paloalto TECHDOCS

BPA 入門

10.2

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 13, 2022

Table of Contents

評估安全性政策功能採用

最佳做法評估 (BPA) 工具可協助您了解目前的安全性政策功能採用層級，並協助您評估安全性狀態的成熟度和有效性。採用 WildFire、弱點保護、SSL 解密等這類功能，可以偵測和防止攻擊。明確了解在不同環境中使用每個功能的方式和位置，對於了解如何最佳保護網路和其重要資產十分重要。

最佳做法入門會顯示如何存取和執行 BPA。BPA 報告的 Capability Adoption Heatmaps（功能採用熱圖）區段可讓您檢閱這些功能跨安全性政策規則庫的採用。觀看熱圖簡介視訊來了解熱圖，並利用 BPA 視訊庫和 BPA+ 視訊庫更深入了解該工具。

在全景管理的環境中，*Panorama* 可能會管理大量的新世代防火牆。您應該在全景或是在每個個別防火牆上執行 *BPA?*權衡是速度和便利性與完整性。

在 *Panorama* 上執行 *BPA* 既快速又方便，可評估受管理防火牆的大部分功能，但不會檢查本機防火牆取代。

在每個受管理防火牆上執行 *BPA* 會評估完整的設定（包括本機取代），但需要更多時間。

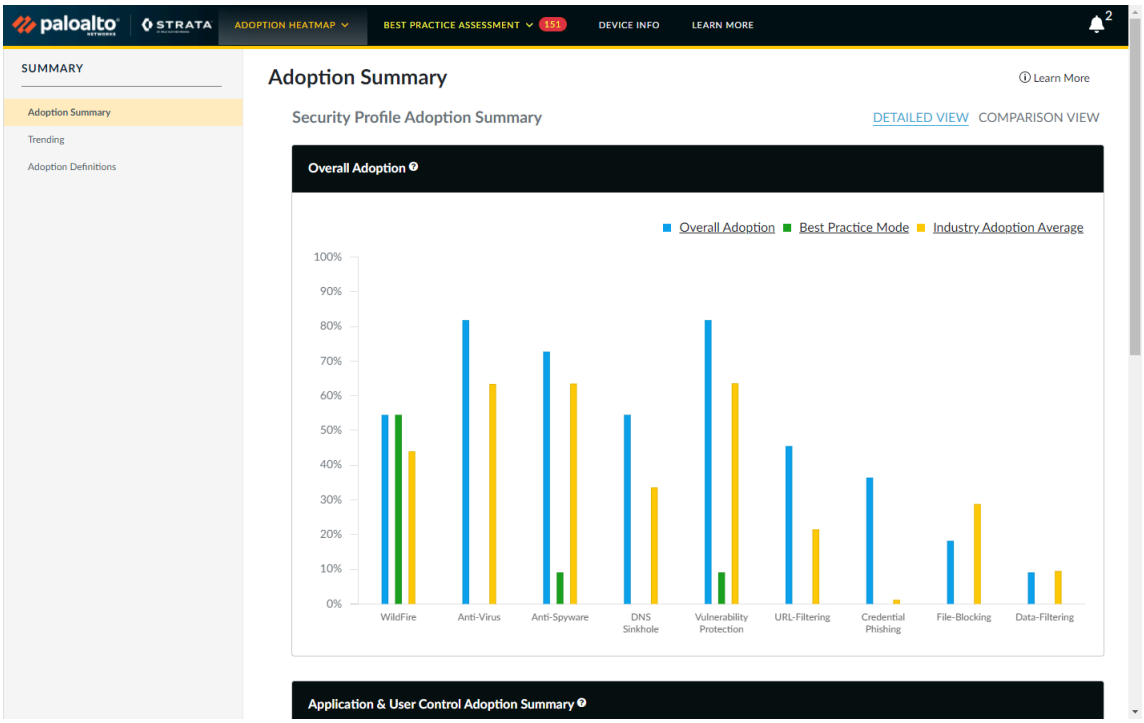
最實用的方法是首先在 *Panorama* 上執行 *BPA*。檢查結果，決定是否需要專注於任何特定的受管理裝置，然後在這些裝置上執行 *BPA*。此方法可節省時間，同時仍然專注於可讓您改善安全性狀態的相關資訊。

檢閱並分析 Heatmap（熱圖）頁籤上的資訊，以識別安全性功能採用漏洞，並判斷您想要改善的項目：

- 檢閱採用摘要
- 識別採用漏洞
- 識別要改善的規則

檢閱採用摘要

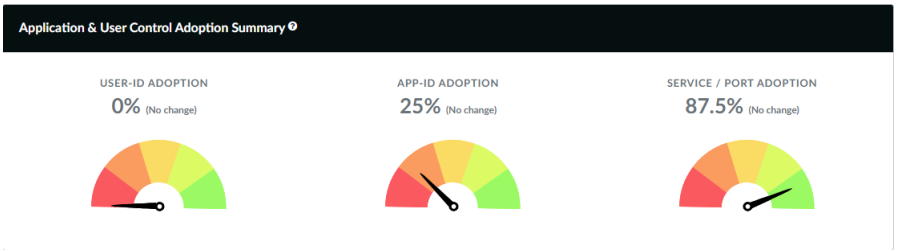
在您或 Palo Alto Networks 業務代表執行 BPA 之後，會在 [Adoption Heatmap（採用熱圖）] 頁面的 [Adoption Summary（採用摘要）] 上開啟產生的 HTML 報告。採用摘要檢視會概述裝置的整體安全性功能採用。此報告會顯示每個度量的目前採用百分比（[Industry Average（企業平均值）] 除外，其提供您企業中的採用平均值），以及自最後一次對裝置設定檔案執行 BPA 之後的採用百分比變更（以括號括住）（或者，如果值與最後一次執行 BPA 相同，則為 **No change**（無變更））。



整體採用—安全性政策允許規則中的安全性設定檔採用。百分比的基礎是已啟用一個或多個設定檔作為規則一部分的允許規則數目。BPA 不會計入已停用的規則或封鎖規則。

企業平均值—您公司產業的允許規則中的平均安全性設定檔採用。

最佳做法模式—允許規則中以建議的最佳做法方式設定的安全性設定檔採用。BPA 只會計入設定檔通過所有最佳做法檢查的規則。

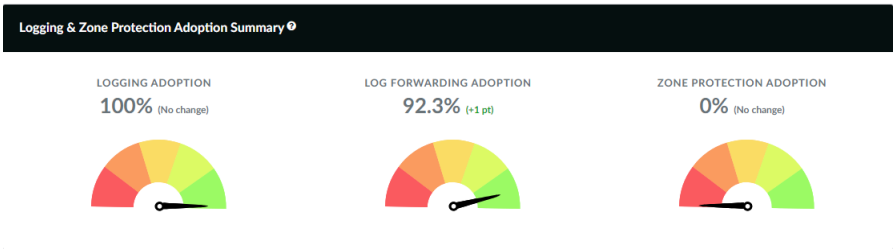


App-ID 採用—跨安全性政策規則的 App-ID 採用。百分比值的基礎是具有一個或多個已定義應用程式的允許規則總數（應用程式不是 **any**（任何））。BPA 不會計入已停用的規則。

User-ID 採用—跨安全性政策規則的 User-ID 採用。百分比值的基礎是具有使用者（包含值 **known-user**（已知使用者）和 **unknown**（未知））或使用者群組的允許規則總數。BPA 不會計入已停用的規則。

服務/連接埠採用—跨安全性政策規則的服務/連接埠採用。百分比值的基礎是具有已定義服務或連接埠的允許規則總數（服務不是 **any**（任何））。BPA 不會計入已停用的規則。

BPA 不會計入封鎖規則的 *App-ID*、*User-ID* 或服務/連接埠採用，因為不同業務的封鎖原理會不同，因此 *BPA* 無法根據封鎖規則進行建議。

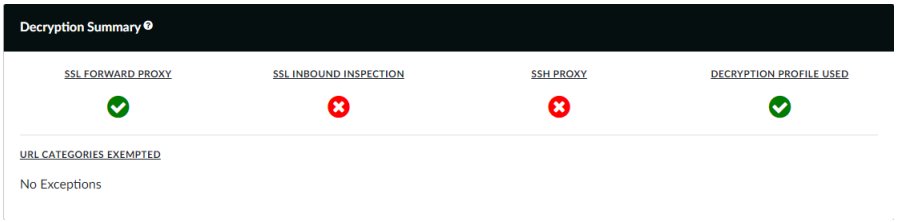


記錄採用—跨安全性政策規則的 **Log at Session End**（工作階段結束時記錄）採用。百分比值的基礎是已啟用 **Log at Session End**（工作階段結束時記錄）的規則總數。BPA 不會計入已停用的規則。

