paloalto TECHDOCS

進階 DNS 安全性管理

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

November 23, 2022

Table of Contents

關於 DNS 安全性訂閱服務

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

Palo Alto Networks® 透過兩種安全性訂閱選項，針對基於 DNS 的威脅提供專門整合式保護：DNS 安全性與進階 DNS 安全性。這些雲端傳遞的安全性訂閱使用與 Palo Alto Networks 威脅防護解決方案共用的基礎來運作，以提供全方位的 DNS 安全性解決方案，因此需要有進階威脅防護或威脅防護訂閱。

DNS 安全性雲端服務旨在保護您的組織免受多種基於 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 安全性可快速產生增強型 DNS 特徵碼集，以防禦已知的惡意 DNS 類別，並可以即時分析 DNS 要求，以保護您的網路免受新產生與未知惡意網域的侵害。DNS 安全性可以偵測各種 DNS 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。

如果有效的威脅防護解決方案在支援的網路安全性平台上運作，客戶可以使用 Palo Alto Networks 產生的網域清單對 DNS 要求執行 sinkhole 動作。這些本機存取的可自訂 DNS 特徵碼清單與防毒軟體和 WildFire 更新一同封裝，並包含發佈時原則執行和保護的最相關威脅防禦。為了擴大使用 DNS 識別威脅的範圍，DNS 安全性訂閱允許使用者使用進階預測分析存取即時保護功能。使用諸如 DGA/DNS 通道偵測和機器學習等技術，可以透過無限可調式雲端服務主動識別和共享隱藏在 DNS 流量中的威脅。由於 DNS 特徵碼和保護功能儲存在雲端架構中，因此您可存取完整的特徵碼資料庫。這些特徵碼使用大量資料來源產生，仍在不斷擴展之中。這讓您能夠使用 DNS 即時抵禦一系列威脅，防止來自新產生之惡意網域的攻擊。為了抵禦未來威脅，DNS 安全性服務將透過內容發佈不斷更新分析、偵測及防禦功能。

若要存取基本 *DNS* 安全性服務，除了運作網路安全性平台所需的任何基本授權之外，您還必須具備有效的進階威脅防護或威脅防護授權以及進階 *DNS* 安全性或 *DNS* 安全性授權。

DNS 安全性訂閱可在以下 Palo Alto Networks 網路安全性平台上使用：

- 新世代防火牆，包括 VM-Series 和 CN-Series
- Prisma Access

進階 DNS 安全性服務是一種補充性訂閱供應項目，與 DNS 安全性訂閱一起運作；DNS 安全性訂閱允許存取進階 DNS 安全性雲端中的新網域偵測器，這些偵測器會檢查 DNS 回應中的變化，以即時偵測各種類型的 DNS 劫持。透過存取在 PAN-OS 11.2 及更新版本上運作的進階 DNS 安全性，您可以偵測並封鎖來自被劫持的網域和設定錯誤的網域的 DNS 回應。透過直接操縱 DNS 回應或利用組織其 DNS 基礎結構的設定，便可將被劫持和設定錯誤的網域引入您的網路，以將使用者重新導向到他們從中發起其他攻擊的惡意網域。這兩種技術之間的主要差異在於入侵發生的位置。如果是 DNS 劫持，攻擊者能夠透過入侵組織其 DNS 基礎結構的某些方面（無論是 DNS 提供者的管理存取權、DNS 解析程序中的 MiTM 攻擊，或是 DNS 伺服器本身），來解析對攻擊者所運作網域進行的 DNS 查詢。設定錯誤的網域也會有類似的問題 - 攻擊者試圖利用過時的 DNS 記錄允許攻擊者獲得客戶子網域擁有權的這個網域設定問題，將自己的惡意網域併入到組織的 DNS 中。

進階 DNS 安全性可以透過運作基於雲端的偵測引擎，來即時偵測並分類被劫持和設定錯誤的網域，這些引擎透過使用基於 ML 的分析來分析 DNS 回應，藉此偵測惡意活動，進而提供 DNS 健康情況支援。由於這些偵測器位於雲端，因此您可以存取各種自動更新和部署的偵測機制，無需使用者在對偵測器進行變更時下載更新套件。首次發行時，進階 DNS 安全性支援兩種分析引擎：DNS 設定錯誤網域與劫持網域。此外，所有 DNS 查詢的 DNS 回應都會傳送到進階 DNS 安全性雲端，以增強回應分析，進而更準確地分類並在即時交換中傳回結果。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 DNS 安全性的啟用與設定是透過反間諜軟體（或 DNS 安全性）設定檔進行的，並且需要作用中的進階 DNS 安全性和進階威脅防護（或威脅防護）授權。

若要存取進階 *DNS* 安全性服務，除了運作網路安全性平台所需的任何基本授權之外，您還必須具備有效的進階威脅防護或威脅防護授權以及進階 *DNS* 安全性授權。

進階 DNS 安全性訂閱可在以下 Palo Alto Networks 網路安全性平台上使用：

- 新世代防火牆，包括 VM-Series 和 CN-Series

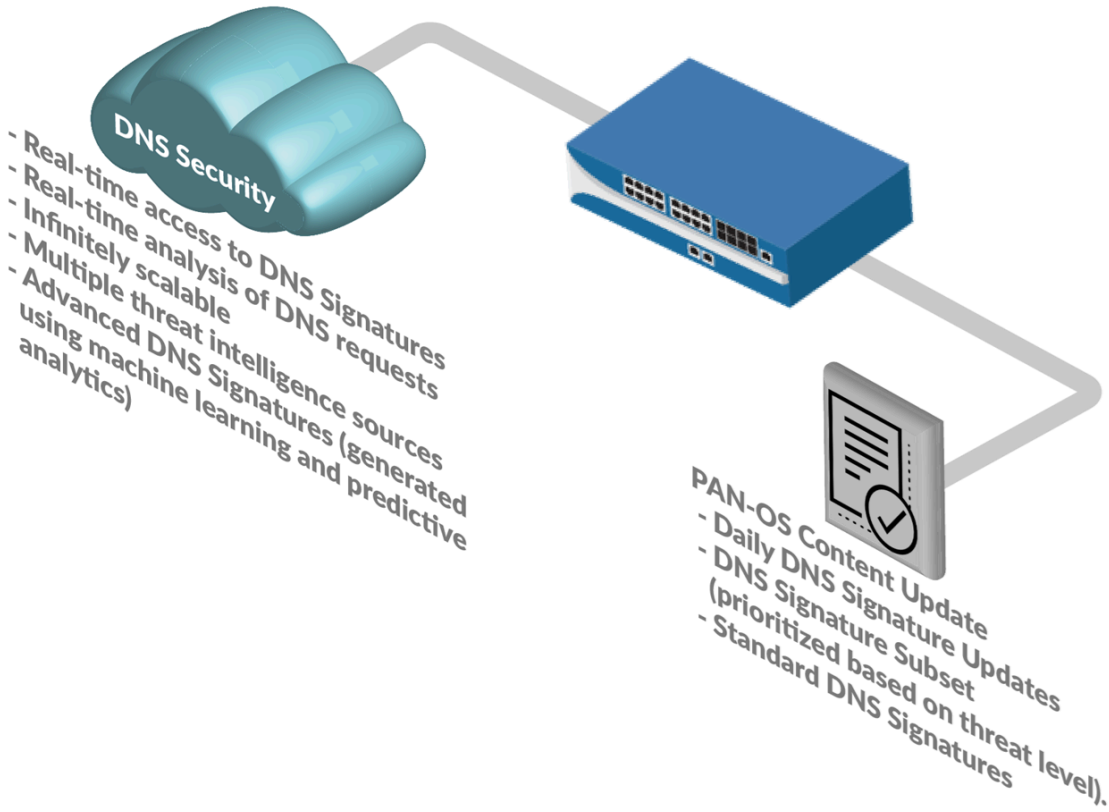
瞭解如何在網路中部署和監控 DNS 安全性和進階 DNS 安全性：

- 設定 DNS 安全性訂閱服務
- 監控 DNS 安全性訂閱服務

雲端傳遞 DNS 特徵碼和保護

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

作為一項雲端服務，進階 DNS 安全性和 DNS 安全性讓您能夠存取無限可調式 DNS 特徵碼和保護來源，以保護組織免受惡意網域攻擊。Palo Alto Networks 產生的網域特徵碼和保護功能有多種來源，包括 WildFire 流量分析、被動 DNS、主動 Web 爬取和 Web 內容分析、URL 沙箱分析、Honeynet、DGA 逆向工程、遙測資料、whois、Unit 42 研究組織及諸如網路威脅聯盟的協力廠商資料來源。此視需雲端資料庫為使用者提供權限存取 Palo Alto Network 的完整 DNS 特徵碼集，包括使用進階分析技術產生的特徵碼，以及即時 DNS 要求分析。本機可用的可下載 DNS 特徵碼集（與防毒軟體和 WildFire 更新一同封裝）具有硬編碼的容量限制（100k 特徵碼），且不包含透過進階分析產生的特徵碼。為了更好地適應每天產生之新 DNS 特徵碼的湧入，雲端特徵碼資料庫允許使用者無需下載更新即可立即存取新增的 DNS 特徵碼。如果網路連線中斷或以其他方式不可用，防火牆將使用盒上 DNS 特徵碼集。



DNS 安全性服務透過對多個 DNS 資料來源進行預測分析和機器學習，來執行即時 DNS 要求分析。其用於為基於 DNS 的威脅產生防護，可以透過設定附加到安全性原則規則的反間諜軟體安全性設定檔來即時存取這些防護。每個 DNS 威脅類別（DNS 特徵碼來源）都允許您定義單獨的原則動作以及特定特徵碼類型的日誌嚴重性級別。這讓您可以根據網路安全性通訊協定，基於威脅的性質來建立特定的安全性原則。Palo Alto Networks 還會根據 PAN-DB 和 Alexa 的指標產生並維護一個明確允許的網域清單。這些允許清單網域經常被存取，且已知沒有惡意內容。DNS 安全性類別和允許清單透過 PAN-OS 內容發佈進行更新和擴展。

PAN-OS 9.1 和更早版本的 *DNS* 安全性來源類別範圍有限。

DNS 安全性和進階 DNS 安全性目前支援偵測下列 DNS 威脅類別：

通用威脅 *ID* 編號（在威脅日誌中指示為 *ID*）對應到 *DNS* 安全性用於對網域進行分類的特定 *DNS* 偵測機制。這顯示了網域的精確分類，以及它所屬的廣泛定義的威脅類別。

- 命令和控制網域—C2 包括惡意軟體和/或遭到入侵的系統用於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的 URL 與網域（這包括 DNS 通道偵測和 DGA 偵測），或用盡目標授權 DNS 伺服器上的資源（如 NXNSattack）。
  - **DNS** 通道偵測（UTID：109001001/109001002）—攻擊者可以使用 DNS 通道對 DNS 查詢和回應中的非 DNS 程式及通訊協定進行資料編碼。這為攻擊者提供了一個開放式後端通道，可用於傳輸檔案或遠端存取系統。DNS 通道偵測使用機器學習來分析 DNS 查詢的行為品質，包括網域的 n-gram 頻率分析、資訊熵、查詢速率及模式，以確定查詢是否與基於 DNS 通道的攻擊一致。這包括某些新世代 DNS 通道惡意軟體，這些惡意軟體會在多個網域中緩慢地外洩資料以避免偵測，例如 TriFive 和 Snugy。結合防火牆的自動原則動作，此功能讓您能夠快速偵測到 DNS 通道中隱藏的 C2 或資料竊取行為，並根據您定義的原則規則自動進行封鎖。

    系統會進一步分析確定具有 DNS 通道功能的網域，以提供有關 DNS 安全性用於將資料嵌入到 DNS 查詢和回應及相關聯惡意程式活動名稱之工具的詳細資訊。屬性詳細資訊在威脅日誌中以為防火牆的威脅 ID/名稱形式提供，在 Prisma Access 上的 DNS 安全性日誌中以威脅名稱防火牆形式提供，格式如下：Tunneling:<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*> 或 Tunneling_infil:<*optional_list_of_tools/campaigns*; dot-separated string)>:<*domain_name*>，根據特定 DNS 通道網域類型而定。
  - **DGA** 網域偵測（UTID：109000001）—網域產生演算法 (DGA) 用於自動產生網域，通常在建立惡意命令與控制 (C2) 通訊通道的背景中大量產生。基於 DGA 的惡意軟體（例如 Pushdo、BankPatch 和 CryptoLocker）透過將執行中的 C2 伺服器位置隱藏在大量可能的可疑位置中，來限制被封鎖的網域數量，可以根據一天的特定時間、加密金鑰、字典衍生的命名配置和其他唯一值等因素透過演算法產生。雖然 DGA 產生的大部分網域都不會解析為有效的網域，但必須將它們全部識別出來，以全面抵禦特定威脅。DGA 分析透過對 DGA 中的其他常用技術進行逆向工程分析，來確定網域是否可能是由機器而不是人產生的。然後，Palo Alto Networks 會使用這些特性來即時識別並封鎖先前未知的 DGA 威脅。
  - **NXNSAttack**（UTID：109010007）—DNS 通訊協定中存在的 NXNSAttack 漏洞會影響所有遞歸 DNS 解析程式，惡意行為者可以使用該漏洞啟動 DDos 之類的放大攻擊來中斷易受攻擊的授權 DNS 伺服器的正常運作。NXNSAttack 可以透過強制遞歸 DNS 解析程式發出大量可能關閉伺服器的無效要求，在授權 DNS 伺服器上產生大量流量峰值。
  - **DNS** 重新繫結（UTID：109010009）—DNS 重新繫結攻擊會誘使使用者存取攻擊者控制的網域，其中設定有短 TTL 參數來操縱解析網域名稱的方法，以惡意利用和繞過瀏覽器中的相同原始政策。這使得惡意行為者能夠將用戶端機器用作中繼來攻擊或存取私人網路中包含的資源。
  - **DNS** 非法上傳（UTID：109001003）—DNS 非法上傳包括 DNS 查詢，這些查詢使惡意行為者能夠透過回應欺詐性 A (IPv4) 和 AAAA (IPv6) 記錄要求來隱藏和解析分鐘有效負載。當用戶端解析多個子網域（每個子網域都包含一個帶有編碼元件的 A/AAAA 記錄）時，可以合併其中包含的資料以形成惡意有效負載，然後可以在用戶端機器上執行該有效負載。執行該有效負載后，它可以引入輔助有效負載以建立 DNS 通道或其他入侵。
  - **DNS** 流量分析（UTID：109010010）—（需要進階 DNS 安全性） DNS 流量分析是基於雲端的分析器，會根據 DNS 流量模式的評估偵測嘗試建立 C2 連線的惡意軟體。當進階 DNS 安全性監控您組織的 DNS 流量時，輸出 DNS 請求序列會被向量化以形成 DNS 流量設定檔，

然後使用 ML 技術進行分析，這些技術可以將唯一的 DNS 要求模式與可識別的惡意 C2 網域設定檔關聯。

- 動態 **DNS** 託管網域（UTID：109020002）—動態 DNS (DDNS) 服務近乎即時地提供主機名稱與 IP 位址之間的對應，以在靜態 IP 不可用時保持不斷變更的 IP 位址連結到特定網域。這為攻擊者提供了一種滲透網路的方法，即使用 DDNS 服務來變更託管命令和控制伺服器的 IP 位址。惡意軟體活動和入侵程式套件可以利用 DDNS 服務作為其裝載散佈策略的一部分。透過將 DDNS 網域用作其主機名稱基礎結構的一部分，攻擊者可以變更與給定 DNS 記錄關聯的 IP 位址，且更容易避開偵測。DNS 安全性透過篩選和交互參照來自各種來源的 DNS 資料以產生候選清單來偵測攻擊性 DDNS 服務，然後對這些候選清單進行進一步驗證以最大程度提高準確性。
- 惡意軟體網域—惡意網域託管和散佈惡意軟體，且可能包含試圖安裝各種威脅（例如可執行檔、指令碼、病毒、偷渡式下載）的網站。惡意網域與 C2 網域的區別在於，其透過外部來源將惡意裝載傳遞到網路中，而對於 C2，受感染的端點通常會嘗試連線到遠端伺服器以擷取額外指令或其他惡意內容。
  - 惡意軟體危害的 **DNS**（UTID：109003001）—惡意軟體危害的 DNS 涵蓋了一系列技術，其中一些是合法的，這些技術會導致產生看似真實的主機名稱和子網域，而這些主機名稱和子網域實際上是惡意的。這包括新觀察到的主機名稱，這些主機名稱模仿現有的信譽良好的主機名稱，試圖冒充或以其他方式誤導和逃避以資料庫為中心的安全性解決方案。這些主機名稱會快速大量產生，以搶佔將它們新增到資料庫清單的先機。網域陰影通常在攻擊者透過較傳統的攻擊取得對網域帳戶的控制權之後進行。這提供了建立用於協調攻擊的非法子網域所需的存取權，即使根網域仍然合法有效，也增加了規避網路安全性的可能性。
  - 勒索軟體網域 (UTID:109003002) — 勒索軟體是惡意軟體之下的子類別，會以鎖定或加密方式阻止使用者存取資料，藉此換取支付贖金，支付之後攻擊者會將系統釋放還給使用者。勒索軟體可以透過惡意勒索軟體網域散布，這些網域託管了看似合法的文件，以誘騙使用者下載。
- 新註冊網域（UTID：109020001）—新註冊的網域是指最近由 TLD 營運商新增的網域，或在過去 32 天內擁有權發生過變更的網域。雖然可以出於合法目的建立新網域，但絕大多數新網域通常用於促進惡意活動，例如作為 C2 伺服器運作或用於散佈惡意軟體、垃圾郵件、PUP/廣告軟體。Palo Alto Networks 監控特定的摘要（網域註冊機構和註冊商）並使用區域檔案、被動 DNS、WHOIS 資料來偵測註冊活動，以便偵測新註冊的網域。
- 網路釣魚網域（UTID：109010001)—網路釣魚網域嘗試透過網路釣魚或網域嫁接偽裝成合法網站，以誘使使用者提交個人資訊或使用者認證等敏感資料。這些惡意活動可以透過社交工程活動（憑藉一個看起來可信的來源，操縱使用者透過電子郵件或其他形式的電子通訊來提交個人資訊）或透過 Web 流量重新導向（將使用者導向到看似合法的欺詐網站）進行。

- 灰色軟體網域（UTID：109010002）—（在安裝 PAN-OS 內容版本 8290 和更新版本時可用）。灰色軟體網域通常不構成直接的安全威脅，但是，其可以促進攻擊媒介的活動、產生各種不適當行為，或者僅包含可疑/冒犯的內容。這可能包括以下類型的網站和網域：
  - 試圖欺騙使用者授予遠端存取權限。
  - 利用熱門的網頁託管和動態網域名稱系統 (DDNS) 服務的子網域來託管和散布惡意內容（子網域信譽 - UTIDL 109002004）。
  - 包含廣告軟體和其他未經請求的應用程式（如 cryptominer、hijacker 和 PUP[可能不需要的程式]）。
  - 使用 Fast Flux 技術部署網域識別隱藏動作（**fastflux** 偵測—UTID：109010005）。
  - 透過 DNS 安全性預測分析說明惡意行為和惡意使用情況（惡意 **NRD** - UTID：109010006）。
  - 由於授權 DNS 伺服器上尚未移除或糾正的設定不當或者陳舊的 DNS 記錄，將流量從合法來源重新導向到惡意網站（懸置 **DNS** - UTID：109010008）。
  - 促進非法活動或詐騙。
  - 包括萬用字元 DNS 項目，這些項目可用於規避封鎖清單或透過將流量路由到惡意網站來實施萬用字元 DNS 攻擊（萬用字元濫用 - UTID：109002001）。
  - 與根據收集的 DNS 資料建置的已建立基線設定檔（異常偵測）相比，指示是否存在具有異常特徵的 DNS 流量。
  - 已提前數月或數年註冊，並在啟動時處於休眠狀態以繞過聲譽檢查。這還包括從未見過或從未以其他方式評估過的新觀察到的網域（策略性老化的網域 - UTID：109002002）。
  - 為可能具有惡意意圖的攻擊者已根據憑證透明度日誌註冊但未使用的網域（庫存網域偵測 - UTID：109002005）。
  - 透過相像的熱門品牌名稱網域以及錯誤輸入的網頁地址來欺騙使用者，目的是將使用者引導到假冒和詐欺網站。（域名搶註/誤植域名網域 - UTID：109002003）。
- 寄放網域（UTID：109010003）—（在安裝 PAN-OS 內容版本 8318 及更新版本時可用）寄放網域通常是託管有限內容的非作用網站，其形式通常為點選廣告，可能會為託管實體帶來收益，但通常不包含對一般使用者有用的內容。儘管其通常充當合法的預留位置或僅起到良性干擾作用，但也可以用作散佈惡意軟體的可能媒介。
- **Proxy Avoidance and Anonymizers**（UTID：109010004）—（在安裝 PAN-OS 內容版本 8340 及更新版本時可用）Proxy Avoidance and Anoymizers 是指向用於繞過內容篩選政策的服務的流量。嘗試透過匿名 Proxy 服務繞過組織的內容篩選原則的使用者將在 DNS 層級被封鎖。
- 廣告追蹤網域（UTID：109004000）—（透過安裝 PAN-OS 內容版本 8586 及更新版本可供使用）廣告追蹤網域為網頁提供某些類型的行銷自動化內容，以追蹤使用者參與度（例如連結點擊、網頁瀏覽等）。通常，這些第三方網域透過使用虛名 URL 加以隱藏，以顯示為原始網域的一部分。
  - **CNAME** 偽裝（UTID：109004001）— CNAME 偽裝提供另一種隱藏 URL 的方法，方法是修改子網域的 Web 要求，使其看起來好像來自同一個網站，但實際上該子網域使用 CNAME

解析為第三方網域。此技術會規避一些基於瀏覽器的隱私權保護，這些保護可能會連線到可疑的 CNAME 目的地。

- 劫持的網域（UTID：109004000）—（需要進階 DNS 安全性）劫持的網域包括攻擊者能夠使合法網域解析為攻擊者所運作 IP 位址所在的網域，達成手段通常是透過破壞組織 DNS 基礎結構的某些方面。這包括未經授權以管理員身分存取 DNS 提供者、DNS 解析程序期間的 MitM 攻擊，或者存取 DNS 伺服器本身。
- 設定錯誤的網域（UTID：109004000）—（需要進階 DNS 安全性）設定錯誤的網域可讓攻擊者利用網域設定問題，將其自己的惡意網域併入到組織的 DNS 中。這些過時的 DNS 記錄讓攻擊者能夠取得客戶子網域的擁有權，並將使用者重新導向至攻擊者出於惡意控制的 IP 或網站。這些不可解析的設定錯誤網域是基於在設定進階 DNS 安全性期間所指定的面向公眾父系網域。
  - 設定錯誤的區域：（UTID：109004200）—未與任何其他設定錯誤類別對應的設定錯誤網域通用類別。
  - 設定錯誤區域懸置（**UTID**：109004201）—由於存在於組織其面向公眾網域中的授權 DNS 伺服器上有設定不當或陳舊的 DNS 記錄，因此將流量從合法來源重新導向到惡意網站的設定錯誤網域。
  - 設定錯誤的可宣告 **NX**（**UTID**：109004202）—定義為組織其 DNS 設定的一部分，但已不再存在 (NXDOMAINS) 的設定錯誤網域，攻擊者可以暗中註冊此網域，用於將使用者重新導向到惡意網站，並可能允許攻擊者取得客戶網路的存取權。

