視偵測到的 C2 威脅的詳細資料。
5. 威脅 **Category**（類別）顯示在日誌詳細資料的 **General**（一般）窗格之下。使用內嵌雲端分析偵測到的 C2 威脅具有威脅類別 inline-cloud-c2。您可以在 **Details**（詳細資料）窗格中，交互參照威脅 **ID** 值，以判斷偵測到的特定 C2 類型。

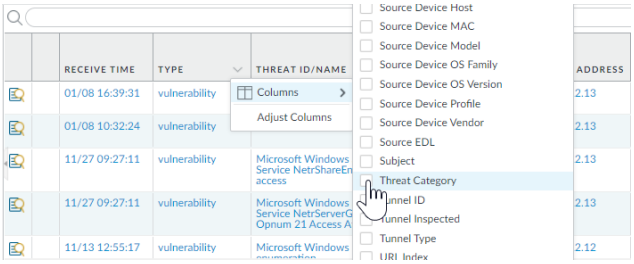
STEP 4 | 依使用內嵌雲端分析（弱點）偵測到的威脅 [類別] 篩選威脅日誌。

1. 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。
2. 將要搜尋的日誌類型變更為 **Threat**（威脅）。
3. 使用內嵌雲端分析專用的威脅類別建立搜尋篩選器（弱點）：`threat_category.value = 'inline-cloud-exploit'`。
4. 選取日誌項目，以檢視偵測到的命令注入和 SQL 注入弱點詳細資料。內嵌入侵（SQL 注入）威脅的 ID 為 99950，而內嵌入侵（命令注入）威脅的 ID 為 99951。

檢閱威脅日誌 (NGFW (Managed by PAN-OS or Panorama))

按威脅類別篩選威脅日誌。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。
2. 新增 Threat Category（威脅類別）欄，以便檢視每個日誌項目的威脅類別：



3. 根據威脅類別篩選：
   - 使用日誌查詢產生器，使用威脅類別 **Attribute**（屬性）新增篩選器，然後在 **Value**（值）欄位中，輸入威脅類別。
   - 選取任何日誌項目的威脅類別，以將該類別新增至篩選器：

依威脅特徵碼類型篩選威脅日誌。

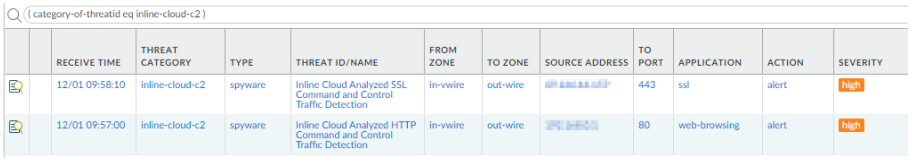
1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。
2. 新增 **Type**（類型）欄（如果不存在），以便您可以檢視每個日誌項目的威脅特徵碼類別：
3. 若要根據特徵碼類型篩選：
   - 使用日誌查詢建置器來新增具有威脅特徵碼類別的 **Attribute**（屬性）篩選器，並在 **Value**（值）欄位中輸入威脅特徵碼類型。您可以從 **vulnerability**（弱點）、**virus**（病毒）和 **spyware**（間諜軟體）中選取，這與您的弱點保護、防毒和反間諜軟體安全性設定檔所處理的特徵碼相對應。
   - 選取任何日誌項目的 **Type**（類型），將該安全威脅特徵碼類型新增至篩選器。您也可以使用篩選器和威脅特徵碼類型手動建立查詢。