日誌轉送採用—跨安全性政策規則的日誌轉送設定檔採用。百分比值的基礎是已設定日誌轉送設定檔的規則總數。BPA 不會計入已停用的規則。

區域保護採用—跨安全性政策允許規則的區域保護採用。百分比值的基礎是來源區域已設定區域保護設定檔的允許規則總數。BPA 不會計入已停用的規則。

針對所有這些度量，每個百分比旁邊以括號括住的值都是自最後一次對裝置設定檔案執行 BPA 之後的採用百分比變更（或者，如果值與最後一次執行 BPA 相同，則為 **No change**（無變更））。



解密摘要—顯示設定是否包含 SSL 轉送 Proxy、SSL 輸入檢查和 SSH Proxy 的解密政策規則。此摘要也會顯示設定是否包含解密設定檔，並識別可排除裝置不進行解密的 URL 類別。

如果您未解密 *URL* 類別（或個別應用程式），則無法檢查其流量，因為防火牆看不到已加密流量的內容。防火牆只能檢查您所解密的流量。

接下來：識別採用漏洞 了解您可以改善安全性之處。

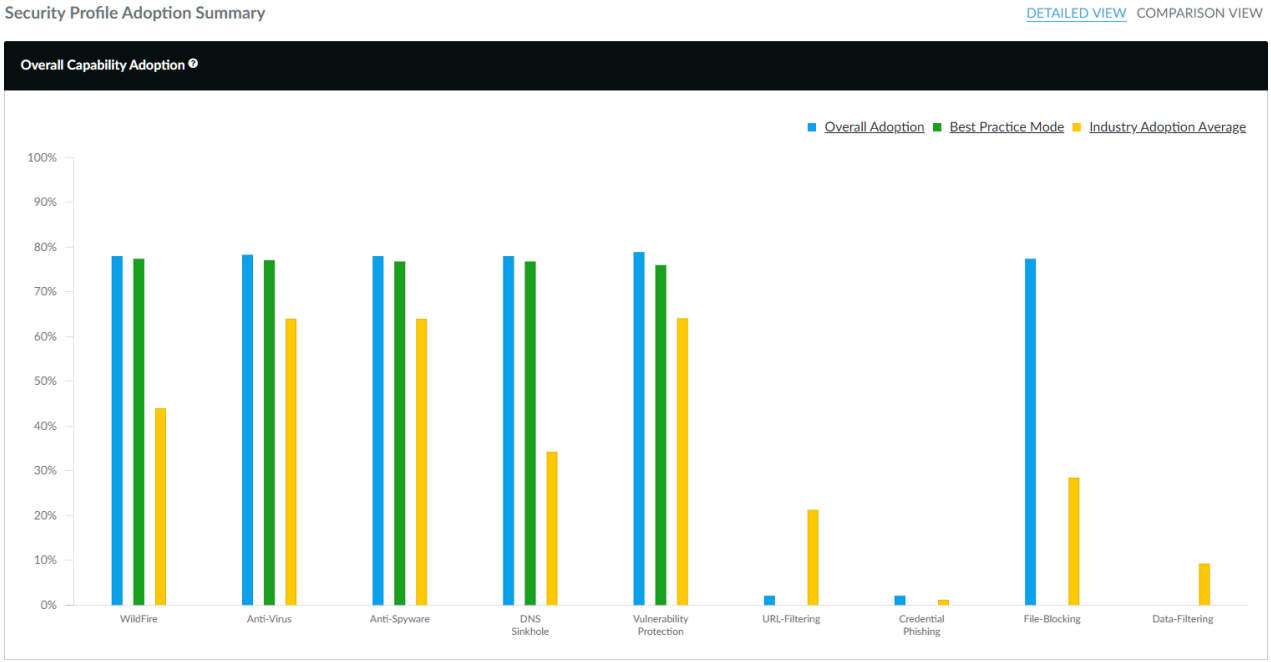
識別採用漏洞

[Adoption Heatmap（採用熱圖）] 選項顯示安全性政策嚴格的位置以及可聚焦改善的安全性政策功能採用漏洞的位置。若要看到最多流量以及獲得最大程度的攻擊保護，請設定安全性功能採用的目標，並使用下列建議作為最佳做法基準線。根據基準線來評估目前狀態，以識別安全性政策功能採用漏洞。

[Adoption Heatmap（採用熱圖）] 有助於識別可改善安全性政策功能採用的裝置、區域 (Zone) 和區域 (Area)。您可以依裝置群組、序號和 Vsys、區域、架構區域、標籤、規則詳細資料和區域對應來檢閱採用資訊。**Local Filters**（本機篩選）會根據裝置群組、來源架構區域、目的地架構區域、目標、來源區域、目的地區域和標籤進行篩選，來縮小範圍並識別漏洞。下列顯示「依架構區域的採用熱圖」（**Adoption Heatmap**（採用熱圖） > **Areas of Architecure**（架構區域））：

Dest Area of Architectu...	Source Area of Architecture	Total Enabled Rule Count	Allow Rule Count	Deny Rule Count	WildFire Adoption %	Anti-Spyware Adoption %	DNS Sinkhole Adoption %	Anti-Virus Adoption %	Vulnerability Protection Adoption %	URL-Filtering Adoption %	Credential Theft Adoption %	File-Blocking Adoption %	Data-Filtering Adoption %	User ID Adoption %	App ID Adoption %	Service / Port Adoption %	Logging Adoption %	Log Forwarding Adoption %	Zo... Pro... Pro... Ad... %
DMZ	Internet	3	3	0	66.7	0.0	0.0	66.7	100.0	0.0	0.0	33.3	0.0	0.0	100.0	100.0	100.0	66.7	
Internet	DMZ	2	2	0	50.0	50.0	50.0	100.0	50.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	100.0	
Datacenter	DMZ	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	100.0	0.0	
PCI	Remote Office/MPLS	1	1	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	0.0	
any	any	9	3	6	0.0	33.3	33.3	0.0	33.3	0.0	0.0	0.0	0.0	0.0	33.3	66.7	100.0	77.8	
Datacenter	Datacenter	2	2	0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	50.0	100.0	100.0	100.0	0.0	
Internet	Remote Users/VPN, Internal Core	8	6	2	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	
DMZ	Remote Users/VPN, Internal Core	1	1	0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0	100.0	100.0	100.0	
Internet	Internal Core	1	0	1	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	100.0	100.0	
App-tier	Web-tier	1	1	0	100.0	100.0	100.0	100.0	100.0	0.0	0.0	100.0	0.0	0.0	100.0	100.0	100.0	0.0	
	Grand Total	350	341	9	78.0	78.0	78.0	78.3	78.9	2.1	2.1	77.4	0.0	30.5	15.2	94.1	100.0	6.6	

在 **Adoption Heatmap**（採用熱圖） > **Summary**（摘要）中，按一下採用摘要，檢查下列功能的採用率。使用建議作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：



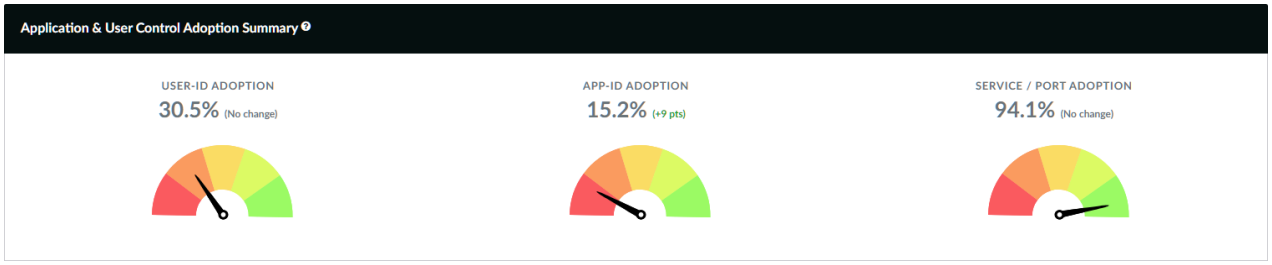
- 將 WildFire、防毒、反間諜軟體、弱點保護和檔案封鎖安全性設定檔套用至所有允許流量的規則，且目標為 100% 或幾乎 100% 採用。如果您未將設定檔套用至允許規則，則請確定有不套用設定檔的良好業務原因。

  在所有允許規則上設定安全性設定檔，可讓防火牆檢查解密流量中是否有威脅，不論為應用程式或服務/連接埠。更新設定之後，請執行 BPA 以測量進度以及捕捉未附加安全性設定檔的新規則。

  您可以在沒有 ***WildFire*** 授權的情況下將 ***WildFire*** 設定檔套用至規則。覆蓋範圍限制為 ***PE*** 檔案，但這仍為未知的惡意檔案提供有用的可見度。