資料收集與記錄

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

DNS 安全性服務在執行網域查閱時，會根據您的安全性政策規則、相關聯的動作和 DNS 查詢詳細資訊收集伺服器回應和要求資訊，以針對基於 Strata Logging Service 的活動應用程式（AIOps for NGFW Free、Prisma Access、Strata Logging Service 等）產生 DNS 安全性日誌。此外，網路安全性平台會將補充 DNS 資料轉送至 DNS 安全性雲端伺服器，並由 Palo Alto Networks 服務用於提供更準確的網域資訊（如提供者 ASN、主機資訊和地理位置識別）。雖然這一補充資料對於運作 DNS 安全性服務並不必要，但它會提供資源來產生改進的分析、DNS 偵測和預防功能。此動作在資料收集發生後不到 30 秒內發生。為了最大限度地減少防火牆效能影響，DNS 安全性遙測會以最小的開銷運作，這可以限制傳送到 Strata Logging Service 的 DNS 遙測資料總量；因此，只有 DNS 查詢的子集會轉送到 Strata Logging Service 作為 DNS 安全性日誌項目。因此，Palo Alto Networks 建議將惡意 DNS 要求日誌視為威脅日誌，而不是 DNS 安全性日誌。

惡意 *DNS* 查詢也會記錄為威脅日誌，並使用 *PAN-OS* 日誌轉送提交給 *Strata Logging Service*（如果設定正確）。

DNS 安全性可以提交以下資料欄位：

欄位	說明
動作	顯示在 DNS 查詢上採取的原則動作。
類型	顯示 DNS 記錄類型。
回應	DNS 查詢中網域解析的 IP 位址。
回應代碼	接收做為 DNS 查詢回答的 DNS 回應碼。
來源 IP	發出 DNS 要求之系統的 IP 位址。
來源使用者	當啟用防火牆 User-ID 功能時，會顯示 DNS 要求者的識別碼。

欄位	說明
來源區域	安全性原則規則中參照的已設定來源區域。

對於新增至 *DNS* 例外狀況允許清單的網域，會繞過 *DNS* 擴展資料收集。

可以使用以下 CLI 命令避免自動提交可用於潛在識別使用者的資料欄位（來源 IP、來源使用者和來源區域）：**`set deviceconfig setting ctd cloud-dns-privacy-mask yes`**。您必須 **`commit`**（提交）變更才能使更新生效。

區域服務網域

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

Palo Alto Networks 維護一個由全球和區域網域組成的網路，這些網域為 DNS 安全性和進階 DNS 安全性作業提供服務。這些服務網域運作即時 DNS 要求分析器、存取 DNS 特徵碼資料庫，並提供進階的相依雲端功能。預設情況下，DNS 安全性和進階 DNS 安全性連線到全球服務網域（分別為 dns.service.paloaltonetworks.com 和 adv-dns.service.paloaltonetworks.com），接著這些網域會自動重新導向到最靠近網路安全平台位置的區域網域。

DNS 安全性區域服務網域

Palo Alto Networks 建議使用預設的全域服務網域設定來改進容錯移轉處理；但是，如果您因為位置的具體情況（例如，當跨越多個重疊的區域網域時）而遇到延遲問題，您可以手動指定服務網域。若要指定 DNS 安全性使用的區域服務網域，您必須為 dns.service.paloaltonetworks.com 新增一個 DNS 項目，該項目包含一個 CNAME 記錄指示屬於 DNS 伺服器設定一部分的有效區域網域。連線到區域網域後，您可以在防火牆上發出 CLI 命令：

```
show dns-proxy dns-signature counters
```

，以檢閱平均延遲。相關段落位於「特徵碼查詢 API」標題下。

下表列出 DNS 安全性服務網域：

位置	URL
南非，開普敦	dns-za.service.paloaltonetworks.com
香港	dns-hk.service.paloaltonetworks.com
日本，東京	dns-jp.service.paloaltonetworks.com
新加坡	dns-sg.service.paloaltonetworks.com

位置	URL
印度，孟買	dns-in.service.paloaltonetworks.com
澳大利亞，雪梨	dns-au.service.paloaltonetworks.com
英國，倫敦	dns-uk.service.paloaltonetworks.com
德國，法蘭克福	dns-de.service.paloaltonetworks.com
荷蘭，埃姆斯哈文	dns-nl.service.paloaltonetworks.com
法國，巴黎	dns-fr.service.paloaltonetworks.com
巴林	dns-bh.service.paloaltonetworks.com
加拿大，魁北克省，蒙特婁	dns-ca.service.paloaltonetworks.com
巴西，聖保羅，奧薩斯庫	dns-br.service.paloaltonetworks.com
美國，愛荷華州，康瑟爾崖	dns-us-ia.service.paloaltonetworks.com
美國，北維吉尼亞州，阿什本	dns-us-va.service.paloaltonetworks.com
美國，奧勒岡州，達拉斯	dns-us-or.service.paloaltonetworks.com
美國，加利福尼亞州，洛杉磯	dns-us-ca.service.paloaltonetworks.com

進階 DNS 安全性區域服務網域

您可以手動指定用於促進進階 DNS 安全性查詢的伺服器。雖然 Palo Alto Networks 建議使用預設的全域服務網域，但如果您遇到延遲時間超出預期或有其他與服務相關的問題，則可以覆寫所選的伺服器。

您可以從 **Device**（裝置） > **Setup**（設定） > **Management**（管理） > **Advanced DNS Security**（進階 **DNS** 安全性） > **DNS Security Server**（**DNS** 安全性伺服器），在 PAN-OS 中指定進階 DNS 安全性服務網域。

此設定不會影響標準 *DNS* 安全性查詢的處理方式。

下表列出進階 DNS 安全性服務網域：

位置	URL
南非，開普敦	za.adv-dns.service.paloaltonetworks.com
巴林	bh.adv-dns.service.paloaltonetworks.com
香港	hk.adv-dns.service.paloaltonetworks.com
日本，東京	jp.adv-dns.service.paloaltonetworks.com
新加坡	sg.adv-dns.service.paloaltonetworks.com
印度，孟買	in.adv.dns.service.paloaltonetworks.com
澳大利亞，雪梨	au.adv-dns.service.paloaltonetworks.com
英國，倫敦	uk.adv-dns.service.paloaltonetworks.com
德國，法蘭克福	de.adv.dns.service.paloaltonetworks.com
荷蘭，埃姆斯哈文	nl.adv.dns.service.paloaltonetworks.com
法國，巴黎	fr.adv-dns.service.paloaltonetworks.com
巴林	bh.adv-dns.service.paloaltonetworks.com
加拿大，魁北克省，蒙特婁	ca.adv.dns.service.paloaltonetworks.com
巴西，聖保羅，奧薩斯庫	br.adv.dns.service.paloaltonetworks.com
美國，愛荷華州，康瑟爾崖	us-ia.adv.dns.service.paloaltonetworks.com
美國，北維吉尼亞州，阿什本	us-va.adv.dns.service.paloaltonetworks.com
美國，奧勒岡州，達拉斯	us-or.adv.dns.service.paloaltonetworks.com
美國，加利福尼亞州，洛杉磯	us-ca.adv.dns.service.paloaltonetworks.com

設定 DNS 安全性訂閱服務

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

在啟用和設定進階 DNS 安全性或 DNS 安全性之前，您必須先取得並安裝威脅防護（或進階威脅防護）授權，和進階 DNS 安全性或 DNS 安全性授權，以及其運作所在任何平台的授權。授權是從 Palo Alto Networks 客戶支援入口網站啟動的，必須處於作用中狀態才能進行 DNS 分析。此外，DNS 安全性訂閱服務（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 DNS 安全性訂閱服務之前，建議您先熟悉安全性訂閱已啟用的安全性平台其核心元件。如需詳細資訊，請參閱產品文件。

若要啟用和設定 DNS 安全性訂閱服務，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 提供的最佳作法，以獲得最佳的可用性和安全性。

- 在我的網路安全平台上啟用 DNS 安全性或進階 DNS 安全性，以防止 DNS 威脅進入我的網路（必要）
- 建立網域特徵碼例外狀況和允許清單以限制誤判，並防止內部 DNS 伺服器觸發 DNS 分類
- 測試可用網域類別的已設定政策動作
- 驗證我的防火牆對 DNS 安全性服務的連線
- 透過在防火牆上自訂 DNS 查閱逾時設定，限制因延遲而導致的連線中斷

啟用 DNS 安全性

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

若要啟用 DNS 安全性，您必須建立（或修改）反間諜軟體安全性設定檔，以存取 DNS 安全性服務、設定 DNS 特徵碼類別的日誌嚴重性和政策設定，然後將設定檔附加至安全性政策規則。

- Strata Cloud Manager
- PAN-OS 和 Panorama

啟用 DNS 安全性 (Strata Cloud Manager)

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。

STEP 2 | 確認 DNS 安全性和威脅防護（或進階威脅防護）授權是否處於作用中狀態。選取 **Manage**（管理）> **Configuration**（設定）> **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**）> **Overview**（概要），然後按一下 **License**（授權）面板中的授權使用條款連結。您應該會在下列安全性服務旁邊看到綠色勾號：防毒、反間諜軟體、弱點保護和 DNS 安全性。

STEP 3 | 確認安全性原則中的 *paloalto-dns-security* App-ID 已設定為 enable（啟用）來自 DNS 安全性雲端安全性服務的流量。

如果您的防火牆部署透過設定為強制執行 *App-ID* 安全性原則的網際網路型周邊防火牆路由管理流量，則必須允許周邊防火牆上的 *App-ID*；如果不這樣做，會阻止 *DNS* 安全性連線。

STEP 4 | 設定 DNS 安全性特徵碼原則設定以傳送惡意 DNS 查詢至已定義 sinkhole。

如果您使用外部動態清單作為網域允許清單，其優先順序不會高於 *DNS* 安全性網域原則動作。因此，當有與 *EDL* 和 *DNS* 安全性網域類別中的項目相符的網域時，仍會套用 *DNS* 安全性下指定的動作，即使 *EDL* 明確設定為「允許」動作也是如此。如果您想要新增 *DNS* 網域例外狀況，請將 *EDL* 設定為 *Alert*（警示）動作，或將它們新增至 *DNS Exceptions*（*DNS* 例外狀況）頁籤中的 *DNS Domain/FQDN Allow List*（*DNS* 網域/*FQDN* 允許清單）。

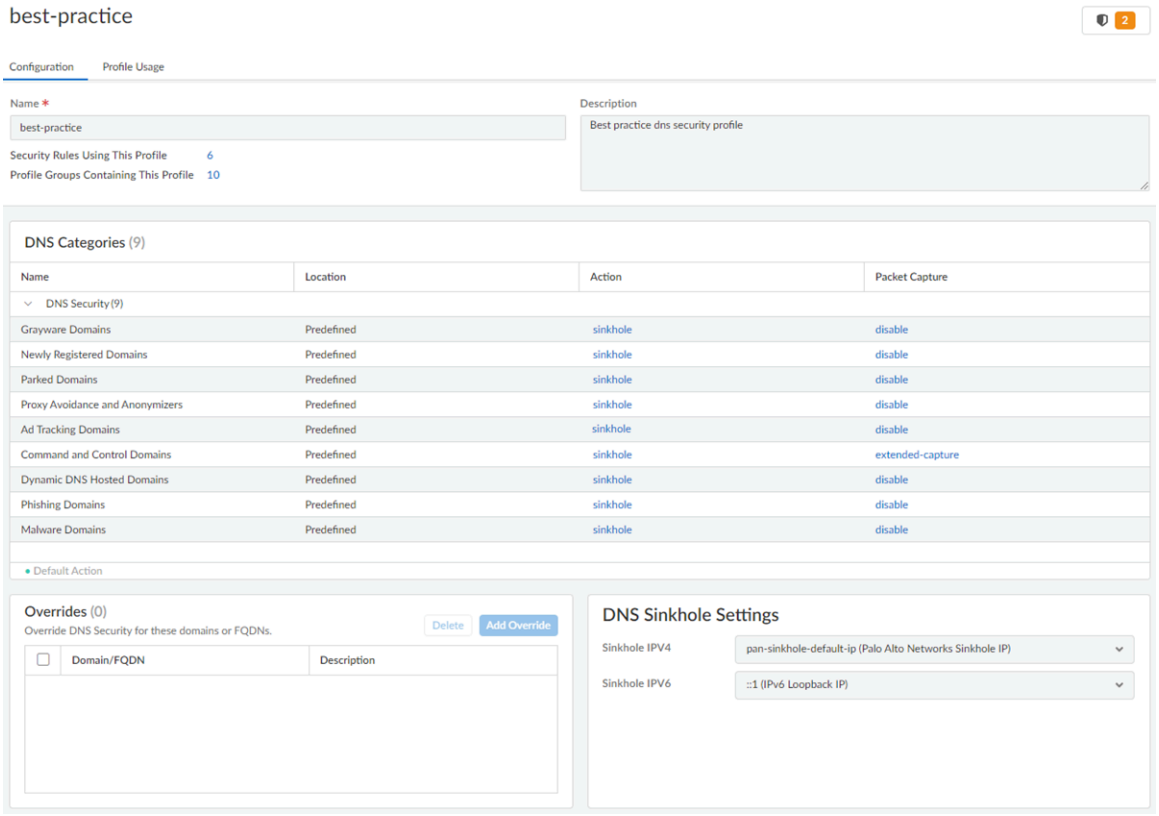
1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **DNS Security**（**DNS** 安全性）。
2. 建立或修改現有的 DNS 安全性設定檔。
3. 輸入設定檔 **Name**（名稱），並提供說明（選用）。
4. 在 **DNS Categories**（**DNS** 類別）區段中，[DNS 安全性] 標題下，有可個別設定的 DNS 特徵碼來源，可讓您定義單獨的政策動作及封包擷取設定。

   Palo Alto Networks 建議為所有特徵碼來源使用預設動作設定，以確保獲得最佳覆蓋範圍，並有助於事件回應和修復。如需設定 *DNS* 安全性設定最佳作法的詳細資訊，請參閱避免網路發生 Layer 4 與 Layer 7 規避攻擊最佳作法。

   - 針對 DNS 特徵碼來源，選取對於已知的惡意軟體網站進行 DNS 查詢時採取的動作。選項包括警示、允許、封鎖或 sinkhole。Palo Alto Networks 建議將動作設定為 Sinkhole。
   - 您可以透過為每個 DNS 特徵碼來源設定政策動作 **Allow**（允許）及相應的日誌嚴重性 **None**（無）來完全繞過 DNS 流量檢查。
   - 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**（延伸擷取）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。
5. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 設定）區段中，確認是否存在有效的 **Sinkhole** 位址。為了您的方便，預設設定 (pan-sinkhole-default-ip) 設定為存取 Palo Alto Networks Sinkhole 伺服器。Palo Alto Networks 可以透過更新自動重新整理此位址。

   Sinkhole 會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 *DNS* 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，如果用戶端位於沒有內部 *DNS* 伺服器的網路中，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。在這些情況下，您應該使用下列 *Sinkhole IP* 位址：*(72.5.65.111)*。

   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。



6. 按一下 **OK**（確定）儲存 DNS 安全性設定檔。

STEP 5 | 將 DNS 安全性設定檔附加到安全性政策規則。

STEP 6 | 測試已強制執行該原則動作。

1. 存取 DNS 安全性測試網域，以確認是否正在強制執行所指定威脅類型的政策動作。
2. 若要監控活動：
   1. 檢視活動日誌，並透過 Sinkhole 動作搜尋 URL 網域，以檢視您所存取測試網域的日誌項目。

STEP 7 | 選用—建立解密政策規則以解密 DNS-over-TLS / 連接埠 853 流量。然後可以使用包含 DNS 政策設定的 DNS 安全性設定檔設定，來處理解密的 DNS 有效負載。當 DNS-over-TLS 流量遭解密時，威脅日誌中產生的 DNS 要求將顯示成來源連接埠為 853 的傳統 **dns-base** 應用程式。

STEP 8 | 有關其他監控選項，請參閱 監控 DNS 安全性訂閱服務

啟用 DNS 安全性 (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 和更新版本支援可個別設定的 DNS 特徵碼來源，讓能夠您針對指定的特徵碼來源定義單獨的政策動作以及日誌嚴重性層級。這使您能夠依據網路安全性通訊協定，以根據網域類型的威脅態勢建立離散、精確的安全性動作。DNS 特徵碼來源定義可透過 PAN-OS 內容版本擴展，因此，當引入新的 DNS 安全性分析器時，您可以根據威脅的性質建立特定政策。升級到 PAN-OS 10.0 及更高版本後，DNS 安全性來源將重新定義為新類別，以提供擴展的精確控制；因此，新類

別將覆寫之前定義的動作並獲取預設設定。確保重新套用適用於新定義的 DNS 安全性類別的任何 sinkhole、日誌嚴重性和封包擷取設定。

- PAN-OS 11.0 和更新版本
- PAN-OS 10.x
- PAN-OS 9.1

啟用 DNS 安全性（PAN-OS 11.0 和更新版本）

STEP 1 | 登入 NGFW。

STEP 2 | 若要利用 DNS 安全性，您必須擁有作用中的 DNS 安全性和威脅防護（或進階威脅防護）訂閱。

確認您是否擁有必要的訂閱。要確認當前哪些訂閱具有授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認顯示了適當的授權且該授權沒有過期。

STEP 3 | 確認安全性原則中的 *paloalto-dns-security* App-ID 已設定為 enable（啟用）來自 DNS 安全性雲端安全性服務的流量。

如果您的防火牆部署透過設定為強制執行 *App-ID* 安全性原則的網際網路型周邊防火牆路由管理流量，則必須允許周邊防火牆上的 *App-ID*；如果不這樣做，會阻止 *DNS* 安全性連線。

STEP 4 | 設定 DNS 安全性特徵碼原則設定以傳送惡意 DNS 查詢至已定義 sinkhole。

如果您使用外部動態清單作為網域允許清單，其優先順序不會高於 *DNS* 安全性網域原則動作。因此，當有與 *EDL* 和 *DNS* 安全性網域類別中的項目相符的網域時，仍會套用 *DNS* 安全性下指定的動作，即使 *EDL* 明確設定為「允許」動作也是如此。如果您想要新增 *DNS* 網域例外狀況，請將 *EDL* 設定為 *Alert*（警示）動作，或將它們新增至 *DNS Exceptions*（*DNS* 例外狀況）頁籤中的 *DNS Domain/FQDN Allow List*（*DNS* 網域/*FQDN* 允許清單）。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 建立設定檔或修改現有的設定檔，或選取一個現有的預設設定檔並加以複製。
3. 輸入設定檔 **Name**（名稱），並提供說明（選用）。
4. 選取 **DNS Policies**（**DNS** 原則）頁簽。
5. 在 DNS 安全性標題下的 **Signature Source**（特徵碼來源）欄中，有可單獨設定的 DNS 特徵碼來源，可用於定義單獨的原則動作以及日誌嚴重性層級。

   Palo Alto Networks 建議變更特徵碼來源的預設 *DNS* 原則設定，以確保獲得最佳覆蓋範圍，並有助於事件回應和修復。請遵循避免網路發生 Layer 4 與 Layer 7 規避攻擊最佳作法中規定的設定 *DNS* 安全性設定的最佳作法。

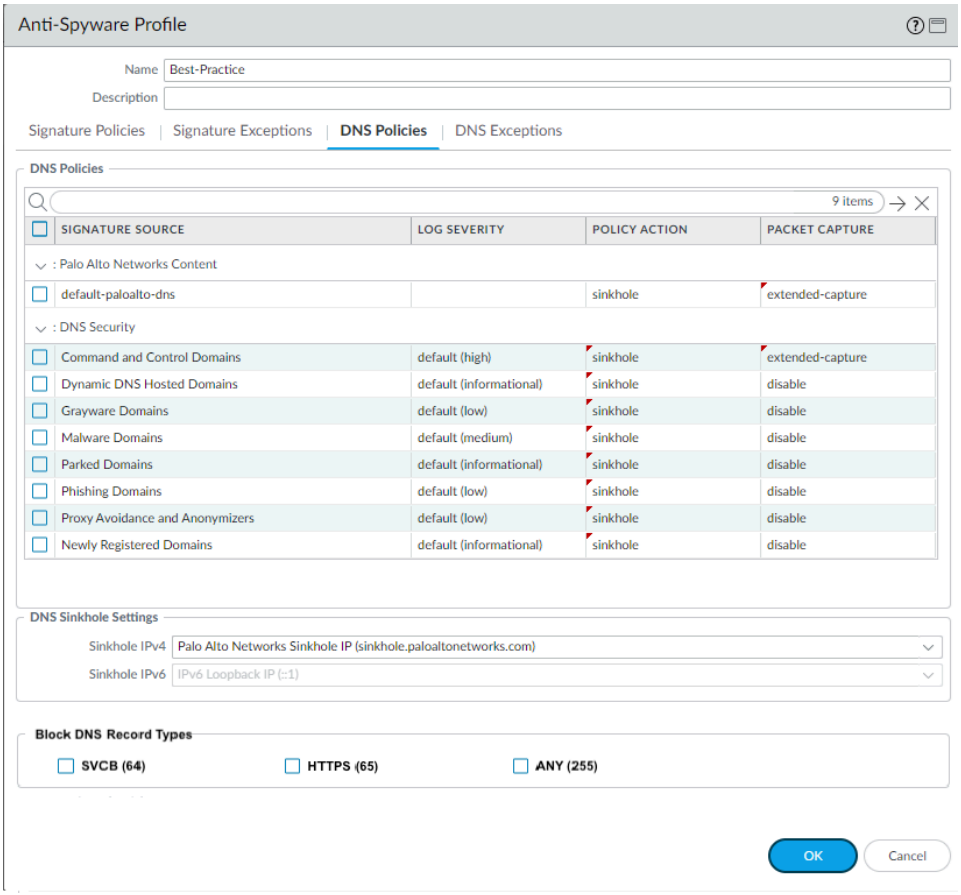
   - 指定防火牆偵測到與 DNS 特徵碼相符的網域時記錄的日誌嚴重性層級。有關各種日誌嚴重性層級的更多資訊，請參閱威脅嚴重性層級。
   - 針對 DNS 特徵碼來源，選取對於已知的惡意軟體網站進行 DNS 查詢時採取的動作。選項包括預設值、允許、封鎖或 Sinkhole。確認動作是否已設為 sinkhole。
   - 您可以透過為每個 DNS 特徵碼來源設定政策動作 **Allow**（允許）及相應的日誌嚴重性 **None**（無）來完全繞過 DNS 流量檢查。
   - 在 **Packet Capture**（封包擷取）下拉式清單中，選取 **single-packet**（單一封包）以擷取工作階段的第一個封包；或選取 **extended-capture**（延伸擷取）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。
6. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 設定）區段，確認已啟用 **Sinkhole**。為了方便您，預設 Sinkhole 位址 (sinkhole.paloaltonetworks.com) 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位址。

   Sinkhole 會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 *DNS* 類別。使用預設的 *Sinkhole FQDN (sinkhole.paloaltonetworks.com)* 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，如果用戶端位於沒有內部 *DNS* 伺服器的網路中，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。在這些情況下，您應該使用下列 *Sinkhole IP* 位址：*(72.5.65.111)*。

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。

7. （選用）在後續 TLS 連線中加密 client hello 期間，封鎖用於交換金鑰資訊的指定 DNS 資源記錄類型。以下 DNS RR 類型可用：SVCB (64)、HTTPS (65) 和 ANY (255)。