依使用內嵌雲端分析（間諜軟體）偵測到的威脅 [類別] 篩選威脅日誌。

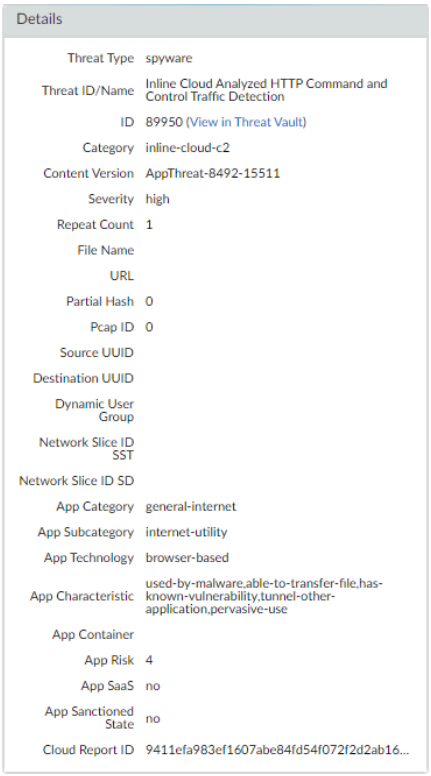
以 *HTTP* 為基礎的 *C2* 流量，最初以威脅名稱內嵌雲端分析的 *HTTP* 命令和控制流量偵測分類，並且與多個威脅 *ID* 相關聯，現在分為三個唯一的威脅名稱，以對應唯一的威脅 *ID*，並更準確地描述進階 *Threat Prevention* 所做的偵測：***Evasive HTTP C2 Traffic Detection***（規避性 ***HTTP C2*** 流量偵測）（特徵碼 *ID*：*89950*），***Evasive Cobalt Strike C2 Traffic Detection***（規避性 ***Cobalt Strike C2*** 流量偵測）（特徵碼 *ID*：*89955*、*89956* 和 *89957*）和***Evasive Empire C2 Traffic Detection***（規避性 ***Empire C2*** 流量偵測）（威脅 *ID*：*89958*）。

如果您未安裝更新內容或正在檢閱 *2023* 年 *12* 月 *11* 日（內容更新的發行日期）之前產生的 *HTTP* 型 *C2* 流量日誌，則所有以 *HTTP* 為基礎的 *C2* 流量將繼續以威脅名稱內嵌雲端分析的 *HTTP* 命令和流量控制偵測分類。

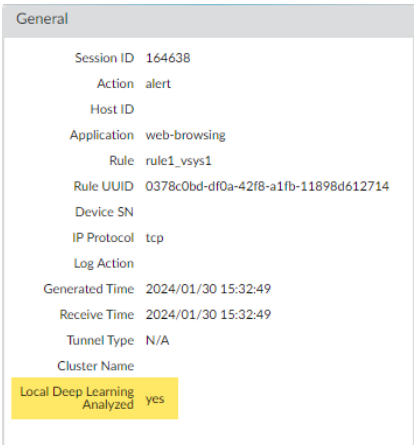
1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。您可以根據威脅的特性篩選日誌。請考慮下列範例：
   - 使用 `( category-of-threatid eq inline-cloud-c2 )` 進行篩選，以檢視已使用進階 Threat Prevention 的內嵌雲端分析機制分析的 C2 威脅日誌。
   - 您可以透過交互參照與特定 C2 類型對應的威脅 ID 值，進一步限制搜尋。例如，`( category-of-threatid eq inline-cloud-c2 ) and (name-of-threatid eq 89958)`，其中 89958 表示規避性 empire C2 流量的威脅 ID。
   - 使用 `(local_deep_learning eq yes)` 進行篩選，以檢視已使用進階 Threat Prevention 的本機深度分析機制分析的威脅日誌。



2. 選取日誌項目以檢視偵測到的 C2 威脅的詳細資料。
3. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資料）窗格下。使用內嵌雲端分析偵測到的 C2 威脅具有威脅類別 inline-cloud-c2。您可以交互參考威脅 **ID** 值，以判斷偵測到的特定 C2 類型。