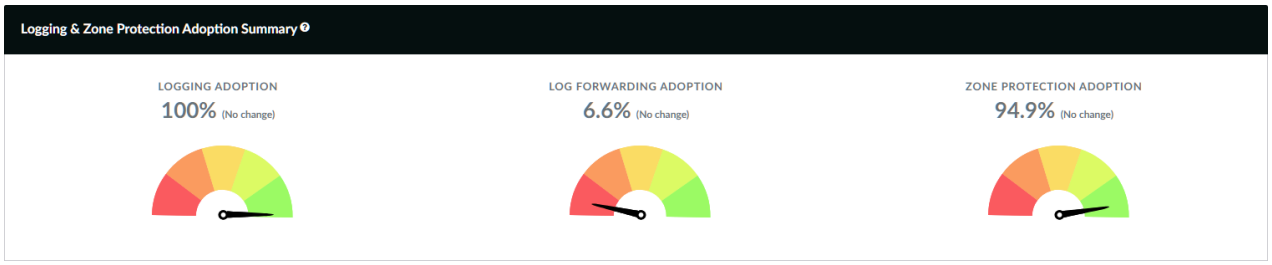
- 在反間諜軟體設定檔中，將 DNS Sinkhole 套用至所有規則，防止受危害的內部主機傳送惡意和自訂網域的 DNS 查詢、識別和追蹤可能受危害的主機，以及避免 DNS 檢查漏洞。啟用 DNS Sinkhole 可保護網路而不影響可用性，因此您可以且應該立即啟用它。
- 將 URL 篩選和認證竊取（網路釣魚）保護套用至所有輸出網際網路流量。

在 [Adoption Summary（採用摘要）] 的 [Application & User Control Adoption Summary（應用程式和使用者控制採用摘要）] 中，檢查下列功能的採用率。使用建議作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：



- 將 App-ID 套用至盡可能接近 100% 的規則。將 User-ID 套用至來源區域或位址範圍內存在使用者的所有規則（部分區域可能沒有使用者來源；例如，資源中心區域中的來源應該是伺服器，而非使用者）。利用 App-ID 和 User-ID 來建立政策，以允許適當的使用者認可（和容忍）應用程式。明確封鎖惡意和不需要的應用程式。
- 目標設為 100% 或接近 100% 服務/連接埠採用，不允許非標準連接埠上的應用程式，除非它有適當的業務原因。

在 [Adoption Summary（採用摘要）] 的 [Logging & Zone Protection Adoption Summary（記錄和區域保護採用摘要）] 中，檢查下列功能的採用率。使用建議作為漏洞識別準則；如果實際採用率與建議不符，則請計劃縮小漏洞：



- 目標是等於或接近記錄和日誌轉送的 100% 採用。
- 設定所有區域上的區域保護設定檔。

總結：

功能	採用目標
WildFire	盡可能接近 100% 的安全性政策規則
防毒軟體	盡可能接近 100% 的安全性政策規則
反間諜軟體	盡可能接近 100% 的安全性政策規則
漏洞	盡可能接近 100% 的安全性政策規則
檔案封鎖	盡可能接近 100% 的安全性政策規則
URL 篩選和認證竊取	所有輸出網際網路流量
App-ID	盡可能接近 100% 的安全性政策規則
使用者-ID	來源區域或位址範圍內存在使用者的所有規則
服務/連接埠	盡可能接近 100% 的安全性政策規則
記錄	盡可能接近 100% 的安全性政策規則
日誌轉送	盡可能接近 100% 的安全性政策規則
區域保護	所有區域

檢視採用熱圖時，請使用 **Local Filters**（本機篩選）以縮小範圍。使用產生的資訊來識別安全性政策功能漏洞、根據漏洞識別準則進行測量，以及調整或建立新的漏洞識別準則來進一步調查。例如，建立篩選以顯示可控制到網際網路架構區域之流量的規則採用：

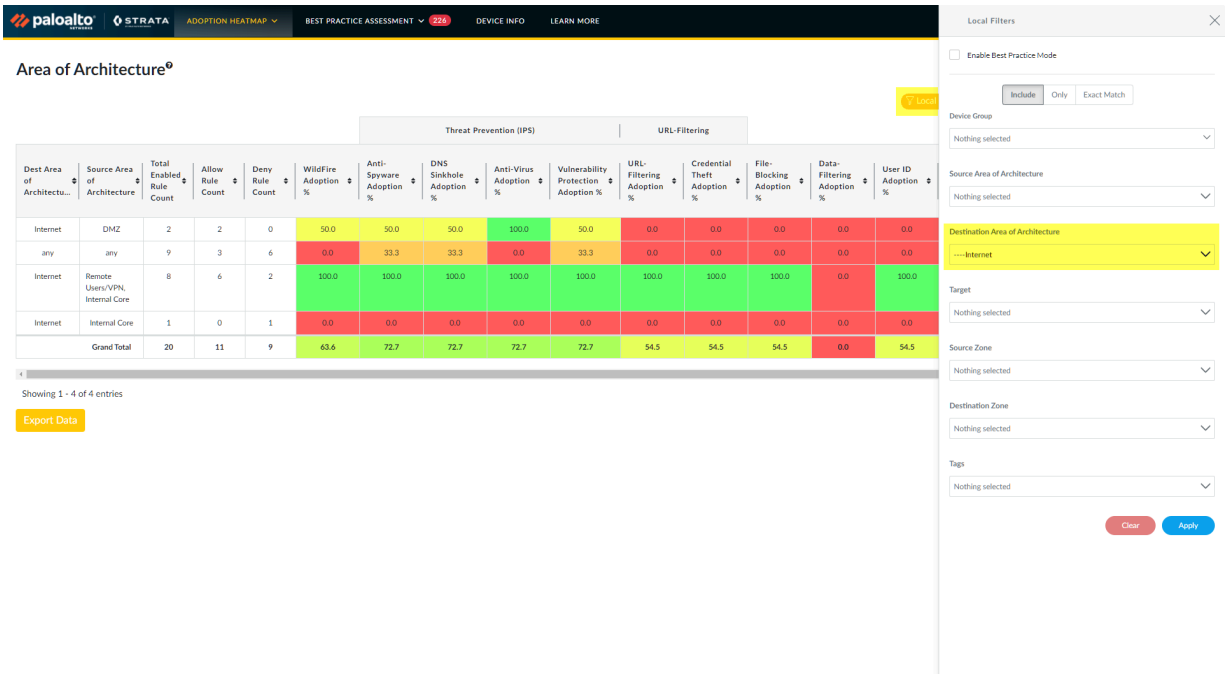
STEP 1 | 選取 **Adoption Heatmap**（採用熱圖） > **Areas of Architecture**（架構區域）。

STEP 2 | 按一下 **Local Filters**（本機篩選）以展開篩選選項。

STEP 3 | 將 **Destination Area of Architecture**（目的地架構區域）設定為 **Internet**（網際網路）。

STEP 4 | 按一下 **Apply**（套用）。

BPA 會篩選結果：



根據安全性目標和準則來解譯結果。例如，如果目標是將 WildFire 套用至 100% 的允許規則，則已篩選的採用熱圖顯示只有 50% 的 DMZ 允許規則具有 WildFire 設定檔，因此您已識別目標設為改善的漏洞。

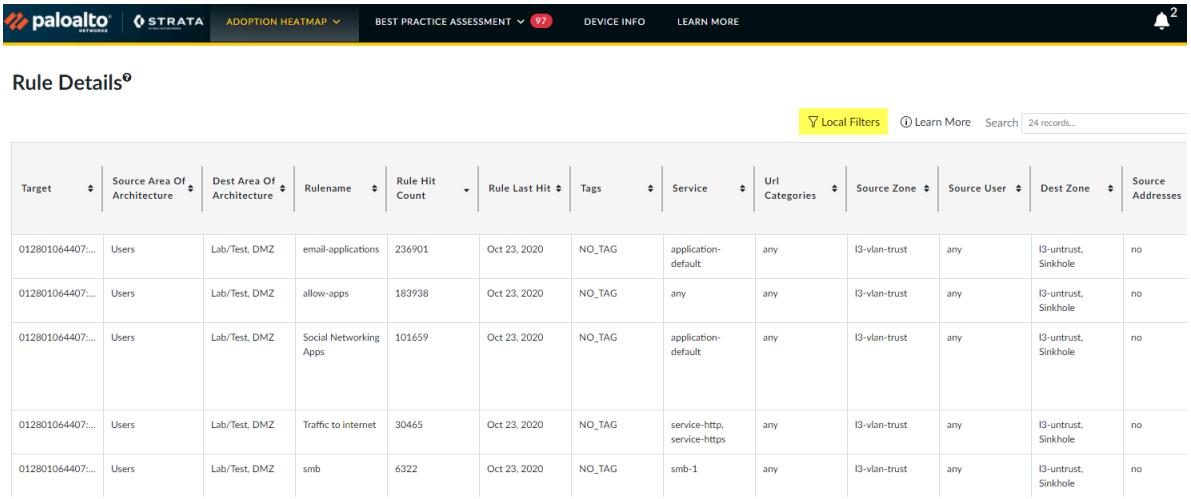
STEP 5 | 下一步：識別要改善的規則。

識別要改善的規則

在您識別安全性政策功能採用漏洞之後，請使用 **Adoption Heatmap**（採用熱圖） > **Rule Detail**（規則詳細資料）檢視以列出需要進一步調查或修復的規則。設定 **Local Filters**（本機篩選），以符合您在識別採用漏洞時所開發的漏洞識別準則。這會產生您可以匯出的規則清單，並將其遞交給操作團隊來負責防火牆安全性政策。