   - 雖然沒有必要為了啟用 *DNS Security over DoH* 來封鎖 *ECH*，但 *Palo Alto Networks* 目前建議封鎖 *ECH* 使用的所有 *DNS* 記錄類型，以獲得最佳安全性。
   - *64* 型和 *65* 型資源記錄標準仍在變化（處於草稿狀態），且可能會不時改變。有關 *DNS SVCB* 和 *HTTPS RR* 的詳細資訊，請參閱：透過 DNS（DNS SVCB 和 HTTPS RR）的服務繫結與參數規格，如 IETF 定義。



8. 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

STEP 5 | 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）。
2. 選取或建立 **Security Policy Rule**（安全性原則規則）。
3. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段結束時記錄）核取方塊以啟用記錄。
4. 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或經過修改的設定檔。
5. 按一下 **OK**（確定）來儲存原則規則。

STEP 6 | 測試已強制執行該原則動作。

1. 存取 DNS 安全性測試網域，以確認是否正在強制執行所指定威脅類型的政策動作。
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。
    3. 如需更多監控選項，請參閱 監控 DNS 安全性訂閱服務

STEP 7 | 選用—建立解密政策規則以解密 DNS-over-TLS / 連接埠 853 流量。然後可以使用包含 DNS 政策設定的反間諜軟體設定檔設定來處理解密的 DNS 有效負載。當 DNS-over-TLS 流量遭解密時，威脅日誌中產生的 DNS 要求將顯示成來源連接埠為 853 的傳統 **dns-base** 應用程式。

STEP 8 | 選用—查看嘗試連線至惡意網域的受感染主機

啟用 DNS 安全性 (PAN-OS 10.x)

STEP 1 | 登入 NGFW。

STEP 2 | 若要利用 DNS 安全性，您必須擁有作用中的 DNS 安全性和威脅防護（或進階威脅防護）訂閱。

確認您是否擁有必要的訂閱。要確認當前哪些訂閱具有授權，請選取 **Device**（裝置）> **Licenses**（授權），並確認顯示了適當的授權且該授權沒有過期。

STEP 3 | 確認安全性原則中的 *paloalto-dns-security* App-ID 已設定為 enable（啟用）來自 DNS 安全性雲端安全性服務的流量。

如果您的防火牆部署透過設定為強制執行 *App-ID* 安全性原則的網際網路型周邊防火牆路由管理流量，則必須允許周邊防火牆上的 *App-ID*；如果不這樣做，會阻止 *DNS* 安全性連線。

STEP 4 | 設定 DNS 安全性特徵碼原則設定以傳送惡意 DNS 查詢至已定義 sinkhole。

如果您使用外部動態清單作為網域允許清單，其優先順序不會高於 *DNS* 安全性網域原則動作。因此，當有與 *EDL* 和 *DNS* 安全性網域類別中的項目相符的網域時，仍會套用 *DNS* 安全性下指定的動作，即使 *EDL* 明確設定為「允許」動作也是如此。如果您想要新增 *DNS* 網域例外狀況，請將 *EDL* 設定為 *Alert*（警示）動作，或將它們新增至 *DNS Exceptions*（*DNS* 例外狀況）頁籤中的 *DNS Domain/FQDN Allow List*（*DNS* 網域/*FQDN* 允許清單）。

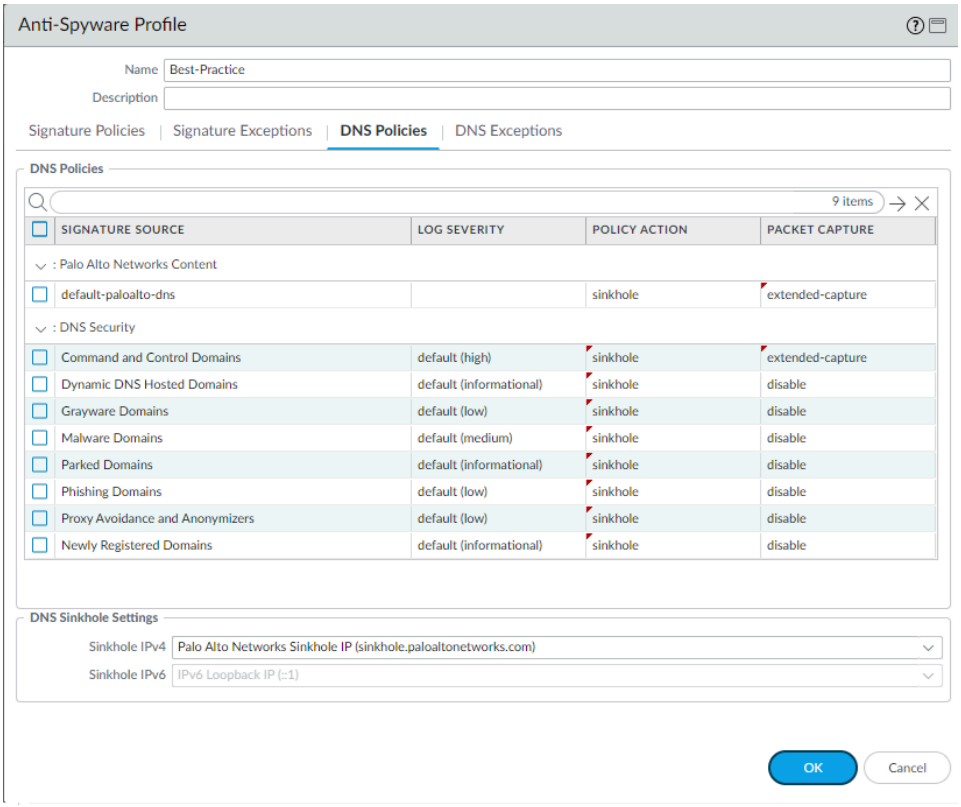
1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 建立設定檔或修改現有的設定檔，或選取一個現有的預設設定檔並加以複製。
3. 輸入設定檔 **Name**（名稱），並提供說明（選用）。
4. 選取 **DNS Policies**（**DNS** 原則）頁簽。
5. 在 DNS 安全性標題下的 **Signature Source**（特徵碼來源）欄中，有可單獨設定的 DNS 特徵碼來源，可用於定義單獨的原則動作以及日誌嚴重性層級。

   Palo Alto Networks 建議變更特徵碼來源的預設 *DNS* 原則設定，以確保獲得最佳覆蓋範圍，並有助於事件回應和修復。請遵循避免網路發生 Layer 4 與 Layer 7 規避攻擊最佳作法中規定的設定 *DNS* 安全性設定的最佳作法。

   - 指定防火牆偵測到與 DNS 特徵碼相符的網域時記錄的日誌嚴重性層級。有關各種日誌嚴重性層級的更多資訊，請參閱威脅嚴重性層級。
   - 針對 DNS 特徵碼來源，選取對於已知的惡意軟體網站進行 DNS 查詢時採取的動作。選項包括預設值、允許、封鎖或 Sinkhole。確認動作是否已設為 sinkhole。
   - 您可以透過為每個 DNS 特徵碼來源設定政策動作 **Allow**（允許）及相應的日誌嚴重性 **None**（無）來完全繞過 DNS 流量檢查。
   - 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**（延伸擷取）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。
6. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 設定）區段，確認已啟用 **Sinkhole**。為了方便您，預設 Sinkhole 位址 (sinkhole.paloaltonetworks.com) 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位址。

   Sinkhole 會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 *DNS* 類別。使用預設的 *Sinkhole FQDN (sinkhole.paloaltonetworks.com)* 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，如果用戶端位於沒有內部 *DNS* 伺服器的網路中，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。在這些情況下，您應該使用下列 *Sinkhole IP* 位址：*(72.5.65.111)*。

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。



7. 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

STEP 5 | 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）。
2. 選取或建立 **Security Policy Rule**（安全性原則規則）。
3. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段結束時記錄）核取方塊以啟用記錄。
4. 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或經過修改的設定檔。
5. 按一下 **OK**（確定）來儲存原則規則。

STEP 6 | 測試已強制執行該原則動作。

1. 存取 DNS 安全性測試網域，以確認是否正在強制執行所指定威脅類型的政策動作。
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。
   3. 如需更多監控選項，請參閱 監控 DNS 安全性訂閱服務

STEP 7 | 選用—建立解密政策規則以解密 DNS-over-TLS / 連接埠 853 流量。然後可以使用包含 DNS 政策設定的反間諜軟體設定檔設定來處理解密的 DNS 有效負載。當 DNS-over-TLS 流量遭解密時，威脅日誌中產生的 DNS 要求將顯示成來源連接埠為 853 的傳統 **dns-base** 應用程式。

STEP 8 | 選用—查看嘗試連線至惡意網域的受感染主機

啟用 DNS 安全性 (PAN-OS 9.1)

STEP 1 | 登入 NGFW。

STEP 2 | 若要利用 DNS 安全性，您必須具備有效的 DNS 安全性和威脅防護訂閱。

確認您是否擁有必要的訂閱。要確認當前哪些訂閱具有授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認顯示了適當的授權且該授權沒有過期。

STEP 3 | 確認安全性原則中的 *paloalto-dns-security* App-ID 已設定為 enable（啟用）來自 DNS 安全性雲端安全性服務的流量。

如果您的防火牆部署透過設定為強制執行 *App-ID* 安全性原則的網際網路型周邊防火牆路由管理流量，則必須允許周邊防火牆上的 *App-ID*；如果不這樣做，會阻止 *DNS* 安全性連線。

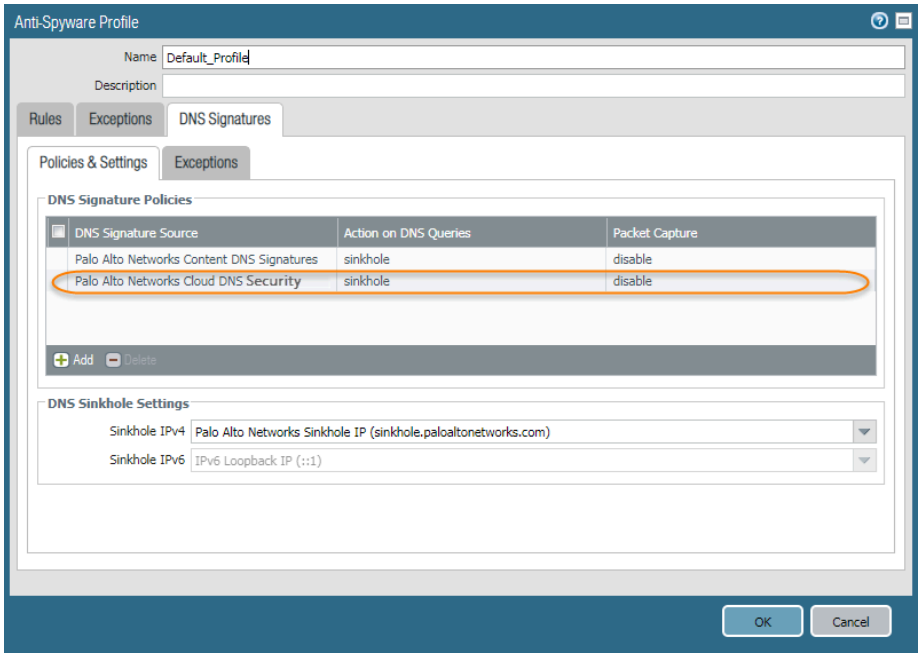
STEP 4 | 設定 DNS 安全性特徵碼原則設定以傳送惡意軟體 DNS 查詢至已定義 sinkhole。

如果您使用外部動態清單作為網域允許清單，其優先順序不會高於 *DNS* 安全性網域原則動作。因此，當有與 *EDL* 和 *DNS* 安全性網域類別中的項目相符的網域時，仍會套用 *DNS* 安全性下指定的動作，即使 *EDL* 明確設定為「允許」動作也是如此。如果您要新增 *DNS* 網域例外狀況，可以使用警示動作來設定 *EDL*。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 建立設定檔或修改現有的設定檔，或選取一個現有的預設設定檔並加以複製。
3. 輸入設定檔 **Name**（名稱），並提供說明（選用）。
4. 選取 **DNS Signatures**（**DNS** 特徵碼） > **Policies & Settings**（原則及設定）頁籤。
5. 如果沒有 **Palo Alto Networks DNS Security**（**DNS** 安全性）來源，按一下 **Add**（新增）並從清單中選取。
6. 針對 DNS 特徵碼來源，選取對於已知的惡意軟體網站進行 DNS 查詢時採取的動作。選項包括警示、允許、封鎖或 sinkhole。確認動作是否已設為 sinkhole。
7. （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。
8. 在 **DNS Sinkhole Settings**（**DNS Sinkhole** 設定）區段，確認已啟用 **Sinkhole**。為了方便您，預設 Sinkhole 位址 (sinkhole.paloaltonetworks.com) 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位址。

   Sinkhole 會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 *DNS* 類別。使用預設的 *Sinkhole FQDN (sinkhole.paloaltonetworks.com)* 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，如果用戶端位於沒有內部 *DNS* 伺服器的網路中，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。在這些情況下，您應該使用下列 *Sinkhole IP* 位址：*(72.5.65.111)*。

   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。
9. 按一下 **OK**（確定）以儲存反間諜軟體設定檔。



STEP 5 | 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）。
2. 選取或建立 **Security Policy Rule**（安全性原則規則）。
3. 在 **Actions**（動作）頁籤上，選取 **Log at Session Start**（工作階段結束時記錄）核取方塊以啟用記錄。
4. 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或經過修改的設定檔。
5. 按一下 **OK**（確定）來儲存原則規則。

STEP 6 | 測試已強制執行該原則動作。

1. 存取 DNS 安全性測試網域，以確認是否正在強制執行所指定威脅類型的政策動作。
2. 若要監控防火牆上的活動：
   1. 檢視威脅活動並搜尋您所存取網域的 URL 測試網域和封鎖的活動。
   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。
   3. 如需更多監控選項，請參閱 監控 DNS 安全性訂閱服務

STEP 7 | 選用—建立解密政策規則以解密 DNS-over-TLS / 連接埠 853 流量。然後可以使用包含 DNS 政策設定的反間諜軟體設定檔設定來處理解密的 DNS 有效負載。當 DNS-over-TLS 流量遭解密時，威脅日誌中產生的 DNS 要求將顯示成來源連接埠為 853 的傳統 **dns-base** 應用程式。

STEP 8 | 選用—查看嘗試連線至惡意網域的受感染主機

啟用進階 DNS 安全性

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 DNS 安全性授權（用於增強型功能支援） ❑ 進階威脅防護或威脅防護授權

進階 DNS 安全性可補充您現有的 DNS 安全性設定，透過檢查 DNS 回應的變更對防止 DNS 劫持提供額外的防護。繼續執行此步驟之前，您應該已完全設定 DNS 安全性設定。

若要啟用進階 DNS 安全性，您必須建立（或修改）反間諜軟體安全性設定檔，以存取進階 DNS 安全性服務、設定 DNS 特徵碼類別的日誌嚴重性和政策設定，然後將設定檔附加至安全性政策規則。

- PAN-OS 11.2 和更新版本
- 雲端管理

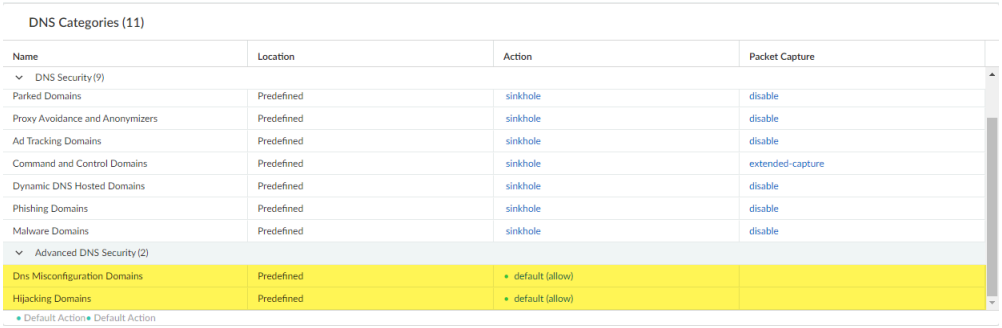
啟用進階 DNS 安全性 (Strata Cloud Manager)

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。

STEP 2 | 確認 DNS 安全性和威脅防護授權是否處於作用中狀態。選取 **Manage**（管理）> **Configuration**（設定）> **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**）> **Overview**（概要），然後按一下 **License**（授權）面板中的授權使用條款連結。您應該會在下列安全性服務旁邊看到綠色勾號：防毒、反間諜軟體、弱點保護和 DNS 安全性。

STEP 3 | 更新或建立新的 DNS 安全性設定檔，以啟用即時進階 DNS 安全性查詢。通常，這是用於 DNS 安全性設定的現有 DNS 安全性設定檔。

1. 選取現有的 DNS 安全性設定檔，或 **Add**（新增）新的設定檔（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Service**（安全性服務） > **DNS Security**（**DNS** 安全性））。
2. 選取您的 DNS 安全性設定檔，然後移至 **DNS Categories**（**DNS** 類別）。



3. 針對每個進階 DNS 安全性網域類別，指定當偵測到對應的網域類型時要採取的 **Action**（動作）。目前有兩種可用的分析引擎：**DNS Misconfiguration Domains**（**DNS** 設定錯誤網域）和 **Hijacking Domains**（劫持網域）。

   政策動作選項：

   - **allow**（允許）—允許 DNS 查詢。

     您可以設定 *Strata Cloud Manager* 以在偵測到適用的網域類型時產生警示，方法是將動作設定為 *allow*（允許），並將日誌嚴重性設定為 *informational*（僅供參考）。

   - **block**（封鎖）—DNS 查詢已封鎖。
   - **sinkhole**—針對以偵測到的惡意網域為目標的 DNS 查詢偽造 DNS 回應。這會將惡意網域名稱的解析導向到特定的 IP 位址（稱為 Sinkhole IP），該位址會作為回應嵌入。預設 Sinkhole IP 位址設定為存取 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。

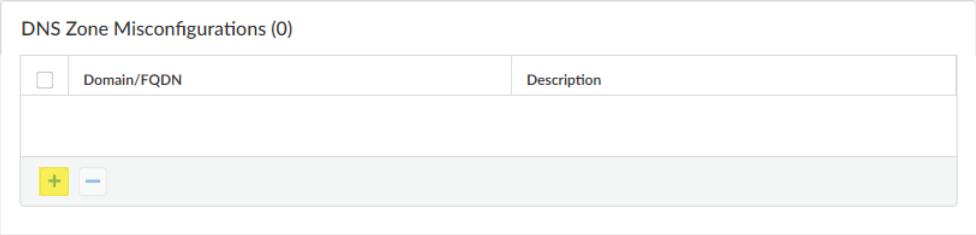
STEP 4 | （選用）指定組織內您希望進階 DNS 安全性分析和監控是否存在設定錯誤之網域的任何面向公眾父系網域。設定錯誤的網域是由網域擁有者無意中建立的，他們使用 CNAME、MX、NS

記錄類型將別名記錄指向第三方網域，使用不再有效的項目，進而使攻擊者能夠透過註冊過期或未使用的網域來接管網域。

TLD（最上層網域）和根層級網域無法新增到 *DNS* 區域設定錯誤清單中。

1. 選取包含進階 DNS 安全性設定的 DNS 安全性設定檔（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 和 **Prisma Access**） > **Security Services**（安全性服務） > **DNS Security**（**DNS** 安全性））。
2. 在 **DNS Zone Misconfigurations**（**DNS** 區域設定錯誤）區段中，新增面向公眾的父系網域以及選用說明，以協助您識別組織內的網域使用情況或擁有權。

   項目必須使用下列格式在網域中包含「.」（例如 *paloaltonetworks.com*），否則會將它剖析為主機名稱，這視為私有網域。



3. 按一下 **OK**（確定）以結束並儲存 DNS 安全性安全性設定檔。

STEP 5 | （選用）監控 Strata Cloud Manager 上使用進階 DNS 安全性偵測到的 DNS 查詢活動。使用 DNS 回應封包分析的進階 DNS 安全性即時分析加以分析的 DNS 安全性類別具有前置詞「adns」，後面接著類別。例如，adns-dnsmisconfig，其中「dnsmisconfig」表示支援的 DNS 類別類型。如果 DNS 網域類別是透過分析 DNS 要求封包決定的，則會顯示指定的類別，前置詞為「dns」，後面接著類別。例如，「dns-grayware」。

1. 存取進階 DNS 安全性測試網域，以確認是否正對指定的威脅類型強制執行政策動作。
2. 選取 **Incidents & Alerts**（事件和警示） > **Log Viewer**（日誌檢視器）。您可以根據特定類型的進階 DNS 安全性網域類別來篩選威脅日誌，例如 `threat_category.value = 'adns-hijacking'`，其中變數 `adns-hijacking` 表示已由進階 DNS 安全性歸類為惡意 DNS 劫持嘗試的 DNS 查詢。日誌中提供以下進階 DNS 安全性威脅類別：

   進階 DNS 安全性類別

   - **DNS** 劫持—`adns-hijacking`

     DNS 劫持網域有威脅 ID（UTID：109,004,100）。

   - **DNS** 設定錯誤—`adns-dnsmisconfig`

     DNS 設定錯誤網域具有三個威脅 ID，這些 ID 對應於 DNS 設定錯誤網域類型的三個變體：dnsmisconfig_zone（UTID：109,004,200), dnsmisconfig_zone_dangling (UTID:109,004,201), and dnsmisconfig_claimable_nx (UTID:109,004,202)。您可以透過交互參照與特定 DNS 設定錯誤網域類型對應的威脅 ID 值，來限制搜尋。例

如，`threat_category.value = 'adns-dnsmisconfig'` 且 `Threat ID = 109004200`，其中 109004200 表示因為 DNS 伺服器設定問題而未將流量路由至作用中網域的 DNS 設定錯誤網域其威脅 ID。

使用進階 DNS 安全性增強型回應分析進行分析的 DNS 類別。

- **DNS**—`adns-benign`
- 惡意軟體網域—`adns-malware`
- 命令與控制網域—`adns-c2`
- 網路釣魚網域—`adns-phishing`
- 動態 **DNS** 託管網域—`adns-ddns`
- 新註冊的網域—`adns-new-domain`
- 灰色軟體網域—`adns-grayware`
- 寄放網域—`adns-parked`
- 代理程式規避與匿名者—`adns-proxy`
- 廣告追蹤網域—`adns-adtracking`

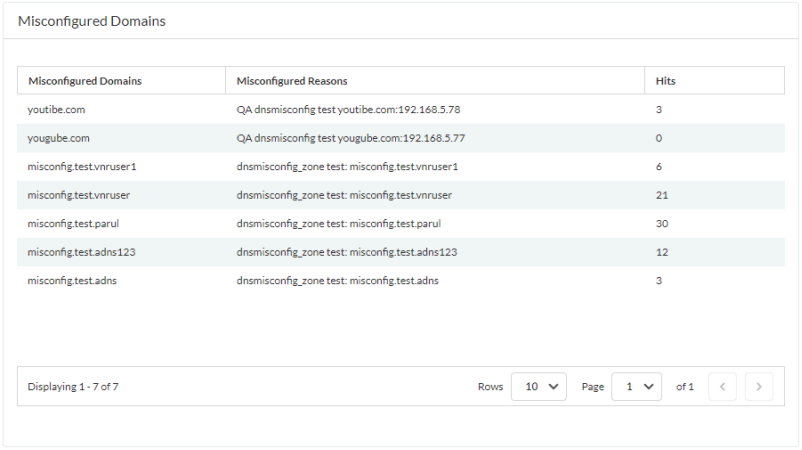
如果 *DNS* 查詢未在進階 *DNS* 安全性的指定逾時期限內完成，則會在可能的情況下使用 *DNS* 安全性分類。在這些情況下，會使用該類別的舊版標記法，例如不是分類為 *`adns-malware`*，而是 *`dns-malware`*，表示使用的是 *DNS* 安全性分類值。