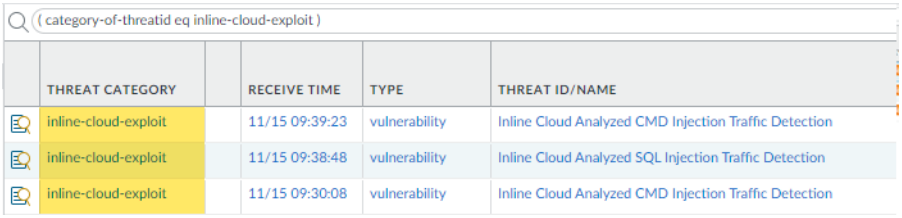
4. 如果使用本機深度學習分析威脅，則 **Local Deep Learning Analyzed**（本機深度學習分析）欄位表示「是」。



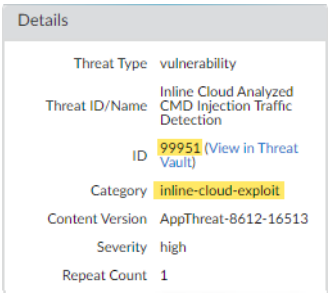
監控防火牆上的活動，以查找已使用內嵌雲端分析（弱點）偵測到的弱點入侵。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）並依 `( category-of-threatid eq inline-cloud-exploit )` 進行篩選，以檢視已使用進階 Threat

Prevention 的內嵌雲端分析機制分析的日誌。內嵌入侵（SQL 注入）威脅的 ID 為 99950，而內嵌入侵（命令注入）威脅的 ID 為 99951。

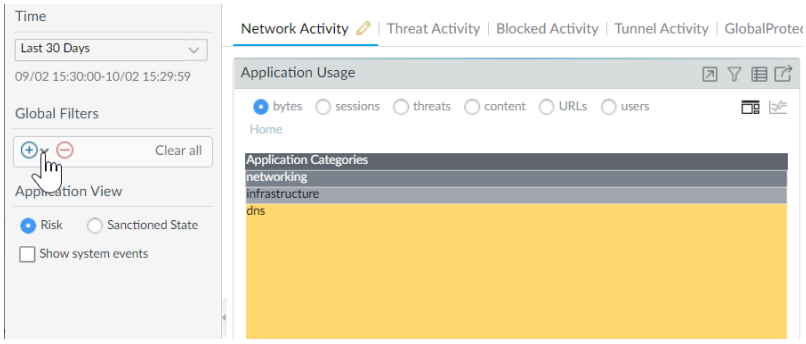


2. 選取日誌項目以檢視弱點入侵的詳細資料。
3. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資料）窗格下。使用內嵌雲端分析偵測到的弱點入侵具有威脅類別 inline-cloud-exploit。

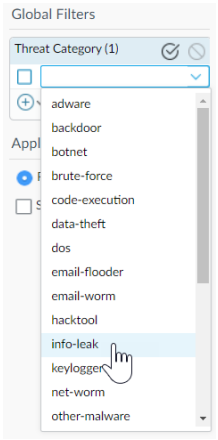


按威脅類別篩選 ACC 活動。

1. 選取 **ACC**，然後將威脅類別新增為全域篩選條件：



2. 選取威脅類別，以篩選所有 ACC 頁籤。



檢視進階 Threat Prevention 報告

我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

「進階 Threat Prevention 報告」可透過威脅資料庫 API 取得，其中包含詳細的分析和偵測資訊，以及有關交易、工作階段和其他相關程序的資訊。根據處理檔案的防火牆上設定的工作階段資訊，以及 JSON 格式的檔案的分析詳細資料，報表包含下表中所描述的部分或全部資訊。

NGFW 無法透過 *PAN-OS* 直接存取報表；您必須改為參考與威脅日誌相關聯的 *cloud_reportid*，並使用威脅資料庫 *API* 來搜尋和擷取報表。

對於 *Prisma Access*（透過 Strata Cloud Manager），可從日誌檢視器 (檢閱威脅日誌) 檢視報表。具有產生的進階 *Threat Prevention* 報表的日誌項目在 ***Cloud ReportID***（雲端報表 ***ID***）欄下的報表 *ID* 值旁邊有一個下載連結。