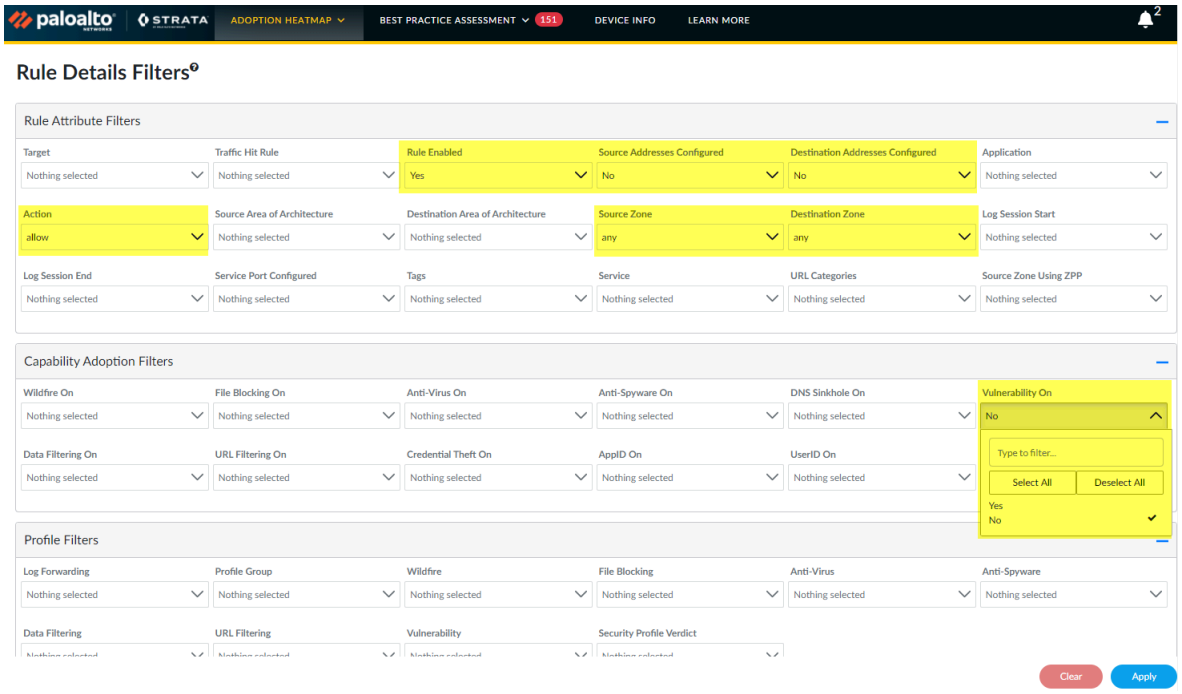
例如，建立規則詳細資料篩選，來識別允許所有流量但未設定弱點保護設定檔的規則：

STEP 1 | 從 [Adoption Heatmap（採用熱圖）] 功能表中，選取 **Rule Detail**（規則詳細資料） 檢視 [Rule Details（規則詳細資料）] 頁面。



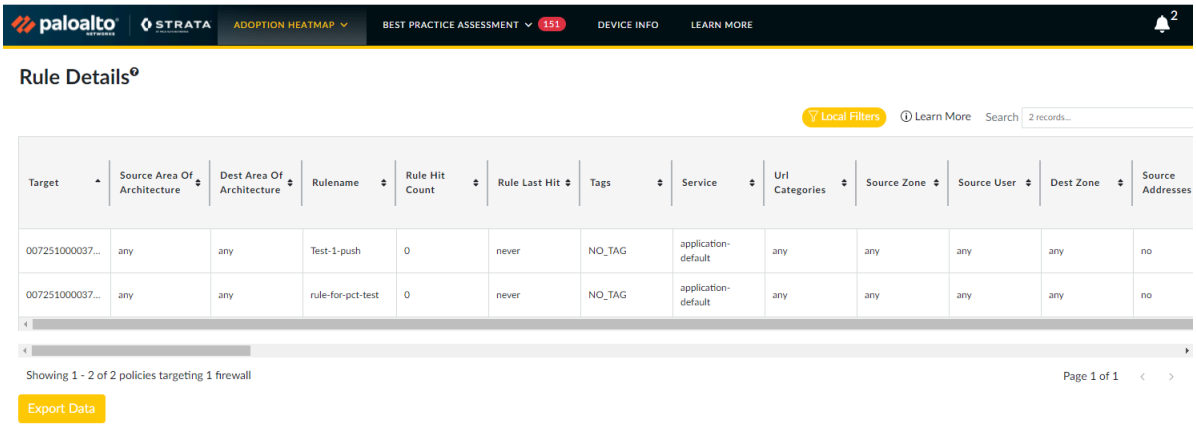
STEP 2 | 按一下 **Local Filters**（本機篩選）來檢視篩選選項，然後選取下列篩選：

- 來源區域 = **any**（任何）
- 目的地區域 = **any**（任何）
- 已設定來源位址 = **No**（否）
- 已設定目的地位址 = **No**（否）
- 動作 = **allow**（允許）
- 已啟用規則 = **Yes**（是）
- 開啟弱點 = **No**（否）



STEP 3 | 按一下 **Apply Filters**（套用篩選）。

BPA 會列出與篩選相符的規則：



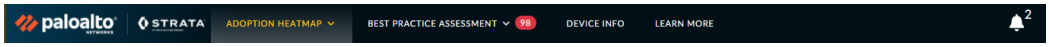
STEP 4 | 若要將已篩選的規則清單匯出至 .csv 檔案，請按一下 **Export Data**（匯出資料）。

STEP 5 | 下一步：評估最佳做法設定。

評估最佳做法設定

最佳做法評估 (BPA) 工具可協助您了解安全性政策中的目前最佳做法設定層級，以評估安全性狀態的成熟度。觀看 BPA 簡介視訊來了解 BPA，並利用 BPA 視訊庫和 BPA+ 視訊庫更深入了解該工具。

會先在 [Adoption Heatmap（採用熱圖）] 頁面上開啟 BPA 報告。按一下 **Best Practice Assessment**（最佳做法評估）來檢視報告的 BPA 區段，其聚焦於新世代防火牆和 Panorama 的設定最佳做法採用。



除了本文件之外，您還可以檢視 BPA 示範以及有關如何執行 BPA 的簡短視訊來深入了解如何使用 BPA。

BPA 報告會根據超過 200 次最佳做法檢查來評估新世代防火牆或 Panorama 設定檔案。BPA 會依政策、物件、網路和裝置/Panorama 資訊來分組評估結果，其與 PAN-OS 使用者介面類似。

在全景管理的環境中，*Panorama* 可能會管理大量的新世代防火牆。您應該在全景或是在每個個別防火牆上執行 *BPA?*權衡是速度和便利性與完整性。

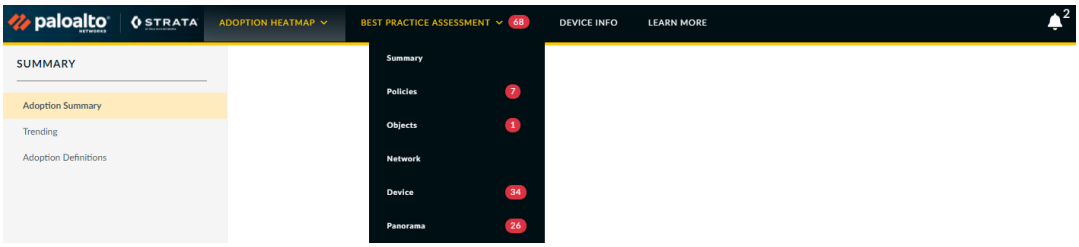
在 *Panorama* 上執行 *BPA* 既快速又方便，可評估受管理防火牆的大部分功能，但不會檢查本機防火牆取代。

在每個受管理防火牆上執行 *BPA* 會評估完整的設定（包括本機取代），但需要更多時間。

最實用的方法是首先在 *Panorama* 上執行 *BPA*。檢查結果，決定是否需要專注於任何特定的受管理裝置，然後在這些裝置上執行 *BPA*。此方法可節省時間，同時仍然專注於可讓您改善安全性狀態的相關資訊。