3. 選取日誌項目以檢視 DNS 查詢的詳細資訊。
4. DNS **Category**（類別）顯示在詳細日誌檢視的 **General**（一般）窗格之下。此外，您還會看到威脅的其他方面，包括來源 URL、特定安全威脅類型和相關聯的特性。

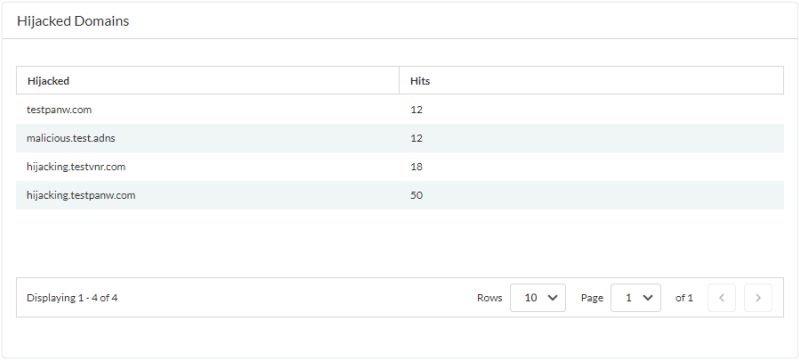
STEP 6 | （選用）擷取進階 DNS 安全性服務所偵測到設定錯誤的網域和被劫持的網域清單。設定錯誤的網域是基於新增至 **DNS Zone Misconfigurations**（**DNS** 區域設定錯誤）的面向公眾父系網域項目。

從網路中移除的設定錯誤的網域項目不會立即反映在進階 *DNS* 安全性儀表板統計資料中。

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。
2. 選取 **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **DNS Security**（**DNS** 安全性），以開啟 DNS 安全性儀表板。
3. 在 DNS 安全性儀表板中參閱下列 Widget：
   - **Misconfigured Domains**（設定錯誤的網域）—檢視與使用者所指定面向公眾的父系網域相關聯的不可解析網域清單。對於每個項目，都有一個設定錯誤原因和基於來源 IP 的流量命中計數。



   - **Hijacked Domains**（被劫持的網域）—檢視由進階 DNS 安全性判定的被劫持網域清單。對於每個項目，都有一個分類原因和基於來源 IP 的流量命中計數。



啟用進階 DNS 安全性（PAN-OS 11.2 和更新版本）

Palo Alto Networks 建議在設定進階 DNS 安全性之前啟用 DNS 安全性功能。

STEP 1 | 登入 NGFW。

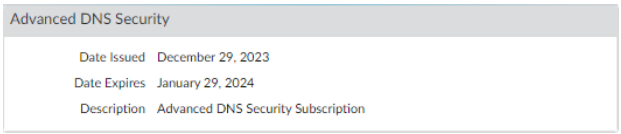
STEP 2 | 將內容發行版本更新至 8832 或更新版本。

STEP 3 | 若要防止使用進階 DNS 安全性存取已知和未知的惡意網域，您必須具備作用中的進階 DNS 安全性授權。應僅在升級到 PAN-OS 11.2 後安裝。

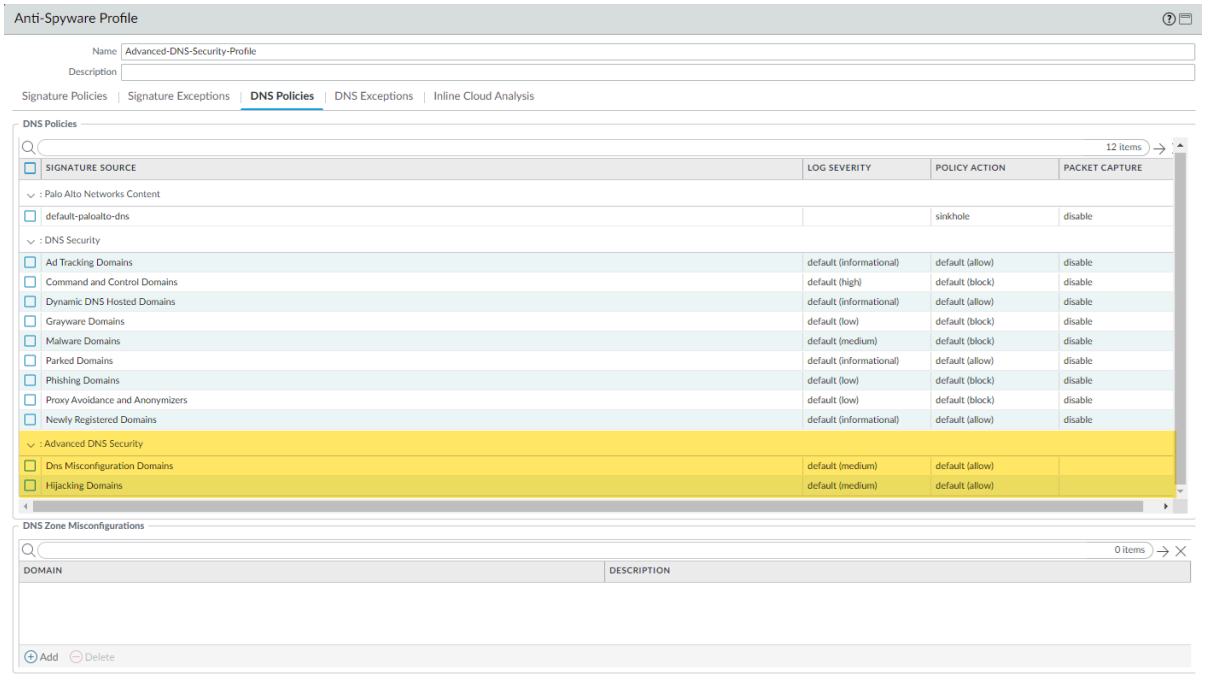
進階 *DNS* 安全性支援一種授權模型，當安裝在先前未經授權的防火牆上時，該模型會將 *DNS* 安全性功能納入進階 *DNS* 安全性授權中。如果從具有現有 *DNS* 安全性授權的防火牆升級，則會顯示項目指出存在單獨的 *DNS* 安全性和進階 *DNS* 安全性授權。在這種情況下，*DNS* 安全性授權是被動項目，所有 *DNS* 安全性和進階 *DNS* 安全性功能均透過進階 *DNS* 授權授予，包括相關的到期日。先前沒有安裝 *DNS* 安全性授權的防火牆會顯示進階 *DNS* 安全性授權，但它同時提供 *DNS* 安全性和進階 *DNS* 安全性功能。

因此，如果您從執行進階 *DNS* 安全性授權的 *PAN-OS* 版本降級到不支援進階 *DNS* 安全性的版本，則防火牆將繼續透過進階 *DNS* 安全性授權顯示和授予 *DNS* 安全性功能，但是限於基礎 *DNS* 安全性功能。

若要確認您具備哪些訂閱的目前作用中授權，請選取 **Device**（裝置） > **Licenses**（授權），並確認有可用的適當授權且該授權未過期。



STEP 4 | 更新或建立新的反間諜軟體安全性設定檔，以啟用即時進階 DNS 安全性查詢。通常，這是用於 DNS 安全性設定的現有反間諜軟體安全性設定檔。



1. 選取現有的反間諜軟體安全性設定檔，或 **Add**（新增）新的安全性設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體））。
2. 選取您的反間諜軟體安全性設定檔，然後移至 **DNS Policies**（**DNS** 政策）。
3. 對於每個進階 DNS 安全性網域類別，指定使用對應的分析引擎偵測到網域類型時，要採用的 **Log Severity**（日誌嚴重性）和 **Policy Action**（政策動作）。目前有兩種可用的分析引擎：**DNS Misconfiguration Domains**（**DNS** 設定錯誤網域）和 **Hijacking Domains**（劫持網域）。

   政策動作選項：

   - **allow**（允許）—允許 DNS 查詢。

     您可以設定防火牆以在偵測到適用的網域類型時產生警示，方法是將動作設定為 *allow*（允許），並將日誌嚴重性設定為 *informational*（僅供參考）。

   - **block**（封鎖）—DNS 查詢已封鎖。
   - **sinkhole**—針對以偵測到的惡意網域為目標的 DNS 查詢偽造 DNS 回應。這會將惡意網域名稱的解析導向到特定的 IP 位址（稱為 Sinkhole IP），該位址會作為回應嵌入。預設

Sinkhole IP 位址設定為存取 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。

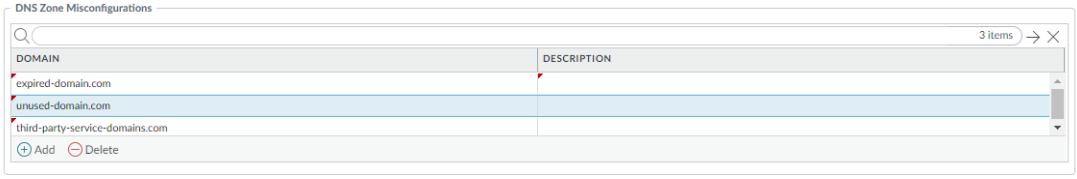
日誌嚴重性選項：

- **none**（無）—事件沒有相關聯的日誌嚴重性層級。
- **low**（低）—對組織基礎結構影響極小的警告等級威脅。這些威脅通常需要本機或實體系統存取權，具經常可能導致隱私受損或 DoS 問題和資訊洩漏。
- **informational**（僅供參考）—未產生立即威脅的可疑事件，但會報告以讓您注意可能存在的深入問題。
- **medium**（中）—帶來輕微影響的次要威脅，例如不會影響目標的 DoS 攻擊或需要攻擊者與受害者位於相同 LAN 的入侵行為，只會影響非標準設定或不重要的應用程式，或提供極其有限的存取權。
- **high**（高）—可能變為重要等級，但具有可減輕攻擊之因素的威脅；例如，難以攻擊、不會導致權限提升或沒有大型受害集區。
- **critical**（嚴重）—嚴重的威脅，例如影響廣泛部署軟體的預設安裝、導致入侵伺服器控管帳戶及攻擊者可廣泛取得攻擊指令碼。攻擊者通常不需要任何特殊驗證認證或有關個別受害者的知識，也不需要操控目標執行任何特殊功能。

4. 按一下 **OK**（確定）以結束反間諜軟體安全性設定檔設定對話方塊，並 **Commit**（提交）您的變更。

STEP 5 | （選用）指定組織內您希望進階 DNS 安全性分析和監控是否存在設定錯誤之網域的任何面向公眾父系網域。設定錯誤的網域是由網域擁有者無意中建立的，他們使用 CNAME、MX、NS 記錄類型將別名記錄指向第三方網域，使用不再有效的項目，進而使攻擊者能夠透過註冊過期或未使用的網域來接管網域。

TLD（最上層網域）和根層級網域無法新增到 *DNS* 區域設定錯誤清單中。



1. 選取反間諜軟體安全性設定檔（**Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）），並移至 **DNS Policies**（**DNS** 政策））。
2. 在 **DNS Zone Misconfigurations**（**DNS** 區域設定錯誤）區段中，新增面向公眾的父系網域以及選用說明，以協助您識別組織內的網域使用情況或擁有權。

   項目必須使用下列格式在網域中包含「.」（例如 *paloaltonetworks.com*），否則會將它剖析為主機名稱，這視為私有網域。
3. 按一下 **OK**（確定）以結束反間諜軟體安全性設定檔設定對話方塊，並 **Commit**（提交）您的變更。

STEP 6 | （選用）設定進階 DNS 特徵碼查閱逾時設定上限。超過此值時，DNS 回應將通過，而不使用進階 DNS 安全性執行分析。

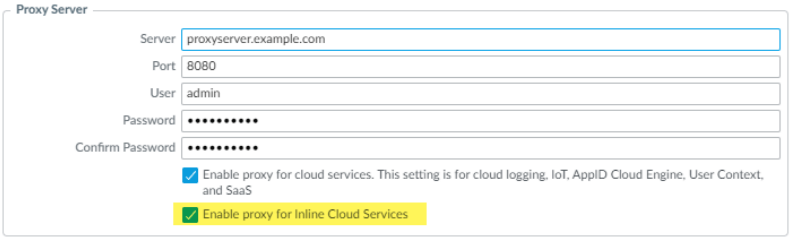
STEP 7 | （選用 [如果您沒有最新的裝置憑證]）安裝用於向進階 Threat Prevention 內嵌雲端分析服務進行驗證的更新的防火牆裝置憑證。對為內嵌雲端分析啟用的所有防火牆重複上述步驟。

如果您已在 IoT 安全性、裝置遙測、進階威脅防護或進階 URL 篩選裝載過程中，安裝了更新的防火牆裝置憑證，則無需執行此步驟。

STEP 8 | （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）。

STEP 9 | （選用） 驗證防火牆與進階 DNS 安全性雲端服務的連線狀態。

STEP 10 | （選用）監控防火牆上使用進階 DNS 安全性偵測到的 DNS 查詢活動。使用 DNS 回應封包分析的進階 DNS 安全性即時分析加以分析的 DNS 安全性類別具有前置詞「adns」，後面接著類別。例如，adns-dnsmisconfig，其中「dnsmisconfig」表示支援的 DNS 類別類型。如果 DNS 網域類別是透過分析 DNS 要求封包決定的，則會顯示指定的類別，前置詞為「dns」，後面接著類別。例如，「dns-grayware」。

1. 存取進階 DNS 安全性測試網域，以確認是否正對指定的威脅類型強制執行政策動作。
2. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅）。您可以根據特定類型的進階 DNS 安全性網域類別來篩選日誌，例如 `(category-of-threatid eq adns-`

hijacking)，其中變數 adns-hijacking 表示已由進階 DNS 安全性歸類為惡意 DNS 劫持嘗試的 DNS 查詢。日誌中提供以下進階 DNS 安全性威脅類別：

進階 DNS 安全性類別

- **DNS** 劫持—adns-hijacking

  DNS 劫持網域有威脅 ID（UTID：109,004,100）。

- **DNS** 設定錯誤—adns-dnsmisconfig

  DNS 設定錯誤網域具有三個威脅 ID，這些 ID 對應於 DNS 設定錯誤網域類型的三個變體：dnsmisconfig_zone（UTID：109,004,200), dnsmisconfig_zone_dangling (UTID:109,004,201), and dnsmisconfig_claimable_nx (UTID:109,004,202)。您可以透過交互參照與特定 DNS 設定錯誤網域類型對應的威脅 ID 值，來限制搜尋。例如，(category-of-threatid eq adns-dnsmisconfig) 且 (threatid eq 109004200)，其中 109004200 表示因為 DNS 伺服器設定問題而未將流量路由至作用中網域的 DNS 設定錯誤網域其威脅 ID。

使用進階 DNS 安全性增強型回應分析進行分析的 DNS 類別。

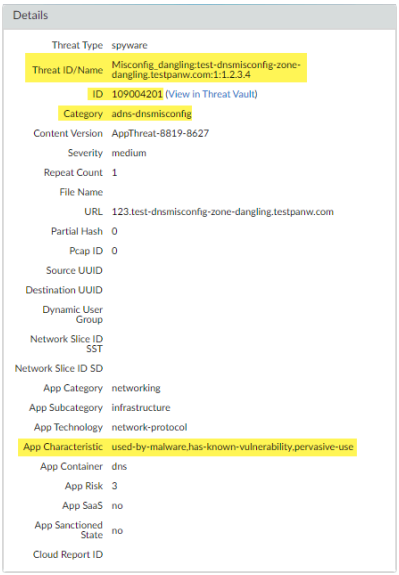
您必須運作執行 *PAN-OS 11.2* 和更新版本的防火牆，才能利用增強型進階 *DNS* 安全性即時分析。

- **DNS**—adns-benign
- 惡意軟體網域—adns-malware
- 命令與控制網域—adns-c2
- 網路釣魚網域—adns-phishing
- 動態 **DNS** 託管網域—adns-ddns
- 新註冊的網域—adns-new-domain
- 灰色軟體網域—adns-grayware
- 寄放網域—adns-parked
- 代理程式規避與匿名者—adns-proxy
- 廣告追蹤網域—adns-adtracking

如果 *DNS* 查詢未在進階 *DNS* 安全性的指定逾時期限內完成，則會在可能的情況下使用 *DNS* 安全性分類。在這些情況下，會使用該類別的舊版標記法，例如不是分類為 *adns-malware*，而是 *dns-malware*，表示使用的是 *DNS* 安全性分類值。

3. 選取日誌項目以檢視 DNS 查詢的詳細資訊。
4. DNS **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資訊）窗格之下。此外，您還可以查看威脅的其他方面，包括威脅 ID，其中包含來源網域、特定威脅類別和其他相關聯特性，以及相關聯的 Q 類型和使用下列格式的 R 資

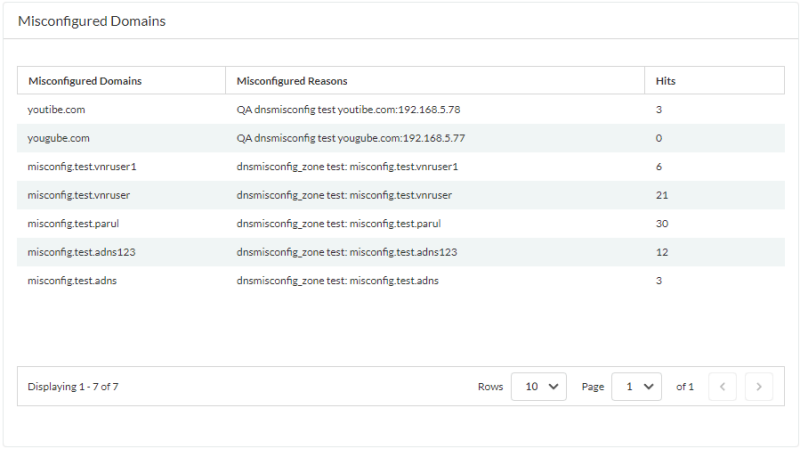
料：hijacking:<FQDN>:<QTYPE>:<RDATA>，其中 <QTYPE> 代表 DNS 資源記錄類型，<RDATA> 代表被劫持的 IP 位址。



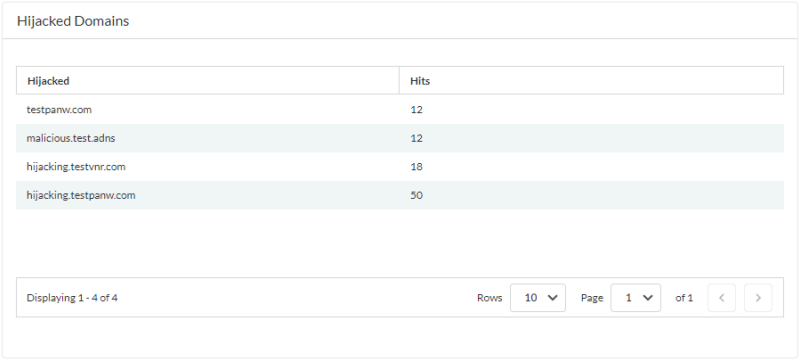
STEP 11 | （選用）擷取進階 DNS 安全性服務所偵測到設定錯誤的網域和被劫持的網域清單。設定錯誤的網域是基於新增至 **DNS Zone Misconfigurations**（**DNS** 區域設定錯誤）的面向公眾父系網域項目。

從網路中移除的設定錯誤的網域項目不會立即反映在進階 *DNS* 安全性儀表板統計資料中。

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。
2. 選取 **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **DNS Security**（**DNS** 安全性），以開啟 DNS 安全性儀表板。
3. 在 DNS 安全性儀表板中參閱下列 Widget：
   - **Misconfigured Domains**（設定錯誤的網域）—檢視與使用者所指定面向公眾的父系網域相關聯的不可解析網域清單。對於每個項目，都有一個設定錯誤原因和基於來源 IP 的流量命中計數。



   - **Hijacked Domains**（被劫持的網域）—檢視由進階 DNS 安全性判定的被劫持網域清單。對於每個項目，都有一個分類原因和基於來源 IP 的流量命中計數。



設定 DNS Security Over TLS

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

您可以藉由解密已加密 DNS 要求內包含的 DNS 有效負載，來取得 DNS Security over TLS 的可見性和控制權。然後，可以使用包含 DNS 政策設定的安全性設定檔設定，來處理解密的 DNS 有效負載。經判定源自 TLS 來源的 DNS 要求在威脅日誌中有來源連接埠 853。

- Strata Cloud Manager
- PAN-OS 和 Panorama

設定 DNS Security Over TLS (Strata Cloud Manager)

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 應用程式。

STEP 2 | 啟用 DNS 安全性 設定為檢查 DNS 要求。如果您要將相同的 **DNS Policies**（**DNS** 政策）設定用於 DNS Security over TLS 流量，則可以使用現有的安全性設定檔。

STEP 3 | 建立解密政策規則，其中包含可解密連接埠 853 上 HTTPS 流量的動作，其中包括 DNS Security over TLS 流量（請參閱解密最佳作法以取得詳細資訊）。當 DNS Security over TLS 流量已解密時，在日誌中產生的 DNS 要求會顯示為傳統的 **dns-base** 應用程式。

STEP 4 | (選用）在防火牆上搜尋已使用 DNS 安全性處理的已解密 TLS-已加密 DNS 查詢的活動。

1. 選取 **Activity**（活動） > **Log Viewer**（日誌檢視器），然後選取 **Threat**（威脅）日誌。使用查詢建立器以使用 **dns-base** 和連接埠 853（專門用於 DNS Security over TLS），來根據應用程式進行篩選，例如 `app = 'dns-base' AND source_port = 853`。
2. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
3. **Application**（應用程式）應在 **General**（一般）窗格中顯示 **dns-base**，在詳細日誌檢視的 **Source**（來源）窗格中顯示 **Port**（連接埠）。威脅的其他相關詳細資訊會顯示在相應的頁籤上。

設定 DNS Security Over TLS (NGFW (Managed by PAN-OS or Panorama))

STEP 1 | 登入 NGFW。

STEP 2 | 啟用 DNS 安全性 設定為檢查 DNS 要求。如果您要將相同的 **DNS Policies**（**DNS** 政策）設定用於 DNS Security over TLS 流量，則可以使用現有的安全性設定檔。

STEP 3 | 建立解密政策規則（類似以下範例），其中包含可解密連接埠 853 上 HTTPS 流量的動作，其中包括 DNS Security over TLS 流量（請參閱解密最佳作法以取得詳細資訊）。當 DNS Security over TLS 流量已解密時，在日誌中產生的 DNS 要求會顯示為傳統的 **dns-base** 應用程式。

		Source				Destination					Decrypt Options					
	NAME	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	URL CATEGORY	SERVICE	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSSL HAN
1	Decrypt Port 853	any	any	any	any	any	any	any	any	Port 853	decrypt	ssl-forward-proxy	default	none	false	true