報告標題	說明
一般資訊	包含處理威脅的防火牆/安全平台的相關資訊。 • 包含進階威脅報告資料的雲端報告 ID 號碼。 • 建立報告期間可能產生的錯誤訊息。
PAN-OS 資訊	包含處理威脅的防火牆/安全平台的相關資訊。 • 防火牆介面 (IPv4/IPv6) • 內容套件版本 • 防火牆主機名稱 • 防火牆型號 • 序號 • PAN-OS 版本
工作階段資訊	在流量周遊轉送威脅的防火牆/安全平台時，包含以流量為基礎的工作階段資訊。

報告標題	說明
	以下為可用選項： • 來源 IP • 來源連接埠 • 目的地 Ip • 目的地連接埠 • 工作階段 ID • 工作階段時間戳記 • 有效負載類型
交易資料	交易資料提供有效負載詳細資料的概觀，並包含偵測服務報告。 以下為可用選項： • 交易 ID • 有效負載的 SHA256 雜湊
偵測服務結果	當進階 Threat Prevention 雲端執行威脅分析時，此區段會包含顯示分析結果的項目。這包括偵測服務報告，其中還提供了所使用的 MITRE ATT&CK® 分類技術，以及有效負載詳細資料。 Empire C2 框架的命令和控制偵測會顯示其他關聯資訊。這包括在不同工作階段中發生的攻擊暫存和命令（惡意入侵後）階段產生的報告。 下列資訊項目可用： • 攻擊說明—說明 C2 攻擊的特性。 • 攻擊詳細資料—指出 Empire C2 攻擊的階段，並描述伺服器與用戶端之間的交換。 • 攻擊證據—列出與已知 Empire C2 一致的行為和動作。 使用 ***Inline Cloud Analyzed HTTP Command and Control Traffic Detection***（內嵌雲端分析 ***HTTP*** 命令和控制流量偵測）分析引擎中的子模組偵測器，來偵測以 *Empire C2* 為基礎的，並具有唯一威脅 *ID 89958*。

監控封鎖的 IP 位址

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

防火牆將保留其封鎖的來源 IP 位址封鎖清單。當防火牆封鎖來源 IP 位址時，例如當您設定任何原則規則時，防火牆將在這些封包使用 CPU 或封包緩衝資源之前封鎖流量：

- 設定了 **Protect**（保護）動作的分類 DoS 保護原則規則（分類 DoS 保護原則規則指定了與來源 IP 位址、目的地 IP 位址或來源及目的地 IP 位址配對相符的輸入連線，並與分類 DoS 保護設定檔關聯，如對新工作階段流量的 DoS 保護中所述）。
- 使用了漏洞保護設定檔的安全性原則規則

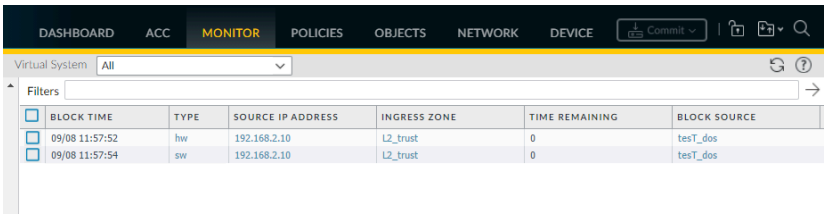
PA-3200 Series、PA-5200 Series、PA-5400 Series（PA-5450 除外）和 PA-7000 Series 防火牆均支援硬體 IP 位址封鎖。

您可以檢視封鎖清單，獲取封鎖清單上某個 IP 位址的詳細資訊，或者檢視硬體和軟體封鎖的位址計數。如果您認為某個 IP 位址不應被封鎖，可將其從清單中刪除。您不能變更清單上位址詳細資訊的來源。您還可以變更硬體封鎖 IP 位址的持續時間。