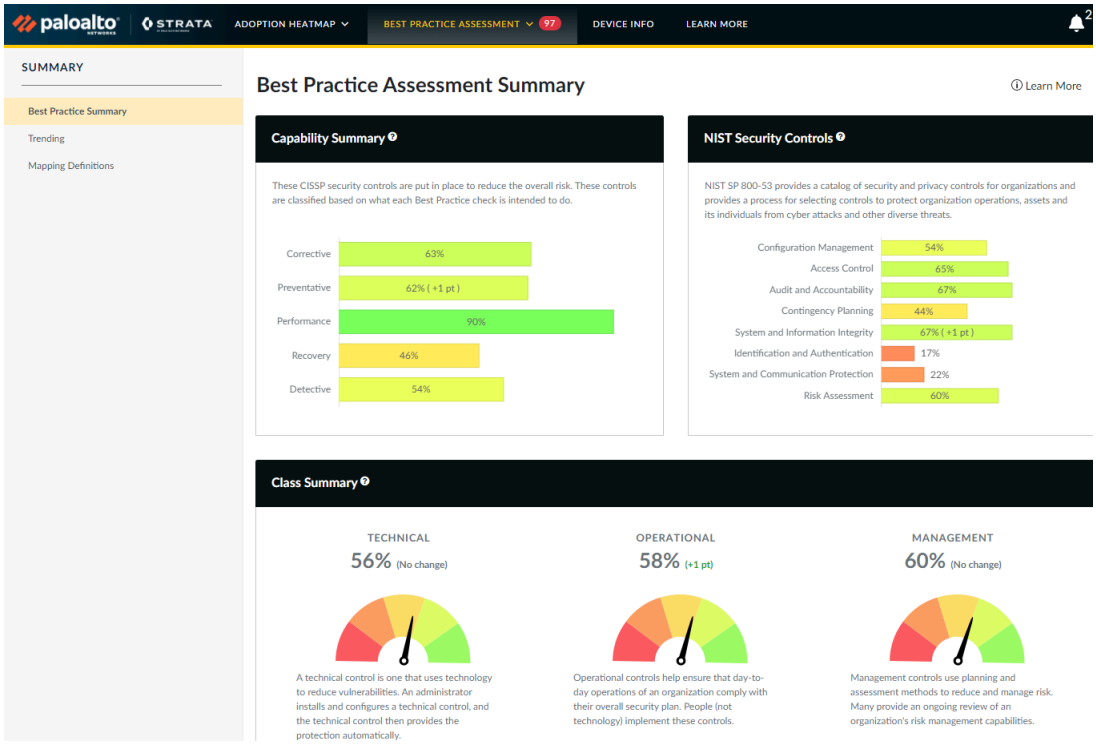
檢閱和分析資訊，以找到聚焦的區域，並改善：

- 檢閱最佳做法摘要
- 檢閱最佳做法政策設定
- 檢閱最佳做法物件設定
- 檢閱最佳做法網路設定
- 檢閱最佳做法裝置和 Panorama 管理設定



檢閱最佳做法摘要

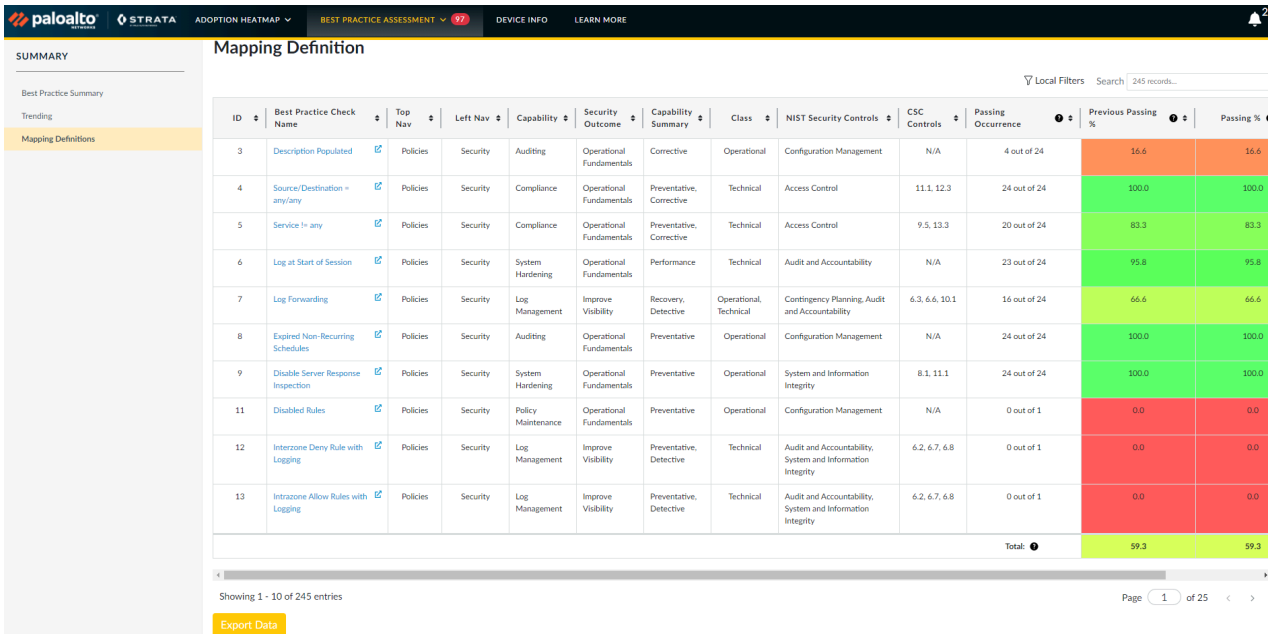
從 **Best Practice Assessment**（最佳做法評估）功能表中，選取 **Summary**（摘要）以檢視最佳做法摘要。



摘要會呈現對應至企業標準控制類別的最佳做法設定檢查結果，例如 Center for Internet Security (CIS) 的重大安全性控制，以及 Security Controls and Assessment Procedures 的 National Institute of Standards and Technology (NIST) 出版物。此資訊的用途是提供不錯的方式來了解 BPA 檢查如何關聯到企業標準，而非作為稽核。

與採用摘要類似，最佳做法摘要所包含的度量顯示目前採用率以及自最後一次對裝置設定產生 BPA 之後的採用進度（以括號括住）。

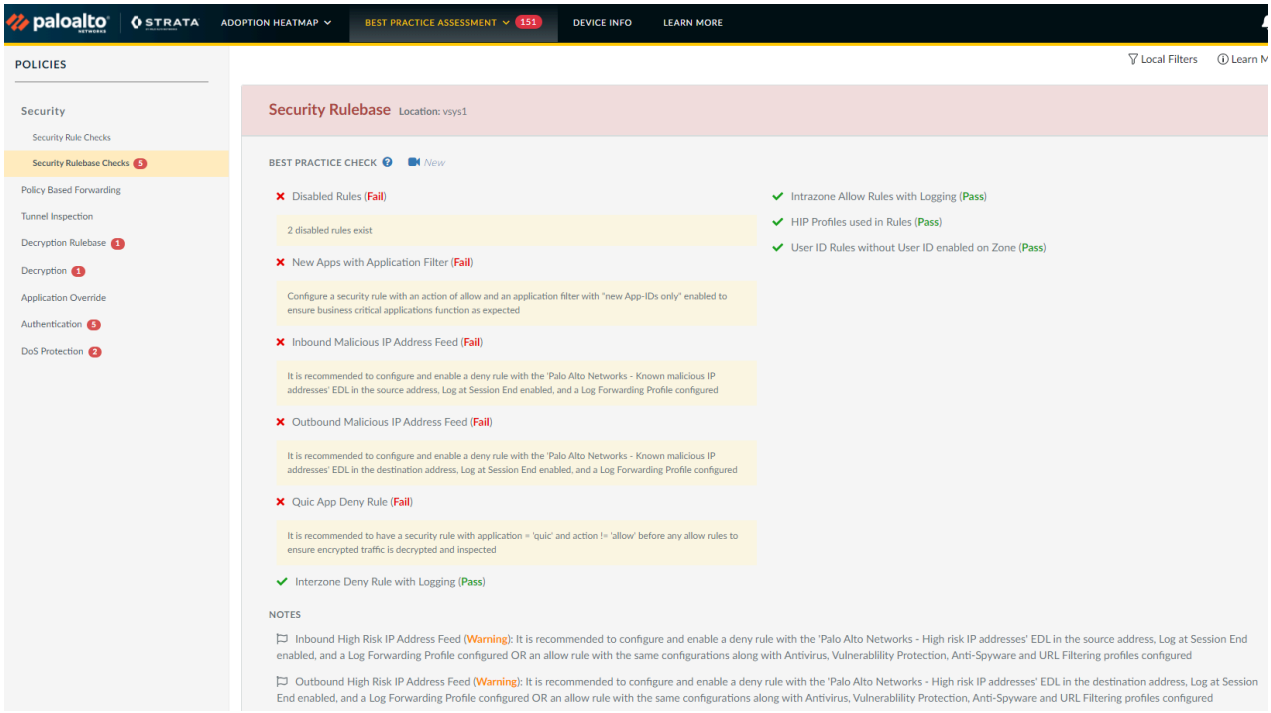
按一下 **Mapping Definitions**（對應定義）（左側側邊欄），以查看所有已對應檢查和其個別評分的完整清單。**Show Filters**（顯示篩選）以設定篩選、**Apply Filters**（套用篩選）至輸出，以及 **Export Mappings**（匯出對應）以將對應匯出至 .csv 檔案。