STEP 4 | (選用）在防火牆上搜尋已使用 DNS 安全性處理的已解密 TLS-已加密 DNS 查詢的活動。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），以使用 **dns-base** 和連接埠 853（專門用於 DNS Security over TLS 交易），來根據應用程式進行篩選，例如 `(app eq dns-base ) 和 ( port.src eq 853)`。
2. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
3. **Application**（應用程式）應在 **General**（一般）窗格中顯示 **dns-base**，在詳細日誌檢視的 **Source**（來源）窗格中顯示 **Port**（連接埠）。威脅的其他相關詳細資訊會顯示在相應視窗。

設定 DNS Security Over DoH

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

您可以使用 HTTPS (DoH—[DNS-over-HTTPS]) 分析和分類流到 DNS 主機的加密 DNS 流量要求內包含的 DNS 有效負載。如果您的組織目前依據 Palo Alto Networks 建議封鎖所有 DoH 要求，則您可以轉移離開該政策，因為 DNS 安全性現在可讓您從加密要求中擷取 DNS 主機名稱，並套用組織現有的 DNS 安全性政策。隨著對 DoH 支援的擴展，這可以讓您安全地存取更多網站。透過設定防火牆來解密源自使用者所指定 DNS 解析程式清單的 DNS 要求有效負載，以啟用 DoH 適用的 DNS 安全性支援，來提供各種伺服器選項的支援。接著，可以使用包含 DNS 政策設定的反間諜軟體設定檔設定，來處理解密的 DNS 有效負載。已判定為 DoH 的 DNS 要求在流量日誌中會標示為 **dns-over-https**。

- Strata Cloud Manager
- PAN-OS 11.0 和更新版本

設定 DNS Security Over DoH (Strata Cloud Manager)

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。

STEP 2 | 建立自訂 URL 類別清單，其中包含您允許流量流入/出的所有 DoH 解析程式（您將需要 DNS 伺服器 URL）。

STEP 3 | 建立解密政策規則，以參照您在上一個步驟中建立的自訂 URL 類別清單。

STEP 4 | 更新或建立用於檢查 DoH 要求的新反間諜軟體安全性設定檔。

STEP 5 | 建立或更新安全政策規則，並參照 DNS 安全性設定檔和內含 DoH 伺服器核准清單的自訂 URL 類別清單（**Manage**（管理）> **Configuration**（設定）> **PAN-OS and Prisma Access**（**PAN-OS** 及 **Prisma Access**）> **Security Services**（安全性服務）> **URL Access Management**（**URL** 存取管理））。

STEP 6 | 建立封鎖政策以解密 HTTPS 流量，並透過使用 App-ID：**dns-over-https** 和下列 URL 類別：**encrypted-dns**，封鎖所有剩餘未經自訂 URL 類別清單明確允許的未認可 DoH 流量（在步驟 5 中參照）。

如果您已經有會封鎖 *DoH* 流量的現有封鎖政策，請確認該規則置於用於與自訂 *URL* 類別清單物件中所列特定 *DoH* 解析程式相符的先前安全性政策規則下方。

STEP 7 | (選用）在防火牆上搜尋已使用 DNS 安全性處理的 HTTPS 加密 DNS 查詢的活動。

1. 選取 **Activity**（活動） > **Logs**（日誌） > **Log Viewer**（日誌檢視器），然後選取 **Threat**（威脅）。
2. 使用 **dns-over-https** 根據應用程式提交日誌查詢，例如 `app = 'dns-over-https'`。
3. 選取日誌項目，以檢視所偵測到使用 DoH 的 DNS 威脅詳細資訊。
4. 威脅 **Application**（應用程式）會顯示在詳細日誌檢視的 **General**（一般）窗格。威脅的其他相關詳細資訊會顯示在相應視窗。

設定 DNS Security Over DoH（PAN-OS 11.0 和更新版本）

STEP 1 | 登入 PAN-OS 網頁介面。

STEP 2 | 建立自訂 URL 類別清單，其中包含您允許流量流入/出的所有 DoH 解析程式（您將需要 DNS 伺服器 URL）。

STEP 3 | 建立解密政策規則，以參照您在上一個步驟中建立的自訂 URL 類別清單。

STEP 4 | 更新或建立用於檢查 DoH 要求的新反間諜軟體安全性設定檔。

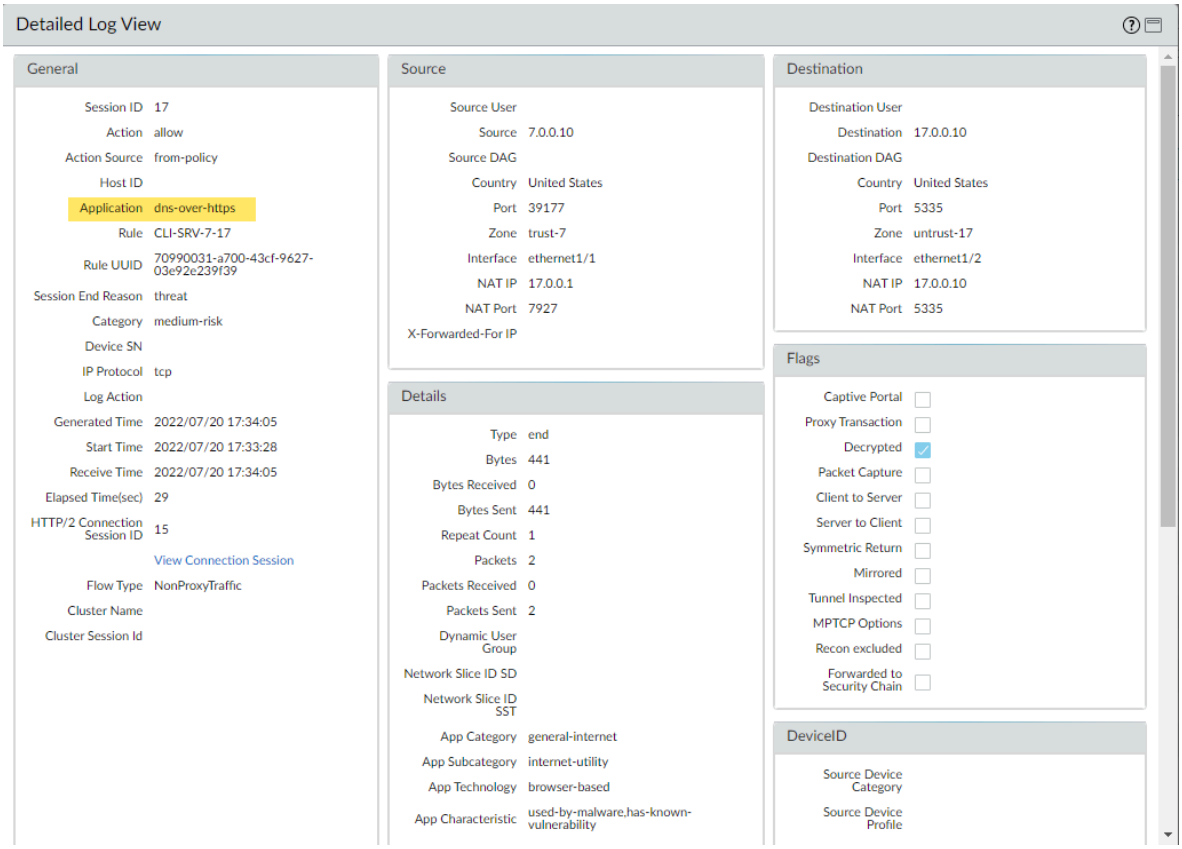
STEP 5 | 建立或更新安全性政策規則，並參照反間諜軟體設定檔和包含 DoH 伺服器核准清單的自訂 URL 類別清單（**Objects**（物件） > **Custom Objects**（自訂物件） > **URL Category**（**URL** 類別））。

STEP 6 | 建立封鎖政策以解密 HTTPS 流量，並透過使用 App-ID：**dns-over-https** 和下列 URL 類別：**encrypted-dns**，封鎖所有剩餘未經自訂 URL 類別清單明確允許的未認可 DoH 流量（在步驟 5 中參照）。

如果您已經有會封鎖 *DoH* 流量的現有封鎖政策，請確認該規則置於用於與自訂 *URL* 類別清單物件中所列特定 *DoH* 解析程式相符的先前安全性政策規則下方。

STEP 7 | (選用）在防火牆上搜尋已使用 DNS 安全性處理的 HTTPS 加密 DNS 查詢的活動。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Traffic**（流量），並使用 **dns-over-https**，例如 `(app eq dns-over-https)`，以根據應用程式篩選。
2. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
3. **Application**（應用程式）應在詳細日誌檢視的 **General**（一般）窗格中顯示 dns-over-https，表示這是已使用 DNS 安全性處理的 DoH 流量。威脅的其他相關詳細資訊會顯示在相應視窗。



建立網域例外狀況與允許 | 封鎖清單

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

DNS 安全性會為 DNS 安全性服務分析過的網域建立威脅特徵碼。對於這些已知網域，當收到 DNS 查詢時會參照該特徵碼。在某些情況下，由於網域中存在某些功能或品質，因此該特徵碼可能會錯誤地將網域歸類為威脅。在這種情況下，您可以新增特徵碼例外狀況來繞過這些誤判。如果有已知為安全的網域（例如內部網域）被歸類為惡意，您可以新增一個會繞過任何 DNS 分析的網域清單。如果您的組織使用第三方威脅摘要作為全方位威脅情報解決方案的一部分，您也可以在 DNS 安全性設定檔中以外部動態清單 (EDL) 形式參照這些威脅摘要。

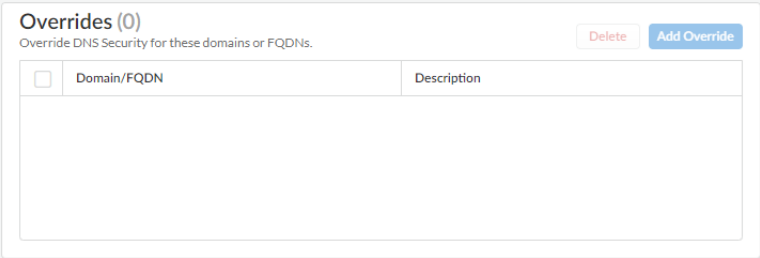
- Strata Cloud Manager
- PAN-OS 和 Panorama

建立網域例外狀況與允許 | 封鎖清單 (Strata Cloud Manager)

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。

STEP 2 | 在發生誤判的情況下新增網域取代。

1. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **DNS Security**（**DNS** 安全性），然後選取要修改的 DNS 安全性設定檔。
2. **Add Override**（新增取代）或 **Delete**（刪除），以視需要修改網域清單項目。每個附加項目都需要網域和說明。



3. 按一下 **OK**（確定）以儲存已修改的 DNS 安全性設定檔。

STEP 3 | 參照外部動態清單 (EDL) 作為 DNS 安全性設定檔的一部分，來匯入第三方威脅摘要。

1. 建立基於網域的外部動態清單（**Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Objects**（物件） > **External Dynamic Lists**（外部動態清單））。有關 EDL 的詳細資訊，請參閱外部動態清單。
2. 選取 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **DNS Security**（**DNS** 安全性）。
3. 在 **External Dynamic Lists**（外部動態清單）面板中，選取網域清單 EDL 並提供 **Policy Action**（政策動作）和 **Policy Action**（封包擷取）設定。在 **Apply to Profiles**（套用到設定檔）中，選擇您想要套用 EDL 網域清單的 DNS 安全性設定檔。
4. 完成更新後 **Save**（儲存）變更。

建立網域例外狀況與允許 | 封鎖清單 (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 和更新版本提供一個附加選項，可透過反間諜軟體安全性設定檔明確新增可允許的網域。如果核准的網域來源會觸發來自 DNS 安全性的誤判回應，您可以為該來源新增網域/FQDN 項目。

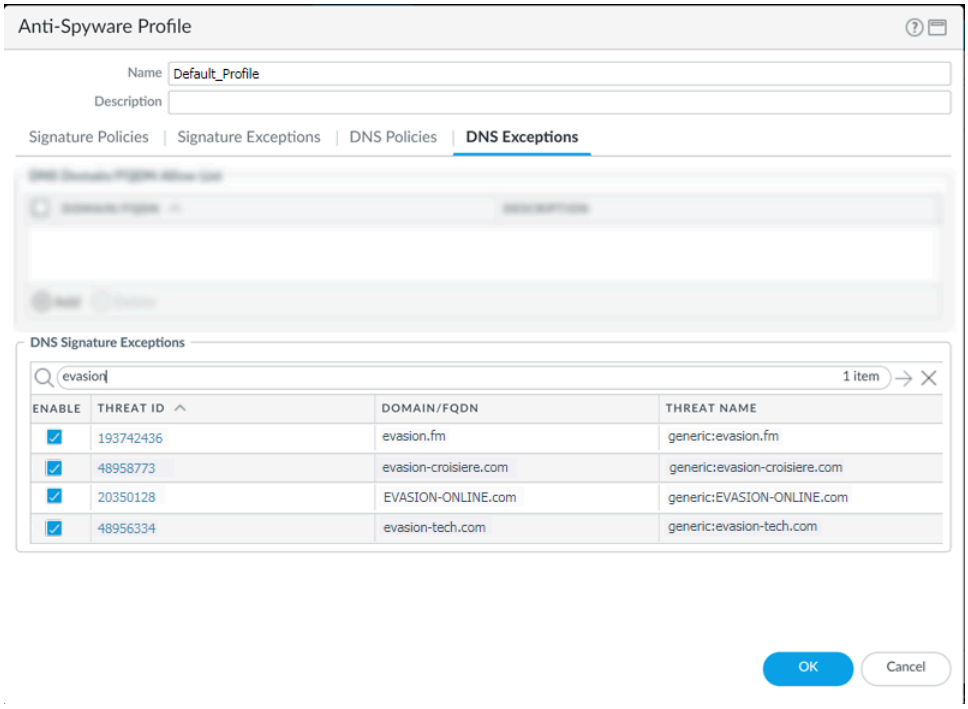
- PAN-OS 10.0 和更高版本
- PAN-OS 9.1

建立網域例外狀況與允許 | 封鎖清單（**PAN-OS 10.0** 和更新版本）

登入 NGFW。

新增發生誤判時的網域特徵碼例外狀況。

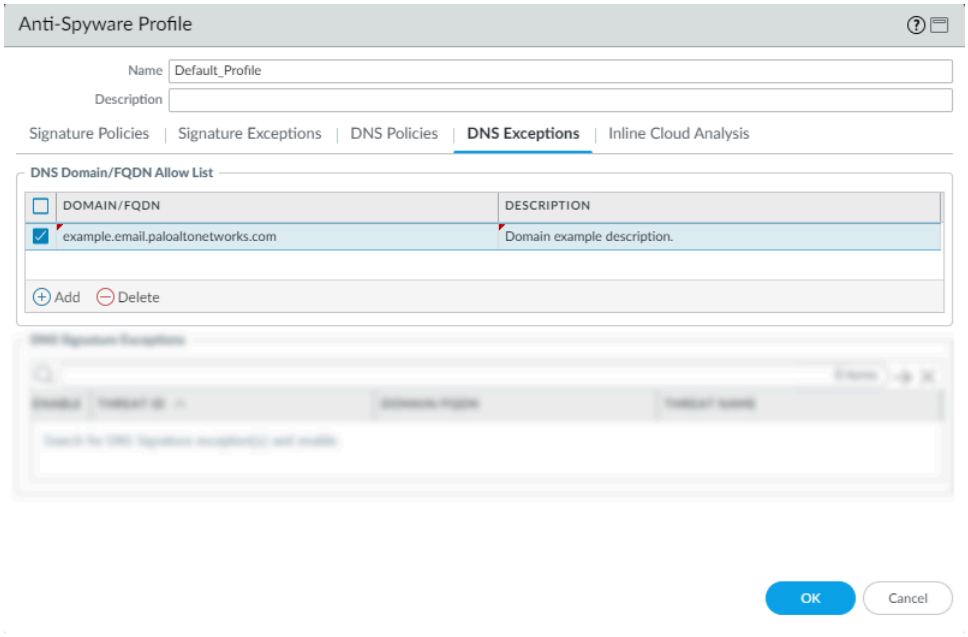
1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 選取要修改的設定檔。
3. **Add**（新增）或修改您希望從中排除威脅特徵碼的反間諜軟體設定檔，然後選取 **DNS Exceptions**（**DNS** 例外）。
4. 透過輸入名稱或 FQDN 搜尋要排除的 DNS 特徵碼。
5. 為您要從強制執行中排除的 DNS 特徵碼選取每個 **Threat ID**（威脅 **ID**）的核取方塊。



6. 按一下 **OK**（確定）以儲存新的或修改後的反間諜軟體設定檔。

新增允許清單以指定明確允許的 DNS 網域/FQDN 的清單。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 選取要修改的設定檔。
3. **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）。
4. 若要 **Add**（新增）新的 FQDN 允許清單，請提供 DNS 網域或 FQDN 位置和說明。



5. 按一下 **OK**（確定）以儲存新的或修改後的反間諜軟體設定檔。

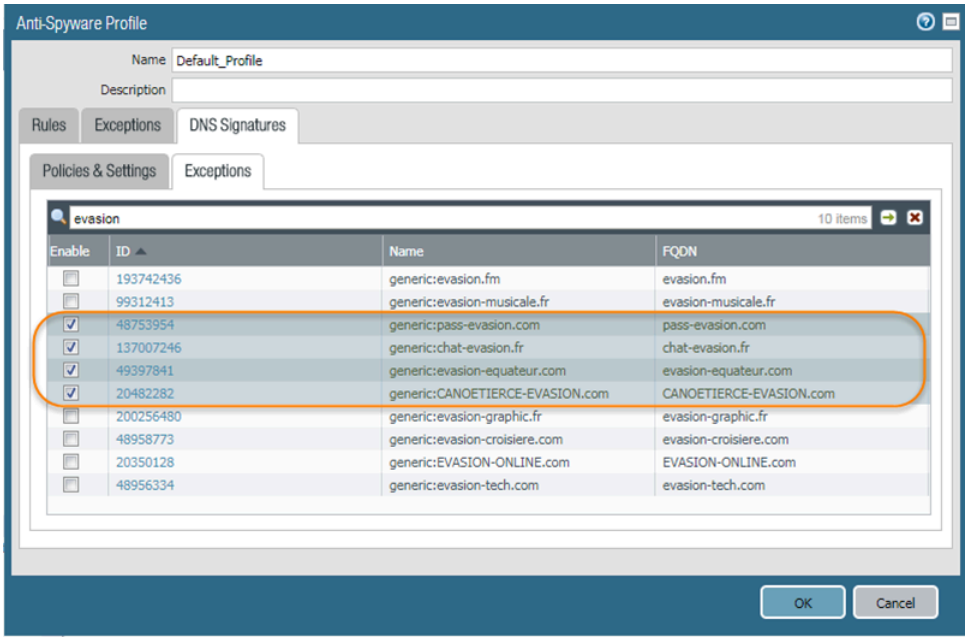
建立網域例外狀況與允許 | 封鎖清單 (PAN-OS 9.1)

允許和封鎖清單在 *PAN-OS 9.1* 中不可用。

登入 NGFW。

新增發生誤判時的網域特徵碼例外狀況。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 選取要修改的設定檔。
3. **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 Signatures > Exceptions**（**DNS** 特徵碼 > 例外）。
4. 透過輸入名稱或 FQDN 搜尋要排除的 DNS 特徵碼。
5. 為您要從強制執行中排除的 DNS 特徵碼選取 **DNS Threat ID**（**DNS** 威脅 **ID**）。



6. 按一下 **OK**（確定）以儲存新的或修改後的反間諜軟體設定檔。

測試網域

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

Palo Alto Networks 提供下列 DNS 安全性測試網域，來根據 DNS 類別驗證您的政策設定。

STEP 1 | 存取以下測試網域，以為一特定威脅類型驗證被強制執行的原則動作：

DNS 安全性

- C2—test-c2.testpanw.com
- DNS 通道—test-dnstun.testpanw.com
- DGA—test-dga.testpanw.com
- 動態 DNS*—test-ddns.testpanw.com
- 惡意軟體—test-malware.testpanw.com
- 新註冊的網域*—test-nrd.testpanw.com
- 網路釣魚*—test-phishing.testpanw.com
- 灰色軟體*—test-grayware.testpanw.com
- 寄放*—test-parked.testpanw.com
- Proxy Avoidance and Anonymizers*—test-proxy.testpanw.com
- Fast Flux*—test-fastflux.testpanw.com
- 惡意 NRD*—test-malicious-nrd.testpanw.com
- NXNS 攻擊*—test-nxns.testpanw.com
- 懸置*—test-dangling-domain.testpanw.com
- DNS 重新繫結*—test-dns-rebinding.testpanw.com
- DNS 滲透*—test-dns-infiltration.testpanw.com
- 萬用字元濫用*—test-wildcard-abuse.testpanw.com
- 策略性老化*—test-strategically-aged.testpanw.com
- 受危害的 DNS*—test-compromised-dns.testpanw.com
- 廣告追蹤*—test-adtracking.testpanw.com
- CNAME 偽裝*—test-cname-cloaking.testpanw.com
- 勒索軟體*—test-ransomware.testpanw.com
- 庫存*—test-stockpile-domain.testpanw.com
- 域名搶註*—test-squatting.testpanw.com
- 子網域信譽*—test-subdomain-reputation.testpanw.com

PAN-OS 9.1 不支援標示 * 的測試網域。

進階 **DNS** 安全性

存取以下測試網域，以確認正在強制執行所指定威脅類型的政策動作：

- **DNS** 設定錯誤網域（可宣告）—http://test-dnsmisconfig-claimable-nx.testpanw.com

在存取該網域之前，應將下列測試網域測試案例新增至 testpanw.com 的 DNS 伺服器區域檔案。這些測試案例會與進階 DNS 安全性特徵碼進行比對，並將產生適當的日誌。確認正在強制執行所指定威脅類型的政策動作。

表 **1: DNS** 設定錯誤網域（區域懸置）測試案例

主機型	記錄類型	記錄資料
*.test-dnsmisconfig-zone-dangling.testpanw.com	A	1.2.3.4

表 **2:** 劫持網域測試案例

主機型	記錄類型	記錄資料
test-ipv4.hijacking.testpanw.com	A	1.2.3.5
*.test-ipv4-wildcard.hijacking.testpanw.com	A	1.2.3.6
test-ipv6.hijacking.testpanw.com	AAAA	2607:f8b0:4005:80d::2005
test-cname-rrname.hijacking.testpanw.com	CNAME	1.test-cname-wc.hijacking.testpanw.com
test-cname-rrname-wc.hijacking.testpanw.com	CNAME	1.test-cname-wildcard-1.hijacking.testpanw.com
*.test-cname-rrname-sub-wc.hijacking.testpanw.com	CNAME	2.test-cname-wc.hijacking.testpanw.com
test-ns-rrname.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-ns-rrname-rdata-wc.hijacking.testpanw.com	NS	1.test-ns-wc.hijacking.testpanw.com
1.test-ns-rrname-sub-wc.hijacking.testpanw.com	NS	test-ns.hijacking.testpanw.com
test-rrname-wc.hijacking.testpanw.com	NS	test-ns-2.hijacking.testpanw.com

對於 *NS* 記錄，您必須使用以下選項：「***dig +trace NS***」

STEP 2 | 透過監控活動來確認 DNS 安全性已處理 DNS 查詢要求。

測試與 DNS 安全性雲端服務的連線

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

DNS 安全性

驗證與 DNS 安全性服務的防火牆連線。如果您無法連線服務，請確認以下網域未被封鎖：dns.service.paloaltonetworks.com。

STEP 1 | 存取防火牆 CLI。

STEP 2 | 使用下列 CLI 命令來驗證防火牆與 DNS 安全性服務的連線可用性。

```
show dns-proxy dns-signature info
```