檢視封鎖清單項目。

1. 選取 **Monitor**（監控） > **Block IP List**（封鎖 **IP** 清單）。（監控 > 封鎖 IP 清單）。

   封鎖清單中的項目在 Type（類型）欄中指示了是被硬體 (hw) 還是軟體 (sw) 封鎖。
2. 在畫面底部檢視：
   - **Total Blocked IPs**（封鎖的 **IP** 總數）以及防火牆支援封鎖的 IP 位址數目。
   - 防火牆已使用封鎖清單容量的百分比。
3. 若要篩選所顯示的項目，可在欄中選取值（將在 **Filters**（篩選）欄位建立篩選器），然後套用篩選器 (→)。否則，防火牆將顯示前 1000 個項目。
4. 輸入 **Page**（頁碼），或按一下畫面底部的箭頭，快速跳轉項目頁面。
5. 若要檢視封鎖清單上某個位址的詳細資料，將滑鼠暫留在來源 IP 位址上，然後按一下向下箭頭連結。按一下 **Who Is** 連結，將顯示該位址的 Network Solutions Who Is 資訊。



刪除封鎖清單項目。

如果您確定某個 *IP* 位址不應被封鎖，可刪除相應項目。然後再修訂造成防火牆封鎖該位址的原則規則。

1. 選取 **Monitor**（監控） > **Block IP List**（封鎖 **IP** 清單）。（監控 > 封鎖 IP 清單）。
2. 選取一個或多個項目，然後按一下 **Delete**（刪除）。
3. （選用）選取 **Clear All**（全部清除），可從清單移除所有項目。

停用或重新啟用硬體 IP 位址封鎖，以進行疑難排解。

停用硬體 *IP* 位址封鎖後，防火牆仍將執行您所設定的任何軟體 *IP* 位址封鎖。

```
> set system setting hardware-acl-blocking [enable | disable]
```

為了節省 *CPU* 與封包緩衝資源，將硬體 *IP* 位址封鎖保持啟用，除非 *Palo Alto Networks* 技術支援人員要求您停用（例如在對流量進行偵錯時）。

在封鎖清單上調整硬體保持封鎖 IP 位址的秒數（範圍為 1-3600；預設值為 1）。

```
> set system setting hardware-acl-blocking duration <seconds>
```

使硬體封鎖清單項目的持續時間短於軟體封鎖清單項目，可降低超出硬體封鎖能力的可能性。

將用於尋找 IP 位址詳細資訊的預設網站從 Network Solutions Who Is 變更為其他網站。

```
# set deviceconfig system ip-address-lookup-url <url>
```

檢視硬體和軟體封鎖的來源 IP 位址計數，例如查看攻擊速率。

檢視硬體封鎖表和封鎖清單上由硬體和軟體封鎖的 IP 位址項目總數：

```
> show counter global name flow_dos_blk_num_entries
```

檢視硬體封鎖表上由硬體封鎖的 IP 位址項目計數：

```
> show counter global name flow_dos_blk_hw_entries
```

檢視封鎖清單上由軟體封鎖的 IP 位址項目計數：

```
> show counter global name flow_dos_blk_sw_entries
```

檢視 PA-7000 系列防火牆上每個插槽的封鎖清單資訊。

```
> show dos-block-table software filter slot <slot-number>
```

進一步瞭解威脅特徵碼

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

防火牆威脅日誌中記錄了防火牆根據威脅特徵碼偵測的所有威脅（設定防毒、反間諜軟體及漏洞保護），ACC 將顯示網路上前幾大威脅的概覽。防火牆記錄的每個事件都包含有用於識別相關威脅特徵碼的 ID。

您可以使用在威脅日誌或 ACC 項目中找到的威脅 ID：

- 輕鬆檢查某個威脅特徵碼是否被設定為安全性政策的例外項 (建立威脅例外)。
- 尋找特定威脅的最新威脅保存庫資訊。由於威脅保存庫與防火牆整合在一起，您可以直接在防火牆內容中檢視威脅詳細資料，或在新瀏覽器視窗中針對防火牆記錄的威脅啟動威脅保存庫搜尋。