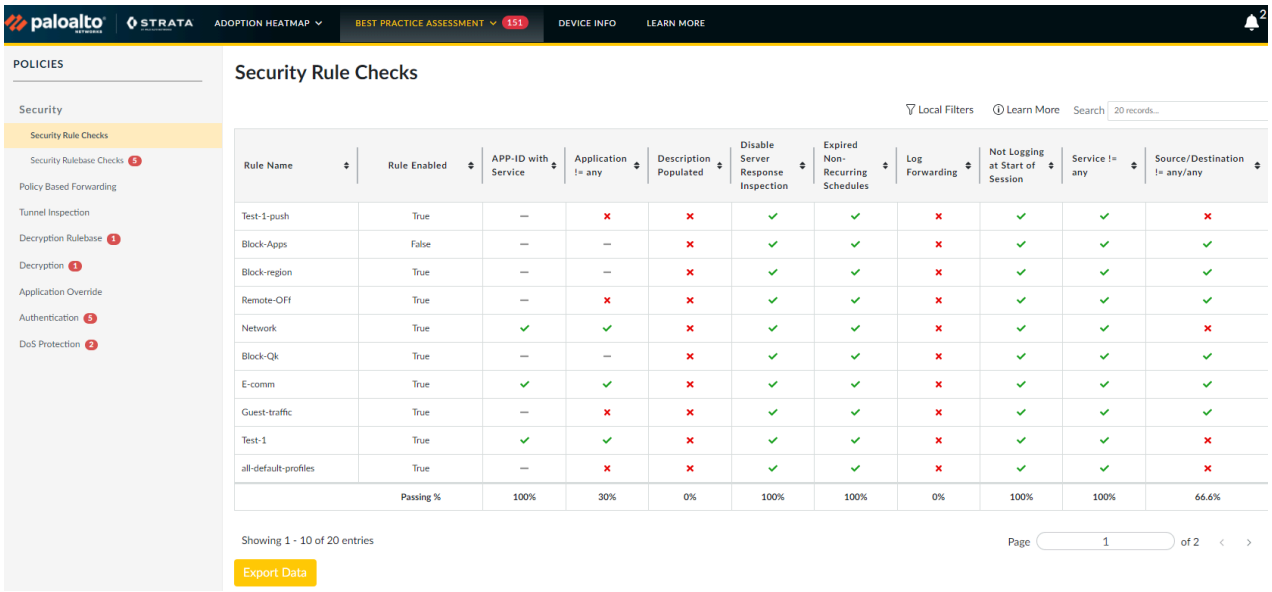
下一步：檢閱最佳做法政策設定。

檢閱最佳做法政策設定

Best Practice Assessment（最佳做法評估） > **Policies**（政策）會顯示所有與不同類型的防火牆政策相關的檢查，並在 **Security Rulebase checks**（應用程式篩選） 頁面上開始。**Security Rulebase checks**（安全性規則庫檢查）會依裝置群組來彙總最佳做法檢查結果，其中具有通過/未通過狀態以及失敗檢查的處理建議。按一下說明（ ）以檢視每個結果的描述和原理以及技術文件連結進行參考。



從左側功能表中選取您想要檢閱的政策類型，以識別潛在的規則改善。例如，**Security Rule Checks**（安全性規則檢查）顯示基於規則的檢查結果。按一下 **Local Filters**（本機篩選）以設定篩選，將結果的範圍縮小為讓一個或多個特定檢查失敗的規則。您可以 **Export Data**（匯出資料），以將清單匯出至 .csv 檔案來進行修復分析。



當您檢閱 **Policy**（政策）資訊時，請最多檢閱下列項目來協助了解政策修復範圍（切換檢視）：

- 安全性—識別讓 **Source/Destination !=any/any** 檢查失敗的規則。
- 安全性—識別讓 **App-ID with Service**（具有服務的 **App-ID**）檢查失敗的規則。
- 安全性—識別讓 **User-ID Rules without User ID enabled on Zone**（未在區域上啟用 **User ID** 的 **User-ID** 規則）檢查失敗的 User-ID 規則。
- 解密規則庫—SSH Proxy 解密檢查。
- 解密—每個解密政策規則都應該有相關聯的解密設定檔。

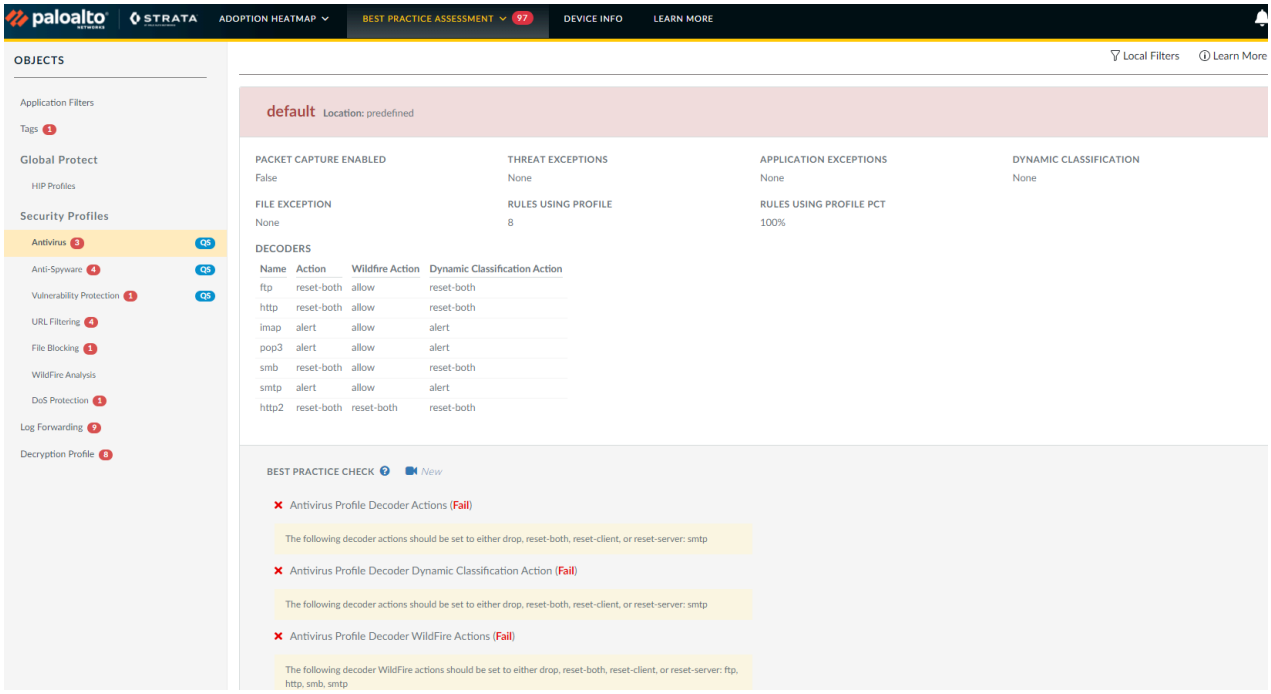
> 例外狀況是您藉由將「不解密」政策套用至流量來選擇不解密的 *TLSv1.3* 流量。當您將「不解密」設定檔附加至政策時，設定檔會檢查憑證資訊，以及封鎖使用錯誤憑證的解密工作階段。不過，因為 *TLSv1.3* 會加密憑證資訊，所以防火牆無法根據憑證資訊來封鎖未解密流量，因此沒有時間點可以將設定檔附加至政策。

- 應用程式覆寫—使用簡單自訂應用程式的應用程式覆寫規則會略過相符流量的第 7 層檢查。減少或刪除使用簡單自訂應用程式的應用程式取代規則，以 改善流量的可見度 並檢查這些規則所控制的應用程式和內容。

下一步：檢閱最佳做法物件設定。

檢閱最佳做法物件設定

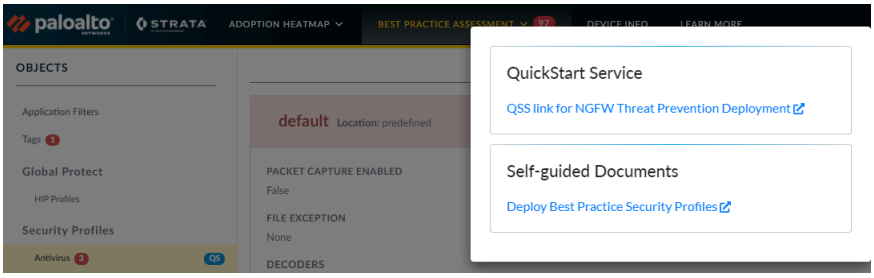
Best Practice Assessment（最佳做法評估） > **Objects**（物件）會顯示所有與不同類型的防火牆物件相關的檢查，並在 **Application Filters**（應用程式篩選） 頁面上開始。選取您想要檢閱的物件以了解現有設定，以及識別與應用程式篩選、標籤、GlobalProtect、安全性設定檔、日誌轉送和解密設定檔相關的最佳做法設定的潛在漏洞。下列範例會顯示當您選取防毒安全性設定檔物件時的結果。