例如：

```
show dns-proxy dns-signture info Cloud URL:
 dns.service.paloaltonetworks.com:443 Telemetry URL:
 io.dns.service.paloaltonetworks.com:443 Last Result:None Last
 Server Address:Parameter Exchange:Interval 300 sec Allow List
 Refresh:Interval 43200 sec Request Waiting Transmission:0 Request
 Pending Response:0 Cache Size:0
```

如果您的防火牆與 DNS 安全性服務有作用中的連線，則伺服器詳細資訊會顯示在回應輸出中。

STEP 3 | 擷取指定網域的交易詳細資料，例如延遲、TTL 和特徵碼類別。

在防火牆上使用以下 CLI 命令以檢閱網域相關詳細資訊：

```
test dns-proxy dns-signature fqdn
```

例如：

```
test dns-proxy dns-signature fqdn www.yahoo.com DNS
 Signature Query [ www.yahoo.com ] Completed in 178 ms
 DNS Signature Response Entries:2 Domain Category GTID TTL
 ------------------------------------------------------------------------
 *.yahoo.com Benign 0 86400 www.yahoo.com Benign 0 3600
```

進階 DNS 安全性

驗證與進階 DNS 安全性服務的防火牆連線。如果您無法存取服務，請確認下列網域未遭封鎖：adv-dns.service.paloaltonetworks.com。如果您已手動設定區域進階 DNS 安全性伺服器，則可能需要確認特定區域網域也已解除封鎖。

驗證防火牆與進階 DNS 安全性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 ADNS(1)
 Current cloud server: qa.adv-dns.service.paloaltonetworks.com:443
 Cloud connection: connected Config:gRPC 連線數：2，工作人員數：8 偵
錯層級：2，不安全的連線：false，憑證有效：true，金鑰有效：true，CA 計
數：306 工作人員上限：12 工作人員在重新連線之前應處理的工作階段數上
限：10240 每個工作人員的訊息數上限：0 略過憑證驗證：false Grpc 連線狀
態：狀態準備就緒 (3)，last err rpc error: code = Unavailable desc
 = unexpected HTTP status code received from server:502 (Bad
 Gateway); transport: received unexpected content-type "text/
html" Pool state:準備就緒 (2) 上次更新：2024-01-24 11:15:00.549591469
 -0800 PST m=+1197474.129493596 last connection retry:2024-01-23
 00:03:09.093756623 -0800 PST m=+1070762.673658768 last pool
 close:2024-01-22 14:15:50.36062031 -0800 PST m=+1035523.940522446
 Security Client AdnsTelemetry(2) Current cloud server: io-qa.adv-
dns.service.paloaltonetworks.com:443 Cloud connection: connected
 Config:gRPC 連線數：2，工作人員數：8 偵錯層級：2，不安全的連線：false，
憑證有效：true，金鑰有效：true，CA 計數：306 工作人員上限：12 工作人員在
重新連線之前應處理的工作階段數上限：10240 每個工作人員的訊息數上限：0 略過
憑證驗證：false Grpc 連線狀態：State Ready (3), last err rpc error:
 code = Internal desc = stream terminated by RST_STREAM with error
 code:PROTOCOL_ERROR Pool state:Ready (2) last update:2024-01-24
 11:25:58.340198656 -0800 PST m=+1198131.920100772 last connection
 retry:2024-01-23 00:03:36.78141425 -0800 PST m=+1070790.361316421
 last pool close:2024-01-22 14:24:26.954340157 -0800 PST m=
+1036040.534242289 ...
```

確認 `Security Client AdnsTelemetry(2)` 和 `Security Client ADNS(1)` 的雲端連線顯示作用中的連線。

為簡潔起見，縮短了 *CLI* 輸出。

如果您無法連線到進階 DNS 安全性雲端服務，請確認未封鎖進階 DNS 伺服器：dns.service.paloaltonetworks.com。

設定查閱逾時

我可以在哪裡使用這個？	我需要哪些內容？
• NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

DNS 安全性

如果防火牆由於連線問題而無法在指定期限內擷取特徵碼裁定，則通過包括所有後續 DNS 回應在內的要求。您可以檢查平均延遲時間，以驗證要求是否在設定的時間內。如果平均延遲時間超過設定的時間段，請考慮將設定更新為高於平均延遲時間的值，以防止要求逾時。

STEP 1 | 在 CLI 中，發出以下命令以檢視平均延遲。

```
show dns-proxy dns-signature counters
```

預設逾時為 100 毫秒。

STEP 2 | 向下捲動特徵碼查詢 API 標題下的輸出至延遲部分，然後驗證平均延遲是否在定義的逾時時間內。該延遲顯示從 DNS 安全性服務擷取特徵碼裁定所花的平均時間。可以在平均值以下找到各種延遲時段的其他延遲統計資料。

```
Signature query API: . . . [latency ] : max 1870 (ms) min 16(ms)
 avg 27(ms) 50 or less :47246 100 or less :113 200 or less :25 400
 or less :15 else :21
```

STEP 3 | 如果平均延遲一直高於預設逾時值，則您可以提高設定，以使要求在給定時間段內處理。選取 **Device**（裝置）> **Content-ID**，然後更新**Realtime Signature Lookup**（即時特徵碼查閱）設定。

STEP 4 | Commit（提交）變更。

進階 DNS 安全性

STEP 1 | 使用以下偵錯 CLI 命令檢視進階 DNS 安全性要求的往返時間記錄（以毫秒為單位）。這些要求會分散在從 0 毫秒到 450 毫秒的延遲範圍內。您可以用來決定 NGFW 的理想延遲上限設定。

```
admin@PA-VM 偵錯資料平面顯示 ctd feature-forward 統計資料
```

在回應輸出中，導覽至 `PAN_CTDF_DETECT_SERVICE_ADNS` 區段。

```
PAN_CTDF_DETECT_SERVICE_ADNS cli_timeout:1 req_total:2
 req_timed_out:0 Hold: adns rtt>=0ms:0 adns rtt>=50ms:2 adns
 rtt>=100ms:0 adns rtt>=150ms:0 adns rtt>=200ms:0 adns rtt>=250ms:0
 adns rtt>=300ms:0 adns rtt>=350ms:0 adns rtt>=400ms:0 adns
 rtt>=450ms:0
```

STEP 2 | 設定進階 DNS 特徵碼查閱逾時設定上限。超過此值時，DNS 回應將通過，而不使用進階 DNS 安全性執行分析。仍會套用透過常規內容更新交付的或屬於已設定 EDL（外部動態清單）或 DNS 例外狀況的 DNS 特徵碼（及其相關聯的政策）。

1. 選取 **Device**（裝置） > **Setup**（設定） > **Content-ID**（內容-ID） > **Advanced DNS Security**（進階 **DNS** 安全性）。
2. 指定更新後的進階 DNS 特徵碼查閱逾時設定（以毫秒為單位）。預設值為 100 毫秒，是建議的設定。
3. 按一下 **OK**（確定）確認您的變更。

或者，您可以使用以下 CLI 命令設定進階 DNS 安全性逾時值。您能夠以 100 毫秒為增量設定 100-15,000 毫秒的值。預設值為 100 毫秒，是建議的設定。

```
admin@PA-VM#set deviceconfig setting adns-setting max-latency
 <timeout_value_in_milliseconds>
```

例如：

```
admin@PA-VM# set deviceconfig setting adns-setting max-latency 500
```

您可以使用以下 CLI 命令檢查目前逾時設定（請參閱輸出的 **max-latency** 項目）。