如果已停用特徵碼，則特徵碼 *UTID* 可能會重新用於新特徵碼。

檢閱內容更新版本資訊，瞭解有關新特徵碼和已停用特徵碼的通知。在以下情況下，可能會停用特徵碼：特徵碼偵測到的活動已不再被攻擊者使用，特徵碼產生了重大誤報，或特徵碼與其他類似特徵碼合併為單一特徵碼（特徵碼最佳化）。

STEP 1 | 確認防火牆是否已連線至威脅保存庫。

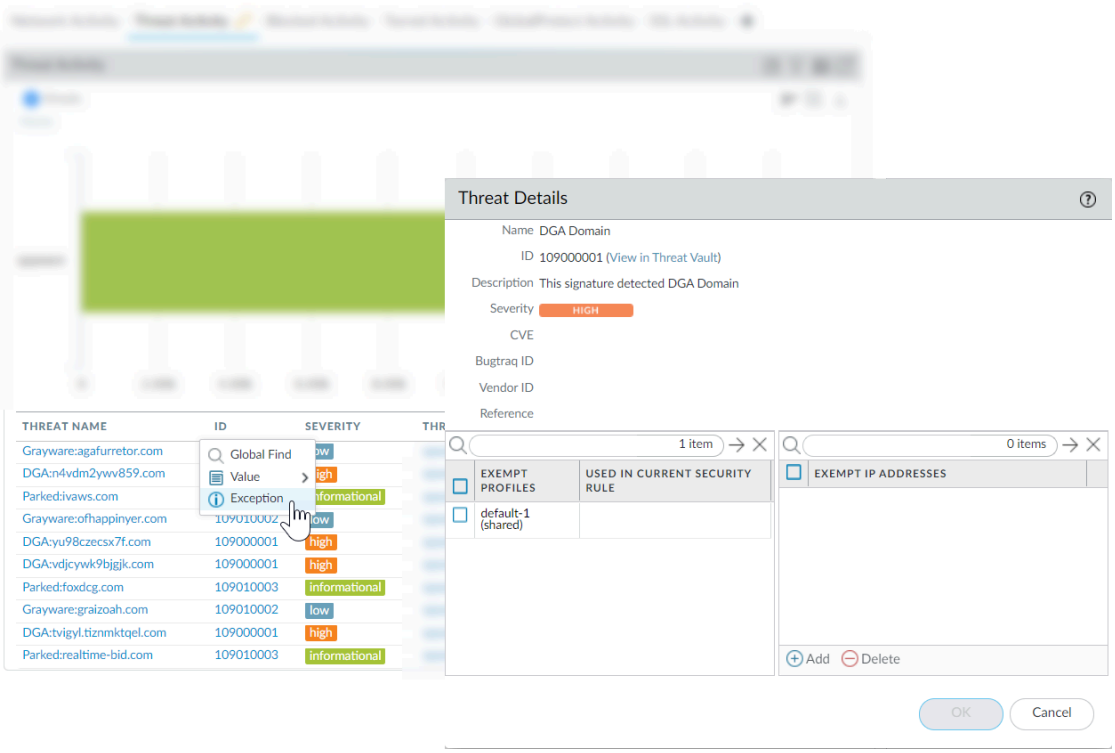
選取 **Device**（裝置） > **Setup**（設定） > **Management**（管理），然後編輯 **Logging and Reporting**（日誌記錄與報告）設定以 **Enable Threat Vault Access**（啟用威脅保存庫存取）。預設會啟用威脅保存庫存取。