針對每個防毒設定檔，報告會顯示目前設定以及有多少規則使用該設定檔。此報告會在目前設定下方顯示最佳做法檢查結果，其中具有通過/未通過狀態以及失敗最佳做法檢查的建議。按一下說明（ ），以取得每個檢查的原理以及最佳做法文件連結。

一個或多個檢查失敗時，設定檔標題會變成紅色。此報告會在底端列出目前未使用的設定檔，且標題為黃色。

螢幕左側之部分設定檔頁面連結旁邊的「QS」按鈕會將您連接至 QuickStart 服務選項。**QuickStart Service**（**QuickStart** 服務）藉由協助您規劃和執行防火牆即平台實作，來協助您增加安全性功能和投資。**Self-guided Documents**（自我引導式文件）可協助您瞭解、建立和部署物件。



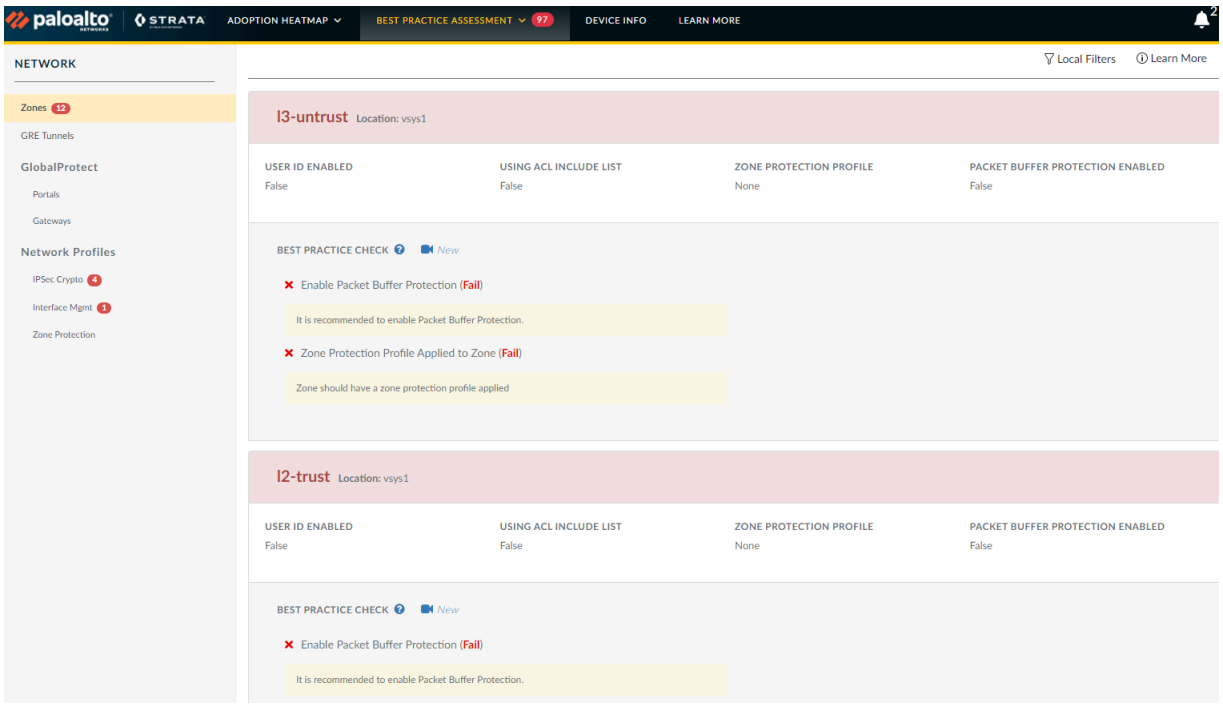
當您檢閱 **Objects**（物件）頁籤時，請最多檢閱下列項目來協助了解潛在修復範圍：

- 防毒—防毒和 WildFire 的解碼器動作。
- 反間諜軟體—嚴格設定檔、DNS Sinkhole。
- 弱點保護—嚴格設定檔。
- **URL** 篩選—是否封鎖已知不良類別。
- **WildFire** 分析—設定檔檔案類型（所有類型都應該傳送至 WildFire 來進行分析）。
- 日誌轉送—是否轉送所有日誌類型（轉送所有日誌類型）。

下一步：檢閱最佳做法網路設定。

檢閱最佳做法網路設定

Best Practice Assessment（最佳做法評估） > **Network**（網路）會顯示所有網路相關設定檢查，並在 **Zones**（區域） 頁面上開始。在左導覽上，選取您想要檢閱的網路檢查以了解現有設定，以及識別與區域、GRE 通道以及 GlobalProtect、IPsec 加密、介面管理和區域保護設定檔相關的最佳做法設定的潛在漏洞。下列範例會顯示區域的結果。



此報告會顯示每個項目的目前設定。每個項目的最佳做法檢查結果都會出現在其目前設定下方。您可以指定 **Device Group**（裝置群組）和（或）**Template**（範本）來限制所顯示資訊的範圍。

每個檢查都有通過/未通過狀態以及失敗最佳做法檢查的建議。按一下說明（ ），以取得每個檢查的原理以及最佳做法文件連結。一個或多個檢查失敗時，項目的標題會變成紅色。

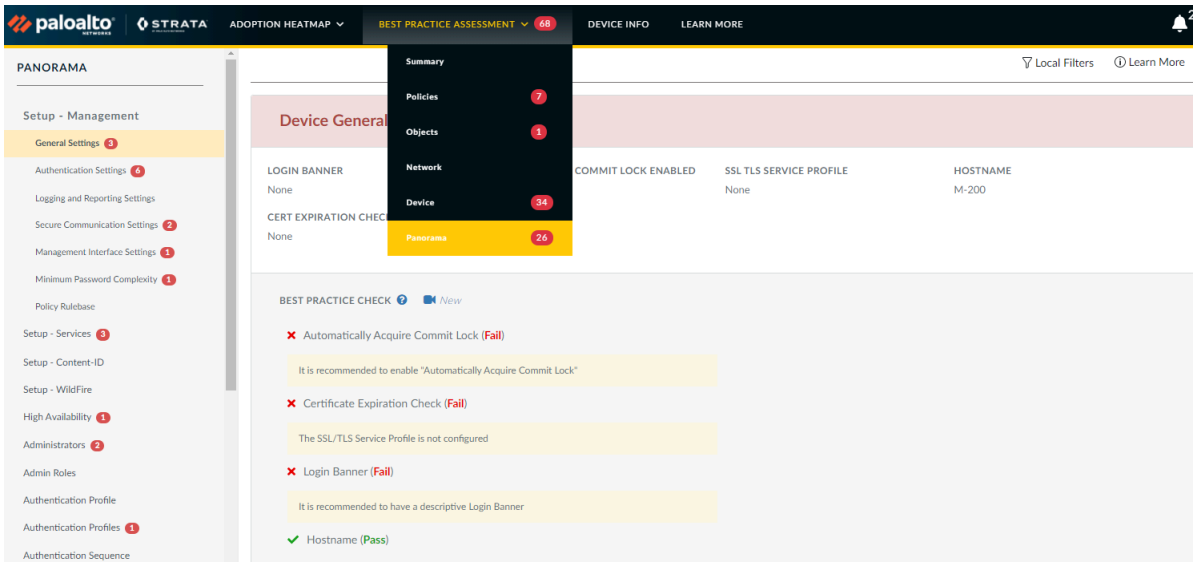
當您檢閱 **Network**（網路）頁籤時，請最多檢閱下列項目來協助了解潛在修復範圍：

- 區域—每個區域是否都已啟用封包緩衝區保護，並具有區域保護設定檔。
- 區域保護—是否已啟用流量保護和基於封包的攻擊保護。

下一步：檢閱最佳做法裝置和 Panorama 管理設定。

檢閱最佳做法裝置和 Panorama 管理設定

Best Practice Assessment（最佳做法評估） > **Device**（裝置）和 **Best Practice Assessment**（最佳做法評估） > **Panorama** 頁面會顯示所有與裝置管理安裝和設定相關的檢查。在獨立防火牆上，**Best Practice Assessment**（最佳做法評估） > **Device**（裝置）會在防火牆裝置之 [Management Setup（管理設定）] 頁面的 [General Settings（一般設定）] 上開始。在 Panorama 上，**Best Practice Assessment**（最佳做法評估） > **Device**（裝置）會在顯示每個範本堆疊之一般設定的頁面上開始。**Best Practice Assessment**（最佳做法評估） > **Panorama** 會在裝置之 [Management Setup（管理設定）] 頁面的 [General Settings（一般設定）] 上開始。選取您想要檢閱的檢查以了解現有設定，以及識別與防火牆和 Panorama 裝置管理相關的最佳做法設定的潛在漏洞。下列範例會顯示 Panorama 裝置上 [General Settings（一般設定）] 的結果。



此報告會顯示每個項目的目前設定。每個項目的最佳做法檢查結果都會出現在其目前設定下方。檢視 **Device**（裝置）的資訊時，您可以指定 **Template**（範本）來限制所顯示資訊的範圍。