```
admin@PA-VM show config pushed-template ... }
 deviceconfig { setting { dns { dns-cloud-server dns-
qa.service.paloaltonetworks.com; } adns-setting { max-latency
 100; } } } ...
```

繞過 DNS 安全性訂閱服務

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

如果有延遲問題或其他網路問題，則可以繞過 DNS 安全性查詢。

如果發生誤判，*Palo Alto Networks* 建議建立特定例外狀況，而不是繞過 *DNS* 安全性查詢。

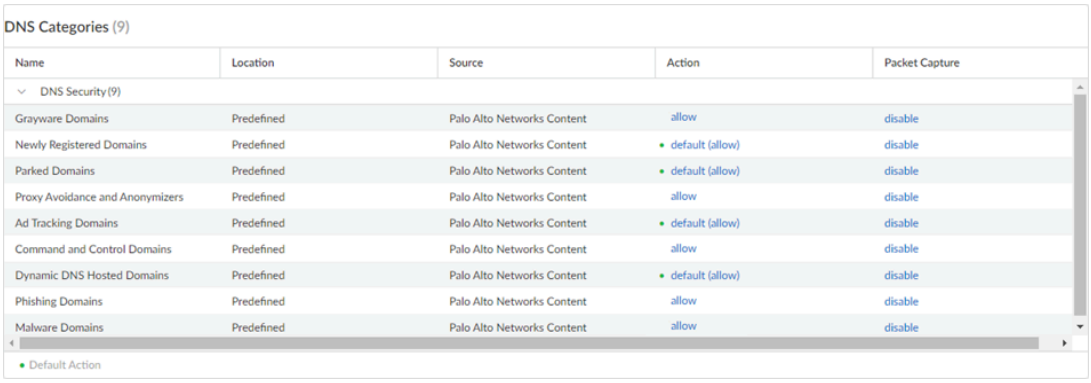
- 雲端管理
- PAN-OS 和 Panorama

繞過 DNS 安全性訂閱服務 (Strata Cloud Manager)

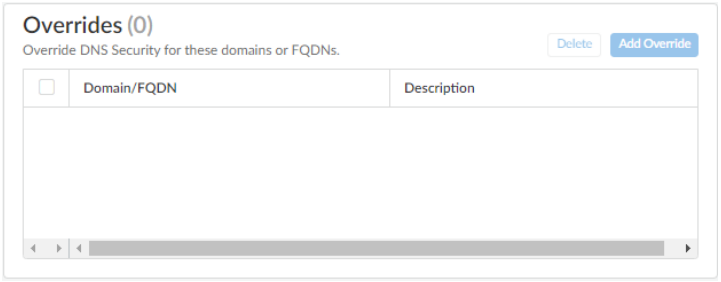
STEP 1 | 使用與您的 Palo Alto Networks 支援帳戶相關聯的認證，並登入中樞上的 Strata Cloud Manager。

STEP 2 | 前往 **Manage**（管理） > **Configuration**（設定） > **NGFW and Prisma Access**（**NGFW** 及 **Prisma Access**） > **Security Services**（安全性服務） > **DNS Security**（**DNS** 安全性），然後選取相關的 DNS 安全性設定檔。

STEP 3 | 設定 DNS 安全性特徵碼政策設定，以繞過 DNS 安全性查詢。對於每個 DNS 類別，將 **Action**（動作）設為 **allow**（允許），將 **Packet Capture**（封包擷取）設為 **disabled**（已停用）。在下文中，DNS 安全性類別已設定為繞過 DNS 安全性查詢。



STEP 4 | 在 **Overrides**（取代）區段中，確認沒有項目存在；視需要刪除所有的 **Domain/FQDN**（網域/**FQDN**）取代。



STEP 5 | 按一下 **OK**（確定）儲存 DNS 安全性設定檔。

繞過 DNS 安全性訂閱服務 (NGFW (Managed by PAN-OS or Panorama))

PAN-OS 10.0 和更新版本支援可個別設定的 DNS 特徵碼來源，讓能夠您針對指定的特徵碼來源定義單獨的政策動作以及日誌嚴重性層級。這需要您針對每個可用的 DNS 特徵碼來源設定政策動作和日誌嚴重性，以繞過 DNS 安全性。此外，您還必須移除 DNS 例外狀況項目，才能完全繞過 DNS 安全性。在 PAN-OS 9.1 上，您只需將 Palo Alto Networks DNS 安全性的政策動作設定為允許動作。

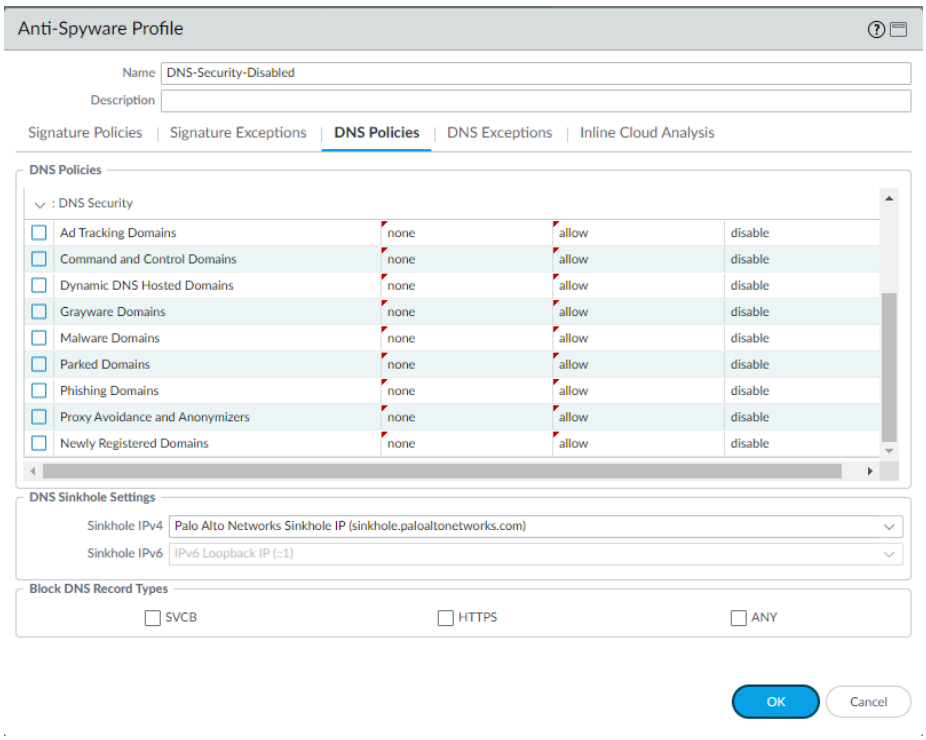
- PAN-OS 10.0 和更高版本
- PAN-OS 9.1

繞過 **DNS** 安全性訂閱服務（**PAN-OS 10.0** 和更新版本）

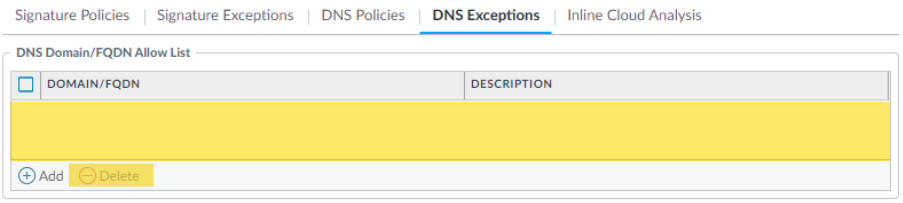
STEP 1 | 登入 NGFW。

STEP 2 | 設定 DNS 安全性特徵碼政策設定，以繞過 DNS 安全性查詢。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 選取包含作用中 DNS 安全性政策設定的設定檔。
3. 選取 **DNS Policies**（**DNS** 原則）頁簽。
4. 對於每個 DNS 類別，將日誌嚴重性設為 **none**（無），將政策動作設為 **allow**（允許），並將封包擷取設為 **disable**（停用）。在下文中，DNS 安全性類別已設定為繞過 DNS 安全性查詢。



STEP 3 | 選取 **DNS Exceptions**（**DNS** 例外狀況），並移除所有 **DNS Domain/FQDN Allow List**（**DNS** 網域/**FQDN** 允許清單）項目。



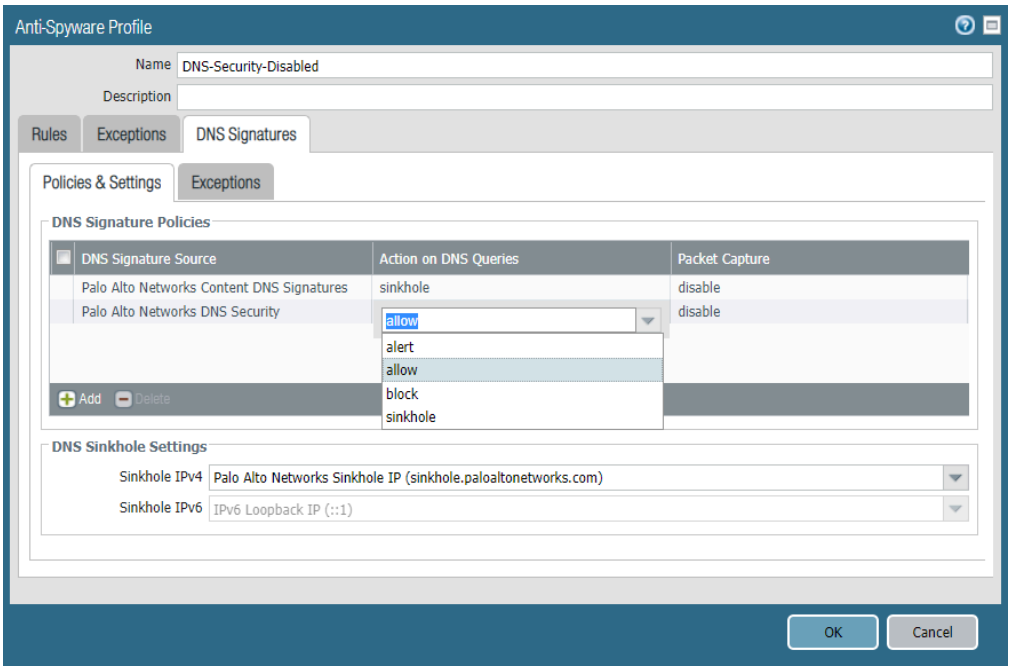
STEP 4 | 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

繞過 DNS 安全性訂閱服務 (PAN-OS 9.1)

STEP 1 | 登入 NGFW。

STEP 2 | 設定 DNS 安全性特徵碼政策設定，以繞過 DNS 安全性查閱。

1. 選取 **Objects**（物件） > **Security Profiles**（安全性設定檔） > **Anti-Spyware**（反間諜軟體）。
2. 選取包含作用中 DNS 安全性政策設定的設定檔。
3. 選取 **DNS Signatures**（**DNS** 特徵碼）頁籤。
4. 在 **Policies & Settings**（政策與設定）下，將 **Palo Alto Networks DNS Security**（**Palo Alto Networks DNS** 安全性）的政策動作設為 **allow**（允許）的動作。



STEP 3 | 按一下 **OK**（確定）以儲存反間諜軟體設定檔。

監控 DNS 安全性訂閱服務

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

Palo Alto Networks 提供數個選項來監控 DNS 安全性和進階 DNS 安全性活動，以適應一系列依賴 DNS 安全性訂閱服務和相關聯流量資料的產品其情報擷取。根據產品平台，您可以存取高階儀表板，這些儀表板會以記錄資料形式，提供 DNS 要求統計資料和使用趨勢，其中包括網路活動脈絡，以及特定使用者的特定 DNS 要求詳細資料。

您也可以檢視 DNS 安全性訂閱服務如何與其他 Palo Alto Networks 應用程式和安全性服務整合，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。

有關 DNS 安全性訂閱服務作業的更多具體詳細資訊，儀表板提供網路 DNS 查詢資料的檢視，以及可深入瞭解各種 DNS 趨勢的功能。每個儀表板卡片都提供一個獨特的檢視，以圖形報告形式顯示 DNS 要求和回應的處理和分類方式。這使您可以一目瞭然組織 DNS 使用統計資訊的概況檢視。它還提供進階 DNS 安全性服務所偵測到設定錯誤的網域和被劫持的網域清單，使您能夠修正任何 DNS 設定錯誤。設定錯誤的網域是基於新增至 **DNS Zone Misconfigurations**（**DNS** 區域設定錯誤）清單的面向公眾父系網域項目。

您也可以檢視在處理 DNS 要求時自動產生的日誌。這些事件檔案帶有時間戳記，並在設定根據 DNS 類別日誌設定時提供稽核追蹤。DNS 日誌項目可以包含有關 DNS 要求的各種詳細資訊，包括相關聯網域造成的 DNS 威脅性質，以及偵測到威脅時採取的動作。

Palo Alto Networks 提供多種方法來根據您的平台監控 DNS 安全性活動。

- Strata Cloud Manager 控管中心
- 檢視 DNS 安全性儀表板
- 檢視 DNS 安全性日誌以瞭解透過我的網路傳遞的 DNS 查詢

檢視 DNS 安全性儀表板

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

DNS 安全性儀表板在組織 DNS 使用情況的快速、視覺化評估報告中，顯示進階 DNS 安全性和 DNS 安全性訂閱服務產生的統計資料。檢視並深入瞭解網路中發現的各種 DNS 趨勢。每個儀表板卡片都提供一個獨特的檢視，顯示 DNS 要求的處理和分類方式。選取儀表板卡片以變更儀表板的內容，或檢視有關特定趨勢、網域或統計資料的詳細資訊。

DNS 安全性儀表板適用於 Prisma Access 和 AIOps for NGFW。您可以與 DNS 安全性儀表板卡片 互動以改變儀表板的內容，或檢視有關特定趨勢、網域或統計資料的詳細資訊。您也可以自訂格式以顯示相關資料點的目前趨勢或歷史資料。

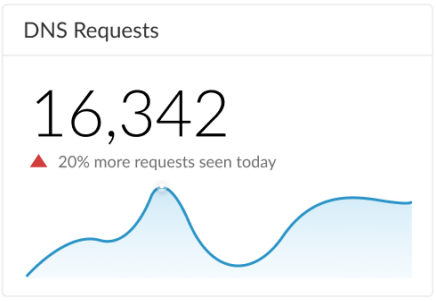
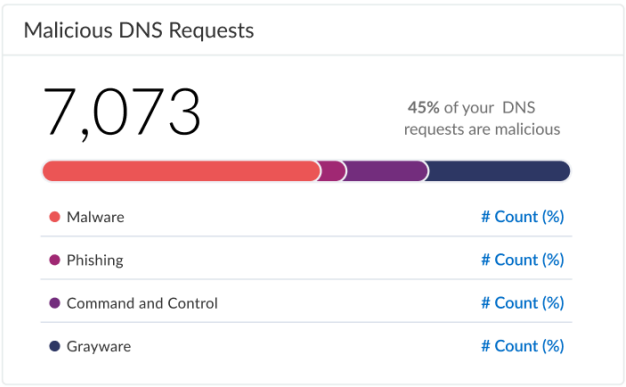
- Strata Cloud Manager
- AIOps for NGFW 免費版

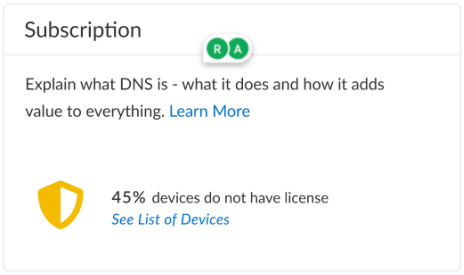
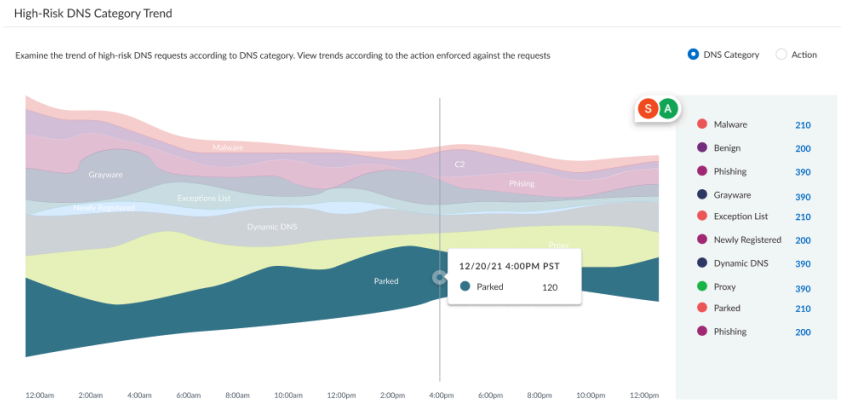
DNS 安全性儀表板卡片

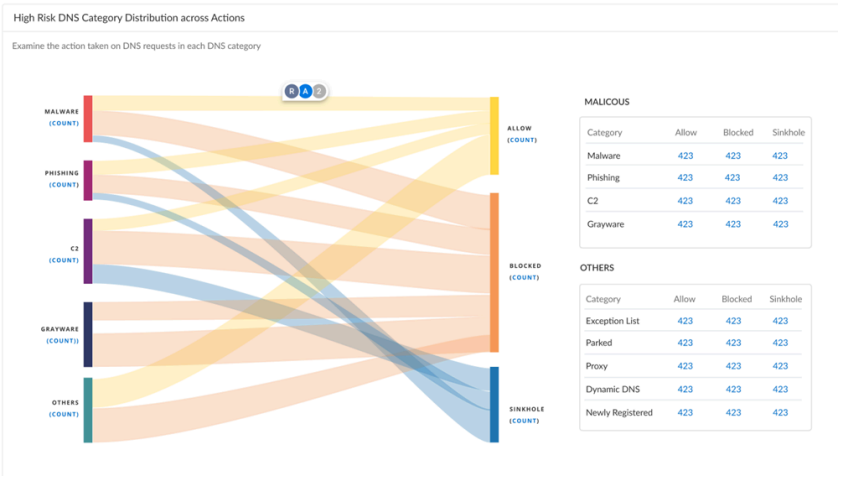
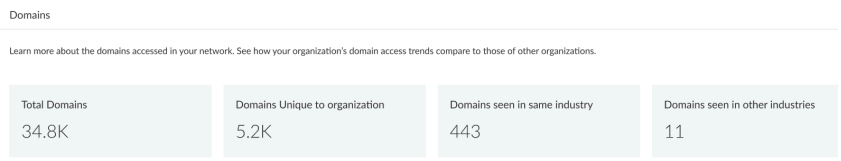
我可以在哪裡使用這個？	我需要哪些內容？
• Prisma Access (Managed by Strata Cloud Manager) • Prisma Access (Managed by Panorama) • NGFW (Managed by Strata Cloud Manager) • NGFW (Managed by PAN-OS or Panorama) • VM-Series • CN-Series	❑ 進階 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

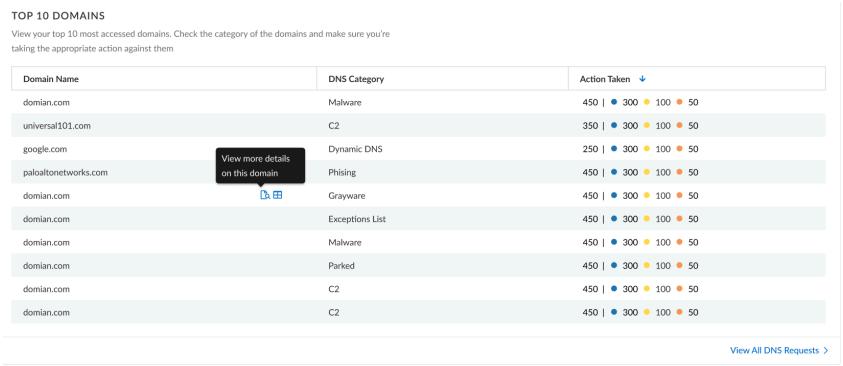
填入 DNS 安全儀表板的卡片是互動的，可讓您檢視其他詳細資訊或轉換至特定要求、事件和網域清單，因為它與內容的顯示方式有關。

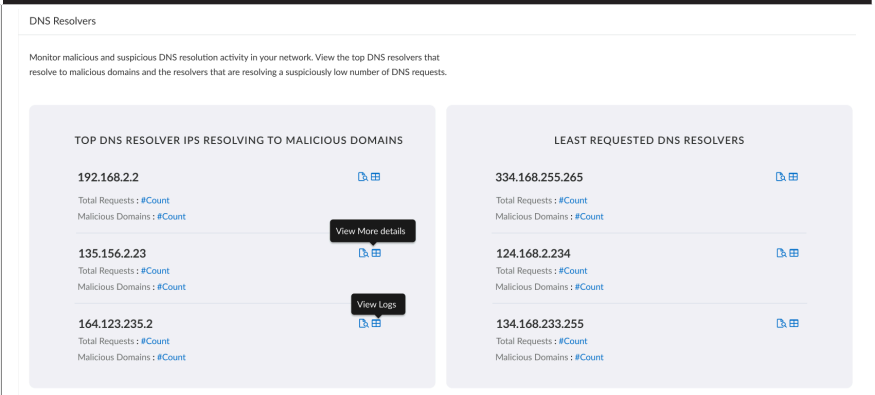
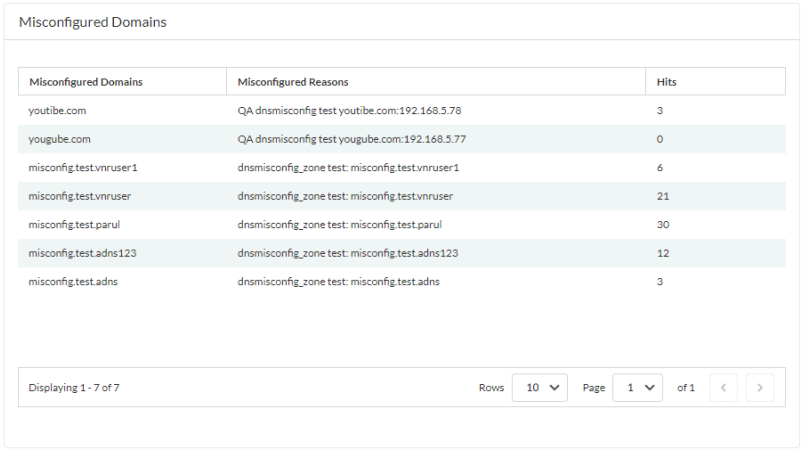
以下清單提供 DNS 安全儀表板卡片概要：

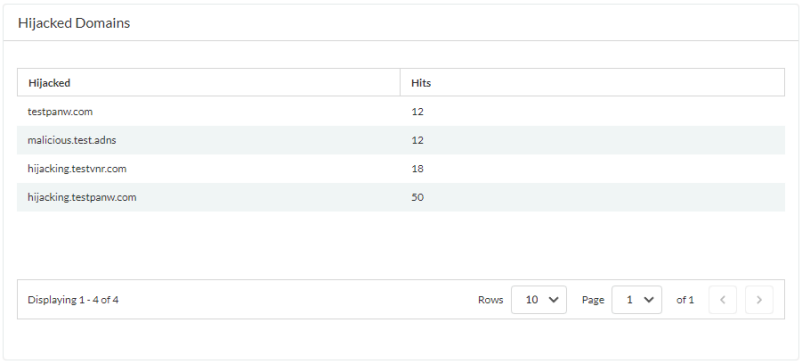
卡片名稱	說明
DNS 要求	顯示 DNS 安全性已處理的 DNS 要求總數。  • 此折線圖會根據使用者定義的時間範圍繪製 DNS 要求數量。指定自訂時間範圍會相應地更新折線圖。 • DNS 類別和動作篩選器不會改變卡片內容。
惡意 DNS 要求	顯示堆疊長條圖，其中顯示已根據目前可用且視為惡意的類型進行分類的 DNS 要求。總數顯示在左上角，而類別變數的細分如下所示。  • 此折線圖會根據使用者定義的時間範圍繪製 DNS 要求數量。指定自訂時間範圍會相應地更新折線圖。 • DNS 類別和動作篩選器不會改變卡片內容。
訂閱	顯示網路中具備作用中 DNS 安全性訂閱的裝置數量。此也顯示未配備 DNS 安全性或訂閱已過期的裝置百分比，以及完整清單的連結。

卡片名稱	說明
	 • 您可以選取 **See a List of Devices**（查看裝置清單）以檢視完整清單。 • 此卡片顯示目前訂閱狀態的快照—篩選器選項沒有任何影響。
高風險 DNS 類別趨勢	顯示趨勢圖，其中會根據在可觀察時間範圍內套用到 DNS 要求的 DNS 類別或動作，顯示 DNS 要求的細分。  • 使用選項按鈕在 DNS 類別或動作趨勢圖之間進行選擇。 • 將游標暫留在代表資料類型的量化波形圖上，可隔離並開啟一個彈出式視窗，其中顯示 DNS 要求數量或所採取動作的類型。 • 指定自訂時間範圍會相應地更新趨勢圖。 • DNS 類別和動作篩選器會反白顯示卡片中所選的變數，但不會將其從圖表中刪除。
跨動作的 DNS 類別分布	顯示流程圖，以視覺化方式顯示針對高風險 DNS 類別所採取動作的分布情況。次要表格顯示對較低優先權 DNS 類別所採取的動作。

卡片名稱	說明
	• 將游標暫留在特定流程上，可開啟一個彈出式視窗，其中顯示針對指定類型所採取動作的數量。 指定自訂時間範圍更新會相應地更新圖表。 • DNS 類別和動作篩選器不會改變卡片內容。  • 系統會根據儀表板頂端套用的篩選器設定，產生首要網域清單。影響整體頁面設定的 Widget 也會決定顯示哪些網域。 • 將游標暫留在列上可檢視使用情況統計資料。 • 按一下網域可檢視 DNS 分析詳細資訊。
網域	根據所選的 DNS 類別，顯示您的網路中、您的產業內和其他產業內可看到的網域數量以及總數。允許您將您組織的 DNS 使用情況與產業內其他組織以及全球收集的資料進行比較，包括僅在您網路中找到的網域要求清單。  • 此卡片中列出的網域包括所有 DNS 類別，無論 DNS 類別和動作篩選器為何。只有時間範圍才會更新卡片的內容。
前 10 個網域	提供您網路中前 10 個最常要求的網域清單，以及 DNS 類別和採取的動作。您可以透過按一下適當的圖示，來檢視網域的更多詳

卡片名稱	說明
	細資訊和相關日誌。選取 **View All DNS Requests**（檢視所有 **DNS** 要求），以取得已存取網域的完整清單。  • 此卡片中列出的網域包括所有 DNS 類別，無論 DNS 類別和動作篩選器為何。只有時間範圍才會更新卡片的內容。 • 按一下網域可檢視 DNS 分析詳細資訊。
DNS 解析程式	提供兩個清單，其中顯示網路中解析最多為和最少為惡意的網域。

卡片名稱	說明
	 • 按一下 DNS 解析程式可檢視 DNS 分析詳細資訊。
設定錯誤的網域（進階 DNS 安全性）	提供與使用者所指定面向公眾的父系網域相關聯的不可解析網域清單。對於每個項目，都有一個設定錯誤原因和基於來源 IP 的流量命中計數。 
被劫持的網域名稱（進階 DNS 安全性）	提供由進階 DNS 安全性判定的被劫持網域清單。對於每個項目，都有一個分類原因和基於來源 IP 的流量命中計數。

卡片名稱	說明
	

檢視 DNS 安全性儀表板 (Strata Cloud Manager)

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。

STEP 2 | 選取 **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **DNS Security**（**DNS** 安全性），以開啟 DNS 安全性儀表板。

STEP 3 | 在儀表板上，使用可用的下拉式選單設定篩選器選項。

1. 依時間範圍篩選—從 **Last hour**（過去 **1** 小時）、**Last 24 hours**（過去 **24** 小時）、**Last 7 days**（過去 **7** 天）或 **Last 30 days**（過去 **30** 天）中選擇，以顯示特定時間範圍內的資料。
2. 依 DNS 類別篩選—從 **Select All**（全選）、**Malware**（惡意軟體）、**Command and Control**（命令與控制）、**Phishing**（網路釣魚）、**Grayware**（灰色軟體）、**Exceptions List**（例外清單）、**Newly Registered**（新註冊的）、**Dynamic DNS**（動態 **DNS**）、**Proxy**、**Parked**（寄放）、**Benign**（良性）、**Ad Track**（廣告追蹤）之中選擇，以根據 DNS 資料篩選資料集。

   例外清單類別是由 *Palo Alto Networks* 根據 *PAN-DB* 和 *Alexa* 的度量維護的可明確允許的網域清單。這些允許清單經常遭存取，且已知沒有惡意內容。
3. 依 DNS 動作篩選—從 **Allow**（允許）、**Block**（封鎖）和 **Sinkhole** 中進行選擇，以根據依據 DNS 安全性設定檔動作設定對 DNS 查詢採取的動作進行篩選。

STEP 4 | 您也可以選擇性地下載、分享和排程活動報告。