STEP 2 | 尋找防火牆所偵測之威脅的威脅 ID。

- 若要查看防火牆根據威脅特徵碼偵測的每個威脅事件，可選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。您可以在 ID 欄中找到所列威脅項目的 ID，或者選取日誌項目以檢視日誌詳細資料，包括威脅 ID。
- 若要查看網路上前幾大威脅的概覽，可選取 **ACC** > **Threat Activity**（威脅活動），然後在 Threat Activity（威脅活動）Widget 中查看。ID 欄中顯示了每個威脅的威脅 ID。
- 若要查看您可以設定為威脅例外（即防火牆將不對該威脅強制執行為特定威脅特徵碼定義的預設動作）的威脅詳細資料，可選取 **Objects**（物件） > **Security Profiles**（系統設定檔） > **Anti-Spyware/Vulnerability Protection**（反間諜軟體/漏洞保護）。**Add**（新增） 或修改設定檔，然後按一下 **Exceptions**（例外） 索引標籤以檢視所設定的例外。如果未設定例外，則可以篩選威脅特徵碼或選取 **Show all signatures**（顯示所有特徵碼）。

STEP 3 | 將滑鼠暫留在 **Threat Name**（威脅名稱）或威脅 **ID** 上，開啟下拉式清單，然後按一下 **Exception**（例外），檢閱威脅詳細資料以及防火牆將對威脅強制執行的動作。

例如，進一步瞭解 ACC 上列出的前幾大威脅：



STEP 4 | 檢閱威脅的最新 **Threat Details**（威脅詳細資料），並根據威脅 ID 啟動威脅保存庫搜尋。

- 所顯示的威脅詳細資料包括威脅的最新威脅保存庫資訊、您可用於進一步瞭解威脅的資源以及與該威脅關聯的 CVE。
- 選取 **View in Threat Vault**（在威脅保存庫中檢視）以在新視窗中開啟威脅資料庫搜尋，並查閱 Palo Alto Networks 威脅資料庫中關於此威脅特徵碼的最新資訊。

STEP 5 | 檢查某個威脅特徵碼是否被設定為安全性原則的例外項。

- 如果 **Used in current security rule**（已在目前的安全性規則中使用）欄已清除，防火牆將對威脅強制執行所建議的預設特徵碼動作（例如封鎖或警示）。
- **Used in current security rule**（已在目前的安全性規則中使用）欄中的勾選記號表示已設定安全性原則規則，根據關聯的 **Exempt Profiles**（豁免設定檔）設定對威脅強制執行非預設動作。

Used in security rule（已在安全性規則中使用）欄並不會指示是否已啟用安全性原則規則，僅指示是否為安全性原則規則設定了威脅例外。選取 ***Policies***（原則）> ***Security***（安全性），以檢查所示的安全性原則規則是否已啟用。

STEP 6 | **Add**（新增）要篩選威脅例外的 IP 位址，或檢視現有的 **Exempt IP Addresses**（豁免 **IP** 位址）。

設定豁免 IP 位址，以僅在相關工作階段有相符的來源或目的地 IP 位址時強制執行威脅例外；對於其他工作階段，將對威脅強制執行預設特徵碼動作。

根據威脅類別建立自訂報告

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 Threat Prevention（支援增強功能）或 Threat Prevention 授權

您可以在防火牆上建立自訂報告，以根據您想要擷取和分析的屬性或關鍵資訊，（按需求）產生或排程（每晚）報告。

根據威脅類別建立自訂報告，以接收關於防火偵測到的特定類型威脅的資訊。

1. 選取 **Monitor**（監控） > **Manage Custom**（管理自訂）報告，以新增新的自訂報告或修改現有報告。
2. 選擇要用作自訂報告來源的 **Database**（資料庫）—在這種情況下，從兩種資料庫來源（摘要資料庫和詳細日誌）中的任何種中選取 **Threat**（威脅）。摘要資料庫資料經過壓縮，以便在產生報告時更快地回應。詳細日誌則需要更長時間才能產生，但能夠提供每個日誌項目的詳細、完整資料。
3. 在查詢產生器中，新增屬性為 **Threat Category**（威脅類別）的報告篩選器，然後在 Value（值）欄位中，選取報告將基於的威脅類別。
4. 若要測試新報告設定，可按一下 **Run Now**（立即執行）。
5. 按一下 **OK**（確定）儲存報告。