每個檢查都有通過/未通過狀態以及失敗最佳做法檢查的建議。按一下說明（ ），以取得每個檢查的原理以及最佳做法文件連結。一個或多個檢查失敗時，項目的標題會變成紅色。

當您檢閱 **Device**（裝置）或 **Panorama** 頁籤時，請最多檢閱下列項目來協助了解潛在修復範圍：

- **Dynamic Updates**（動態更新）—防毒、應用程式、威脅和 WildFire 更新。
- **Management Interface Settings**（管理介面設定）—網路連線服務、允許的 IP 位址。
- **Administrators**（管理員）—本機管理員、管理員密碼設定檔。檢查 **Device (設備)** > **Administrators (管理員)** 或**Panorama** > **Administrators (管理員)**，確定管理員的密碼已設定最少必要複雜性。
- **Minimum Password Complexity**（最低密碼複雜度）—密碼最低複雜性需求檢查。

下一步：排定最佳做法變更的優先順序。

排定最佳做法變更的優先順序

BPA 報告中的資訊量可能會爆滿。本章提供建議來協助您排定設定改善的優先順序，以關閉安全性漏洞、先實作最高價值增強功能，並達成最佳做法安全性狀態。

在全景管理的環境中，*Panorama* 可能會管理大量的新世代防火牆。您應該在全景或是在每個個別防火牆上執行 *BPA?*權衡是速度和便利性與完整性。

在 *Panorama* 上執行 *BPA* 既快速又方便，可評估受管理防火牆的大部分功能，但不會檢查本機防火牆取代。

在每個受管理防火牆上執行 *BPA* 會評估完整的設定（包括本機取代），但需要更多時間。

最實用的方法是首先在 *Panorama* 上執行 *BPA*。檢查結果，決定是否需要專注於任何特定的受管理裝置，然後在這些裝置上執行 *BPA*。此方法可節省時間，同時仍然專注於可讓您改善安全性狀態的相關資訊。

下列各主題聚焦於如何依序改善通常用來實作新部署的安全性狀態，並依序聚焦於管理、可見度、控制和強制執行。在每個區域中，現有部署可能已達成某種程度的成熟度。

- 加強裝置管理狀態
- 改善流量的可見度
- 實作初始最佳做法控制
- 微調並增強最佳做法控制

加強裝置管理狀態

加強裝置管理狀態可藉由防止可能會危害防火牆的未經授權存取來保護其安全、降低非預期事件的操作影響，並更好地查看防火牆操作。

- 遵循管理存取權的最佳做法，防止未經授權和不安全地存取裝置的管理介面。
- 將所有系統和設定日誌轉送至 Panorama 和協力廠商監控解決方案，以追蹤系統相關事件和設定變更。
- 建立設定備份排程，更快速地修復設定相關問題和系統故障。

在您設定變更之後，請執行 BPA 以驗證變更、測量進度，以及排定後續變更的優先順序。

下一步：改善流量的可見度。

改善流量的可見度

您無法保護自己免於看不到的威脅，因此您必須隨時確定已具有跨所有使用者和應用程式的流量的完整可見度。完整查看網路上的應用程式、內容和使用者，是邁向明智政策控制的第一步：

- 將安全性設定檔採用最大化。在您 檢閱採用摘要 並識別採用漏洞之後，請使用安全轉換步驟來修復漏洞，以達成完整最佳做法安全性設定檔實作。
- 將跨安全性政策規則庫的記錄採用最大化（包含日誌轉送），以檢查所有 流量。
- 設定動態內容更新的最佳做法，確定防火牆具有最新應用程式和威脅特徵碼以保護您的網路，以及您根據網路安全性和可用性需求來部署更新。
- 根據最佳做法計劃 SSL 解密部署。
- 在使用者區域（使用者從中啟動流量的內部信任區域）中啟用 User-ID，以將應用程式流量和相關聯的威脅對應至使用者和裝置。

  請不要在外部不受信任區域中啟用 *User-ID*。如果您在外部不受信任區域上啟用 *User-ID*（或用戶端探查，例如 *WMI*），則探查可能會傳送至您受保護的網路以外，並公開 *User-ID* 資訊（例如 *User-ID* 代理程式服務帳戶名稱、網域名稱和加密密碼雜湊），進而讓攻擊者得以危害您的網路。

- 減少或刪除應用程式覆寫規則，以檢查這些規則所控制的應用程式和內容（應用程式覆寫規則是不允許防火牆檢查流量的第 4 層規則）。不需要或減少基本應用程式覆寫規則的範圍：
  - 驗證規則的使用案例是否仍然存在。通常會建立應用程式覆寫規則來克服與效能、通訊協定解碼器或未知應用程式相關的特定問題。經過一段時間，PAN-OS 更新、內容更新或硬體升級可能會移除部分應用程式覆寫規則的需求。如果您在防火牆上執行 PAN-OS 9.0 或更新版本，或在管理執行 PAN-OS 8.1（或更新版本）的防火牆的 Panorama 上執行 PAN-OS 9.0 或更新版本，則可以使用政策最佳化工具以將規則轉換為第 7 層規則。
  - 減少應用程式覆寫規則的範圍，讓它只影響最少可能的流量。定義太廣的規則可能會覆寫多於必要或預定流量的流量。在每個應用程式覆寫規則中定義來源和目的地區域、位址和（或）連接埠，以盡可能限制規則的範圍。
  - 建立內部應用程式的第 7 層自訂應用程式。
  - 使用自訂逾時值來建立服務物件。
- 計劃部署 DoS 和區域保護並進行基準線 CPS 測量，以設定合理的流量保護閾值。

當您實作這些原生 App-ID、Content-ID、User-ID 和 SSL 解密功能時，防火牆可以查看和檢查您的所有流量（應用程式、威脅和內容），並將事件關聯到使用者，不論位置、裝置類型、連接埠、加密或攻擊者的具規避性技術為何。

改善功能採用（例如 *SSL* 解密、記錄、流量保護、安全性設定檔等等）可能會導致額外的防火牆資源耗用。了解您防火牆的容量，並確定對其進行適當地調整，以處理任何其他負載。*Palo Alto Networks SE* 或 *CE* 可以協助您調整部署的大小。您也可能需要額外日誌儲存空間。

在您設定變更之後，請執行 BPA 以驗證變更、測量進度，以及排定後續變更的優先順序。

下一步：實作初始最佳做法控制。

實作初始最佳做法控制

在您查看並瞭解網路上的流量（應用程式、內容、威脅和使用者）之後，請實作嚴格控制以減少攻擊面，並防止已知和未知威脅來完成轉換為最佳做法設定。

- 在您 檢閱採用摘要 並識別採用漏洞之後，請遵循安全轉換步驟來達成最佳做法安全性設定檔以封鎖威脅並減少攻擊面，包含在資料中心實作嚴格控制以保護您業務的最重要資產。
- 為資料中心和周邊防火牆建立基於應用程式的安全性政策規則；請使用不在資料中心內的其他防火牆的周邊防火牆最佳做法建議。如果您在防火牆上執行 PAN-OS 9.0 或更新版本，或在管理執行 PAN-OS 8.1（或更新版本）的防火牆的 Panorama 上執行 PAN-OS 9.0 或更新版本，則可以使用政策最佳化工具以將基於連接埠的規則轉換為基於應用程式的規則。
- 建立基於使用者的存取政策。
- 部署最佳做法區域保護設定檔至所有區域。
- 部署 SSL 解密，讓防火牆可以查看（解密）和檢查加密流量。

在您實作控制功能之後，防火牆可以掃描所有允許的流量並偵測與封鎖網路和應用程式層弱點入侵、緩衝區溢位、DoS 攻擊、連接埠掃描以及已知和未知惡意軟體變體。防火牆可以控制應用程式和使用者存取權，以及封鎖惡意和不需要的應用程式。

在您設定變更之後，請執行 BPA 以驗證變更、測量進度，以及排定後續變更的優先順序。

下一步：微調並增強最佳做法控制。

微調並增強最佳做法控制

在您對網路流量（應用程式、內容、威脅和使用者）實作控制之後，請開始微調控制，並實作其他功能來改善安全性狀態。

- 如果您尚未將內部應用程式轉換為自訂應用程式來查看和控制流量，則請將內部應用程式轉換為自訂應用程式。
- 在您使用安全轉換步驟開始移至最佳做法設定檔之後，請將安全性設定檔調整為最佳做法。
- 根據 Palo Alto Networks 的威脅情報和可信協力廠商摘要，來封鎖已知惡意 IP 位址。
- 部署 GlobalProtect 或 Prisma Access，將新世代安全性平台延伸至各地的使用者和裝置。
- 啟用認證竊取防護。
- 設定基於網路的多因素驗證。

接下來：執行 BPA 以驗證變更、測量進度以及排定後續變更的優先順序；深入了解最佳做法，以及深入了解 Panorama 和 PAN-OS 新世代防火牆的許多安全性功能。