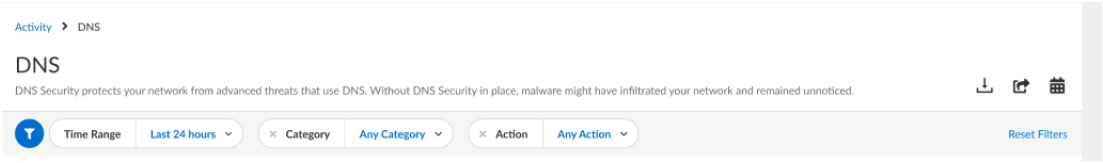
STEP 5 | 您可以將儀表板卡片提供的資料進行再脈絡化、互動與轉換。如需每個 DNS 安全儀表板卡片的概述，請參閱 DNS 安全性儀表板卡片。

檢視 DNS 安全性儀表板 (AIOps for NGFW Free)

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 AIOps for NGFW Free 應用程式。

STEP 2 | 選取 **Dashboards**（儀表板） > **More Dashboards**（更多儀表板） > **DNS Security**（**DNS** 安全性），以開啟 DNS 安全性儀表板。

STEP 3 | 在儀表板上，使用可用的下拉式選單設定篩選器選項。



1. 依時間範圍篩選—從 **Last hour**（過去 **1** 小時）、**Last 24 hours**（過去 **24** 小時）、**Last 7 days**（過去 **7** 天）或 **Last 30 days**（過去 **30** 天）中選擇，以顯示特定時間範圍內的資料。
2. 依 DNS 類別篩選—從 **C2 (DGA, Tunneling, other C2)**（**DGA**、通道、其他 **C2**）、**Malware**（惡意軟體）、**Newly Registered Domain**（新註冊的網域）、**Phishing**（網路釣魚）、**Dynamic DNS**（動態 **DNS**）、**Allow List**（允許清單）、**Benign**（良性）、**Grayware**（灰色軟體）、**Parked**（寄放）、**Proxy** 和 **Any Category**（任何類別）之中選擇，以根據 DNS 類型篩選資料集。

   允許清單類別是由 *Palo Alto Networks* 根據 *PAN-DB* 和 *Alexa* 的度量維護的可明確允許的網域清單。這些允許清單經常遭存取，且已知沒有惡意內容。
3. 依 DNS 動作篩選—從 **Allow**（允許）、**Block**（封鎖）和 **Sinkhole** 中進行選擇，以根據依據 DNS 安全性設定檔動作設定對 DNS 查詢採取的動作進行篩選。

STEP 4 | 您也可以選擇性地下載、分享和排程活動報告。

STEP 5 | 您可以將儀表板卡片提供的資料進行再脈絡化、互動與轉換。如需每個 DNS 安全儀表板卡片的概述，請參閱 DNS 安全性儀表板卡片。

檢視 DNS 安全性日誌

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 DNS 安全性授權（用於增強型功能支援）或 DNS 安全性授權 ❑ 進階威脅防護或威脅防護授權

您可以瀏覽、搜尋和檢視當 DNS 安全性遇到合格事件時自動產生的 DNS 安全性日誌。通常，這包括 DNS 安全性分析的任何網域類別，除非特別將其日誌嚴重性層級設定為無。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）。

DNS 安全性日誌可直接在防火牆上或透過基於 Strata Logging Service 的日誌檢視器（AIOps for NGFW Free、Cloud Management、Strata Logging Service 等）存取。雖然防火牆允許您存取當使用者進行 DNS 查詢時產生的惡意威脅日誌項目，但不會記錄良性 DNS 要求。此外 DNS 安全性資料也透過日誌轉送（以威脅日誌形式）和 DNS 安全性遙測（以 DNS 安全性日誌形式）轉送至 Strata Logging Service，之後再由各種活動日誌檢視器應用程式參照這些資料。DNS 安全性遙測功能會以最小的開銷運作，這可限制傳送到 Strata Logging Service 的資料量；因此無論嚴重性層級、威脅類型或類別為何，皆只會將 DNS 查詢的子集轉送至 Strata Logging Service 作為 DNS 安全性記錄項目。使用日誌轉送所轉送至 Strata Logging Service 的惡意 DNS 要求威脅日誌完整可用。因此，Palo Alto Networks 建議將惡意 DNS 要求日誌視為威脅日誌，而不是 DNS 安全性日誌。

- Strata Cloud Manager
- PAN-OS 和 Panorama
- AIOps for NGFW 免費版
- Strata 記錄服務

檢視 DNS 安全性日誌 (Strata Cloud Manager)

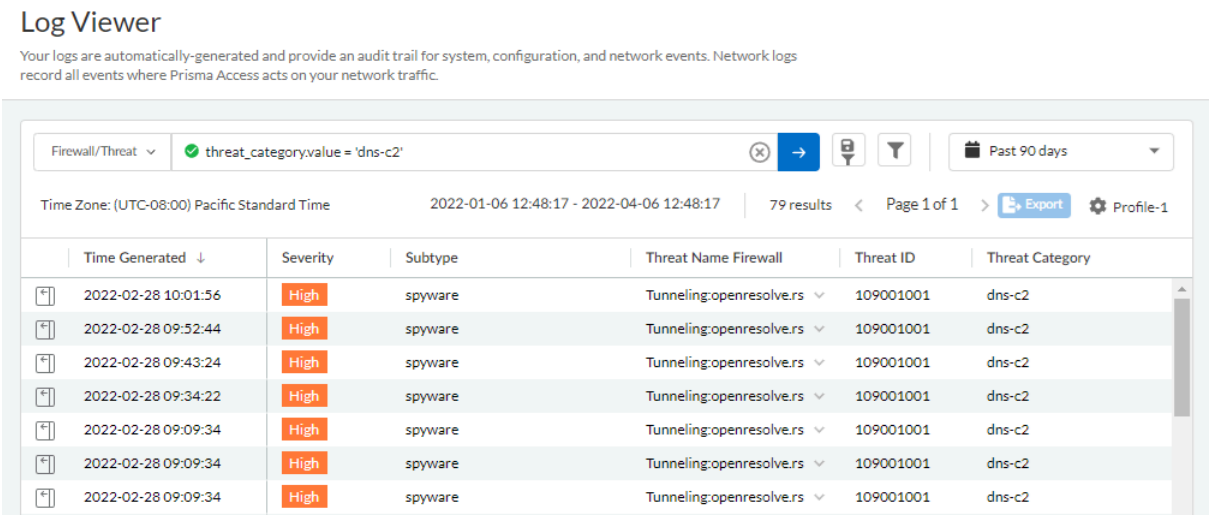
經 *DNS* 安全性分析的良性 *DNS* 查詢不會顯示在日誌檢視器中。登入您的 *Strata Logging Service* 應用程式以存取良性 *DNS* 日誌項目。

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。

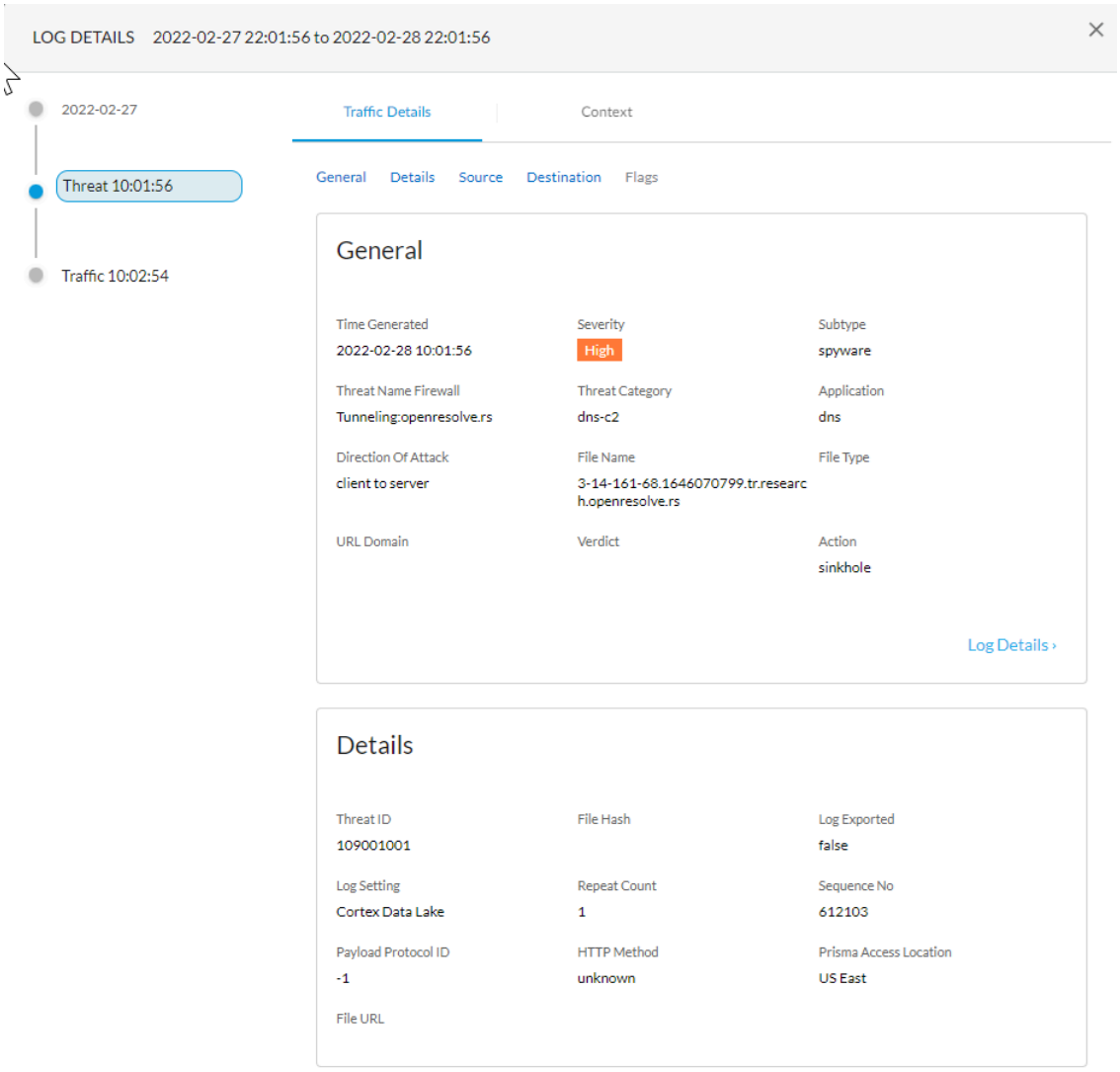
STEP 2 | 搜尋已使用 DNS 安全性處理的 DNS 查詢。

1. 選取 **Incidents and Alerts**（事件和警示）> **Log Viewer**（日誌檢視器）。
2. 使用威脅篩選器限制搜尋，並根據 DNS 類別提交日誌查詢，例如，`threat_category.value = 'dns-c2'` 以檢視已判定為 C2 網域的日誌。若要搜尋其他 DNS 類型，請將 c2 取代成其他支援的 DNS 類別（ddns、寄放、惡意軟體

等）。視需要調整搜尋準則，包括其他查詢參數（例如嚴重性層級和子類型）以及日期範圍。



3. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
4. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **General**（一般）窗格中。威脅的其他相關詳細資訊會顯示在相應視窗。



5. 對於庫存網域和 DNS 通道網域，包括基於通道的 APT（進階持續性威脅），您可以檢視攻擊中使用的各種工具，以及與網域相關聯的攻擊活動。這會反映在所指定網域的日誌項目其 [Threat ID/Name（威脅 ID/名稱）] 欄位中。具有屬性的 DNS 網域其威脅 ID/名稱使用以下格式；在此範例中，對於 DNS 通道網域：`Tunneling:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`，其中 `tool_name` 是指用於將資料內嵌到 DNS 查詢和回應中的 DNS 通道工具，同時也是網路威脅活動名稱（以逗號分隔的清單）。這些活動可以是業界接受的事件，並使用相同的命名慣例，或者可以是由 Palo Alto Networks 識別和命名並在Unit 42 威脅研究部落格中描述的事件。此類活動的部落格（在本例為「利用 DNS 通道技術」）可在此處找到：利用 DNS 通道追蹤與掃描。

   初步偵測完成後，相關聯工具和活動屬性可能需要一段時間，才能在日誌以及 *Palo Alto Networks ThreatVault* 和 *Test-A-Site* 中檢視當屬性元件完成並已經過驗證後，完整的 *DNS* 通道工具和活動詳細資訊將如預期顯示在 *[Threat ID/Name（威脅 ID/名稱）]* 與活動欄位中。

檢視 DNS 安全性日誌 (NGFW (Managed by PAN-OS or Panorama)）

STEP 1 | 登入 PAN-OS 網頁介面。

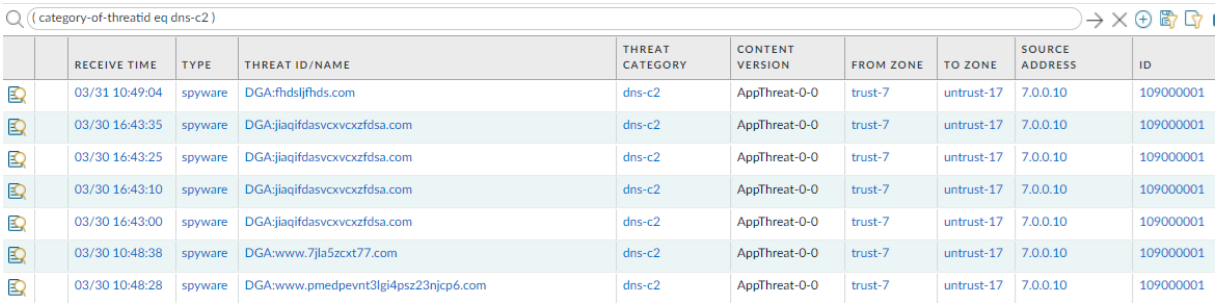
STEP 2 | 在防火牆上搜尋已使用 DNS 安全性處理的查詢活動。

1. 選取 **Monitor**（監控） > **Logs**（日誌） > **Threat**（威脅），然後根據 DNS 類別篩選。

   考量以下範例：

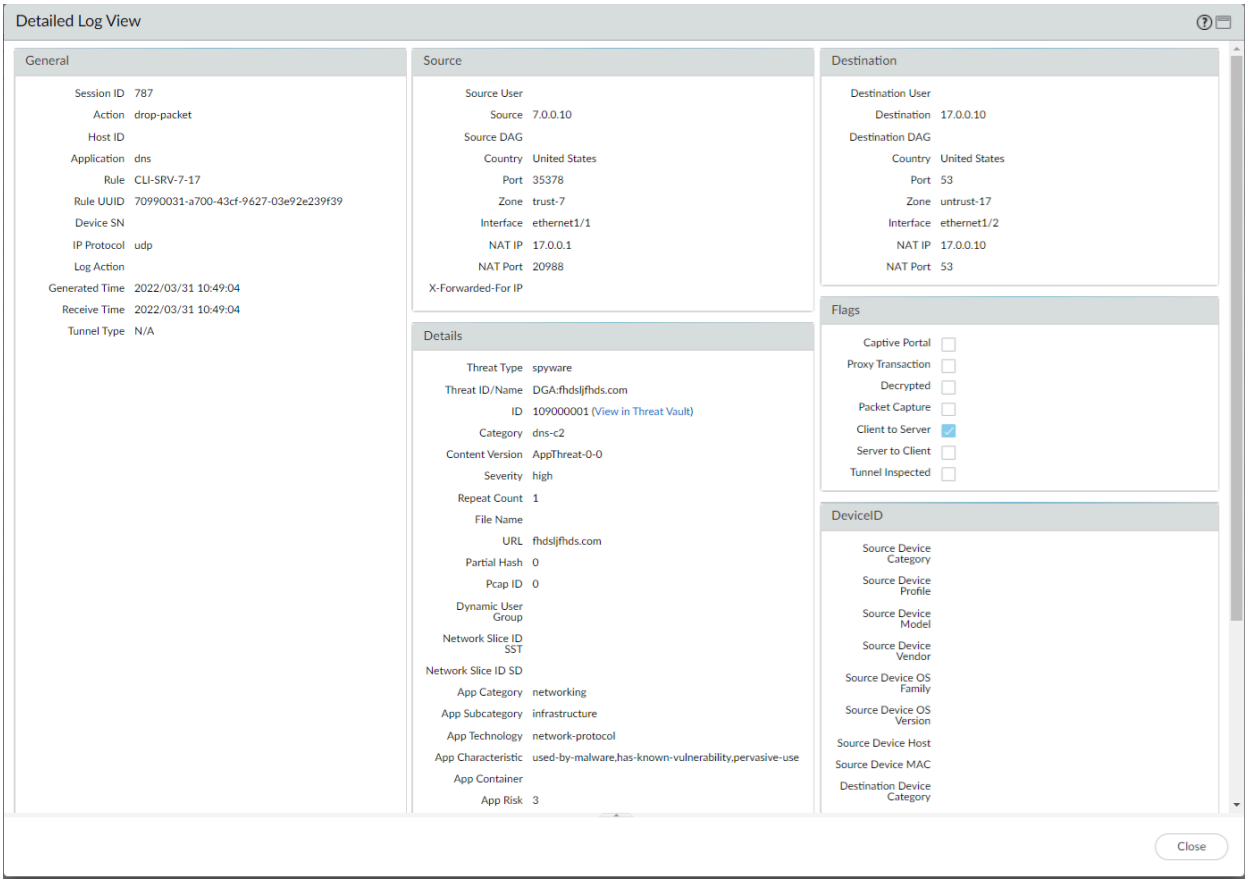
   - `(category-of-threatid eq dns-c2)` 可檢視已由 DNS 安全性判定為 C2 網域的日誌。
   - `(category-of-threatid eq adns-hijacking)`，其中變數 `adns-hijacking` 表示已由進階 DNS 安全性歸類為惡意 DNS 劫持嘗試的 DNS 查詢。

   若要搜尋其他 DNS 類型，請將 c2 取代成其他支援的 DNS 類別（ddns、寄放、惡意軟體等）。



	RECEIVE TIME	TYPE	THREAT ID/NAME	THREAT CATEGORY	CONTENT VERSION	FROM ZONE	TO ZONE	SOURCE ADDRESS	ID
	03/31 10:49:04	spyware	DGA:fhdsljfhds.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:35	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:25	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:10	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 16:43:00	spyware	DGA:jiaqifdasvcxvcxzfdsa.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:38	spyware	DGA:www.7jla5zcxt77.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001
	03/30 10:48:28	spyware	DGA:www.pmedpevnt3lgi4psz23njcp6.com	dns-c2	AppThreat-0-0	trust-7	untrust-17	7.0.0.10	109000001

2. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
3. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資訊）窗格中。威脅的其他相關詳細資訊會顯示在相應視窗。



4. 對於庫存網域和 DNS 通道網域，包括基於通道的 APT（進階持續性威脅），您可以檢視攻擊中使用的各種工具，以及與網域相關聯的攻擊活動。這會反映在所指定網域的日誌項目其 [Threat ID/Name（威脅 ID/名稱）] 欄位中。具有屬性的 DNS 網域其威脅 ID/名稱使用以下格式；在此範例中，對於 DNS 通道網域：`Tunneling:<tool_name>,<tool_name>,<tool_name>,...:<domain_name>`，其中 `tool_name` 是指用於將資料內嵌到 DNS 查詢和回應中的 DNS 通道工具，同時也是網路威脅活動名稱（以逗號分隔的清單）。這些活動可以是業界接受的事件，並使用相同的命名慣例，或者可以是由 Palo Alto Networks 識別和命名並在Unit 42 威脅研究部落格中描述的事件。此類活動的部落格（在本例為「利用 DNS 通道技術」）可在此處找到：利

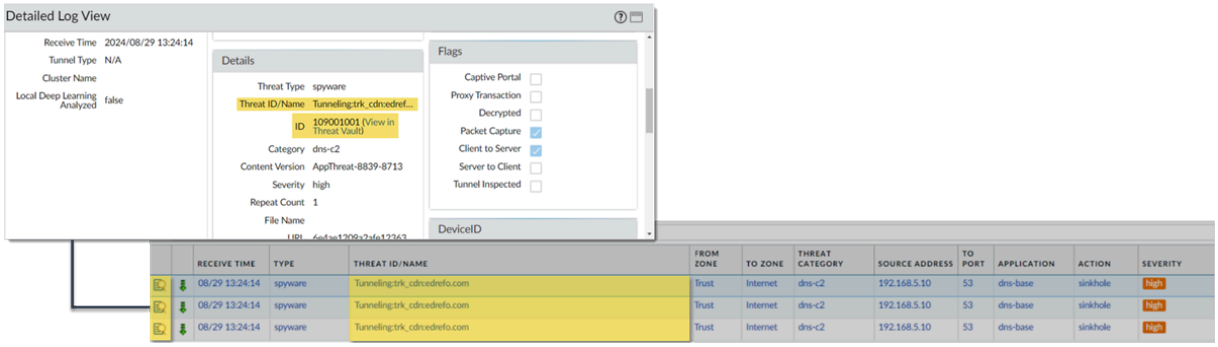
用 DNS 通道追蹤與掃描。或者，您也可以從 Palo Alto Networks ThreatVault 和 URL 篩選測試 A 網站檢視屬性資訊。

初步偵測完成後，相關聯工具和活動屬性可能需要一段時間，才能在日誌以及 *Palo Alto Networks ThreatVault* 和 *Test-A-Site* 中檢視當屬性元件完成並已經過驗證後，完整的 *DNS* 通道工具和活動詳細資訊將如預期顯示在 *[Threat ID/Name*（威脅 *ID/*名稱）*]* 與活動欄位中。

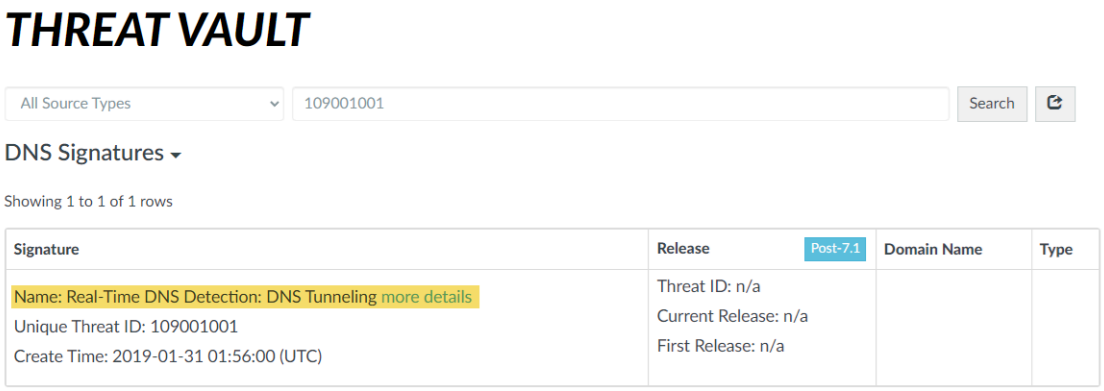
考量以下範例：

- **DNS** 通道網域 **APT** 屬性

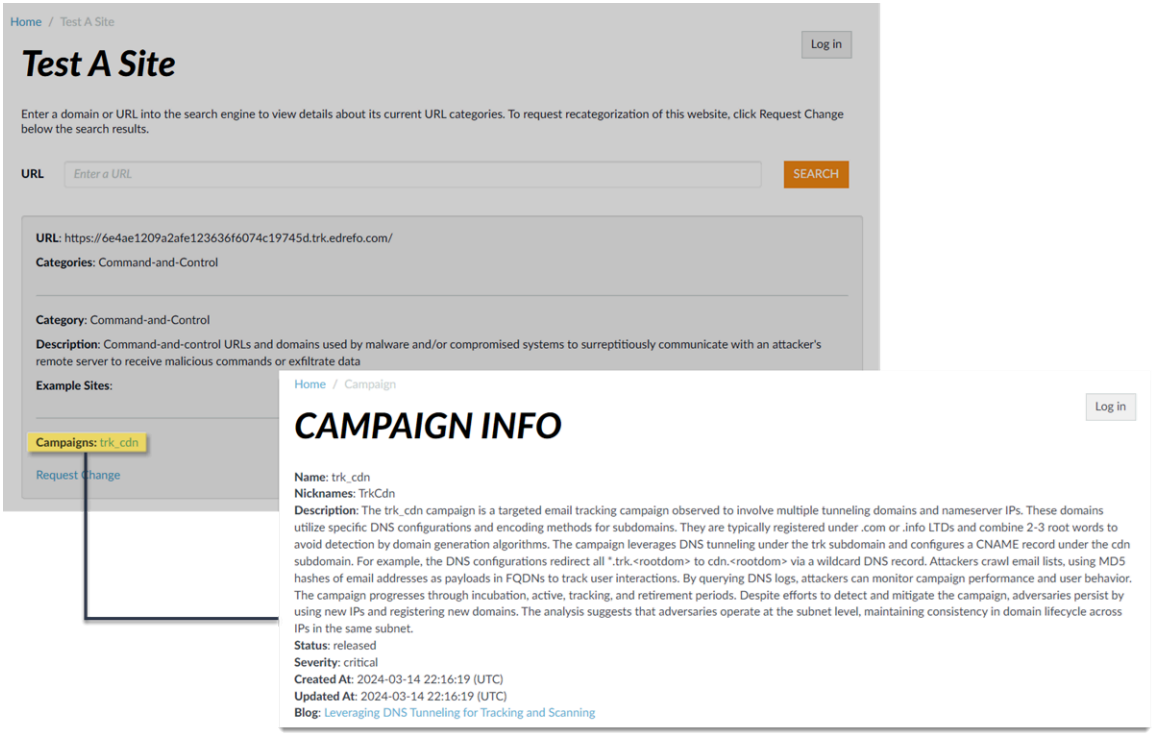
  1. PAN-OS



  2. ThreatVault

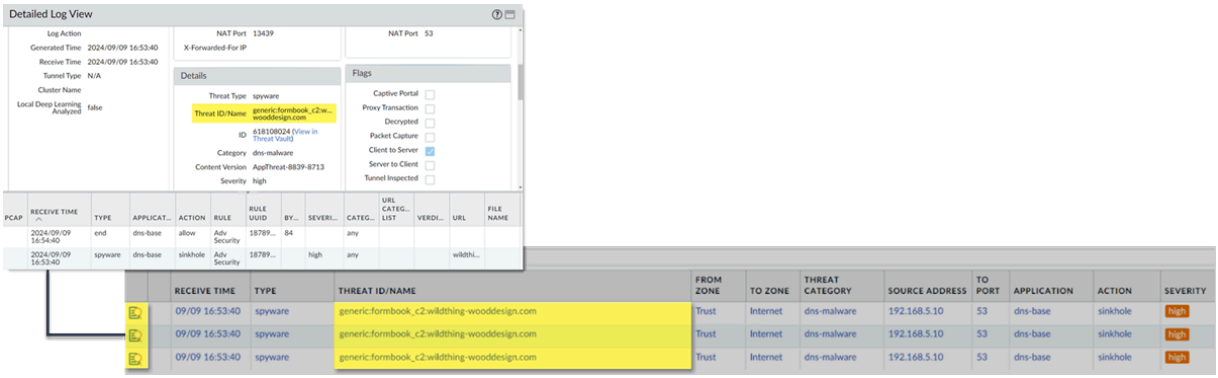


  3. URL 篩選 Test-A-Site

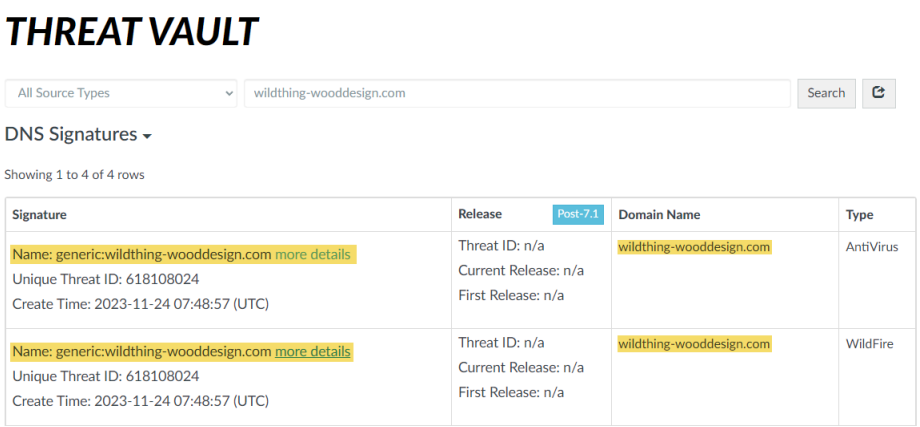


- 庫存網域 **APT** 屬性

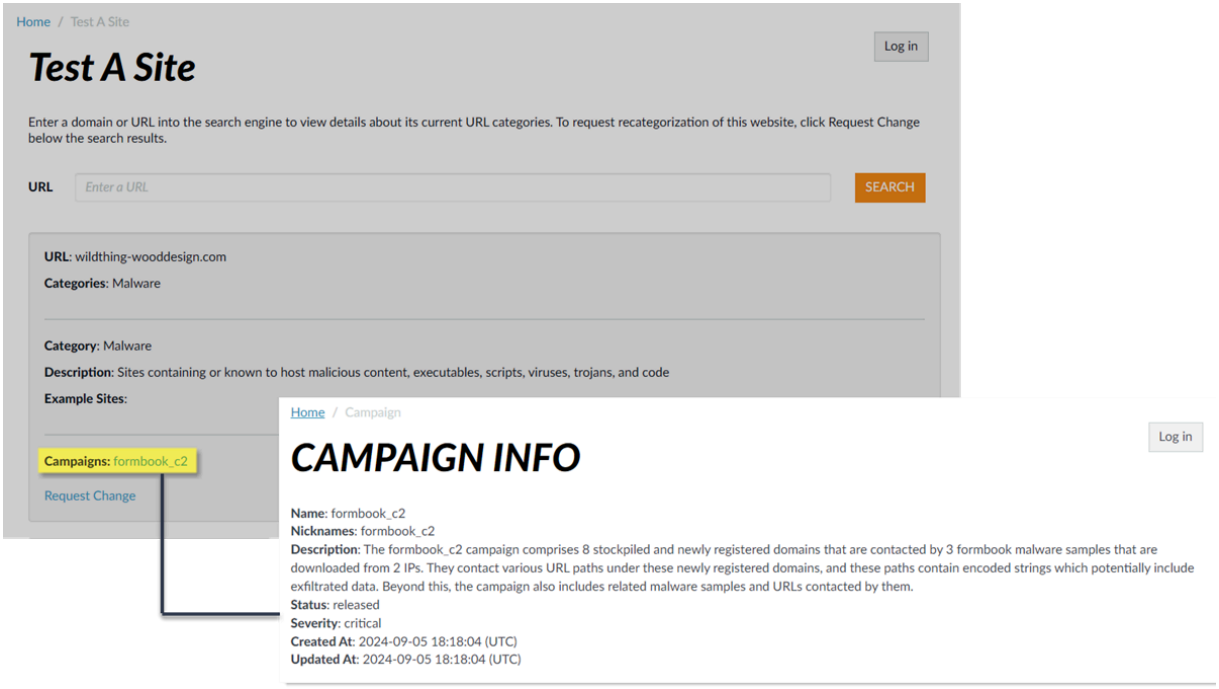
1. PAN-OS



2. ThreatVault



3. URL 篩選 Test-A-Site



檢視 DNS 安全性日誌 (AIOps for NGFW Free）

經 *DNS* 安全性分析的良性 *DNS* 查詢不會顯示在 *AIOps for NGFW Free* 日誌檢視器中。登入您的 *Strata Logging Service* 應用程式以存取良性 *DNS* 日誌項目。

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 AIOps for NGFW Free 應用程式。

STEP 2 | 在 AIOps for NGFW Free 中搜尋已使用 DNS 安全性處理的 DNS 查詢。

1. 選取 **Incidents and Alerts**（事件和警示）> **Log Viewer**（日誌檢視器）。
2. 使用威脅篩選器限制搜尋，並根據 DNS 類別提交日誌查詢，例如，`threat_category.value = 'dns-c2'` 以檢視已判定為 C2 網域的日誌。若要搜尋其他 DNS 類型，請將 c2 取代成其他支援的 DNS 類別（ddns、寄放、惡意軟體等）。視需要調整搜尋準則，包括其他查詢參數（例如嚴重性層級和子類型）以及日期範圍。
3. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
4. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資訊）窗格中。威脅的其他相關詳細資訊會顯示在相應視窗。

檢視 DNS 安全性日誌 (Strata Logging Service）

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 Logging Service 應用程式。

STEP 2 | 根據日誌類型分配儲存區。如果尚未在 Strata Logging Service 上為 DNS 安全性日誌分配儲存區空間，則將無法透過 Strata Logging Service 檢視日誌項目。

STEP 3 | 在 Strata Logging Service 中搜尋已使用 DNS 安全性處理的 DNS 查詢。

1. 選取 **Explore**（探索）以開啟 Strata Logging Service 日誌檢視器。
2. 使用威脅篩選器限制搜尋，並根據 DNS 類別提交日誌查詢，例如，`threat_category.value = 'dns-c2'` 以檢視已判定為 C2 網域的日誌。若要搜尋其他 DNS 類型，請將 c2 取代成其他支援的 DNS 類別（ddns、寄放、惡意軟體等）。視需要調整搜尋準則，包括其他查詢參數（例如嚴重性層級和子類型）以及日期範圍。
3. 選取日誌項目以檢視所偵測到 DNS 威脅的詳細資訊。
4. 威脅 **Category**（類別）顯示在詳細日誌檢視的 **Details**（詳細資訊）窗格中。威脅的其他相關詳細資訊會顯示在相應視窗。