資料中心最佳做法安全性原則

Version 10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

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

About the Documentation

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

Copyright

Last Revised

November 2, 2020

Table of Contents

資料中心安全性原則最佳做法檢查清單

您企業最寶貴的資產儲存於資料中心內，包括專有源代碼、智慧財產及敏感的公司和客戶資料。您的客戶和員工相信您會保證其資料的機密性和完整性，並希望可隨時存取這些資料，因此實施資料中心最佳做法安全性原則來保護您的資料並防止有效攻擊至關重要。僅強化網路周邊是不夠的，因為攻擊可以來自網路內部，可以來自認證受到攻擊的合作夥伴和承包商，而且如果攻擊者在您的網路中找到了立足點，便可透過在裝置之間橫向移動從網路內部發起攻擊。

如果您很熟悉 Palo Alto Networks 平台，則可透過使用這一簡化的檢查清單來實施預先部署、部署及部署後資料中心安全性原則最佳做法，從而節省時間。在完整的資料中心最佳做法安全性政策文件或 PAN-OS 10.0 管理員指南中，每節都包含詳細資訊的連結，其中包括如何設定政策規則和安全性設定檔。

- 規劃資料中心最佳做法部署
- 部署資料中心最佳做法
- 遵循部署後資料中心最佳做法

規劃資料中心最佳做法部署

透過制定策略和部署計劃，準備在資料中心實作最佳做法。使用積極的安全性強制執行（建立規則，以允許您想要允許之使用者與應用程式流量並拒絕其他所有內容）以實現零信任架構。

STEP 1 | 設定目標。

- 定義資料中心網路的理想未來狀態，以便您具有明確待實現的目標，並知道何時實現了這些目標。
- 保護已啟動連線之每個區域中的流量：
  1. 流向資料中心的本機使用者流量。
  2. 從網際網路流向資料中心的流量。
  3. 從資料中心流向網際網路的流量。
  4. 資料中心內伺服器或 VM 之間的流量（資料中心內的東西向流量）。
- 請勿在資料中心內允許不明使用者、應用程式或流量。
- 建立標準化的可調式設計，使您可以在整個資料中心一致地複製並套用該設計。

STEP 2 | 與 IT /支援部門、安全性部門等利益關係人及需要資料中心存取權限的群組（如工程、法律、財務與人力資源）合作，共同制定存取策略。

- 確定需要存取權限的使用者以及其需要存取的資產。瞭解這一點，您就可以根據存取層次要求建立使用者群組，確保可依使用者群組設計高效的安全性原則規則。
- 確定想要在資料中心內允許（認可）的應用程式。若要減少受攻擊面，請僅出於合法業務原因認可應用程式。

STEP 3 | 評估資料中心可瞭解其現行狀態，使您可以建立計劃，將資料中心安全性轉換為所需的未來狀態。

- 對實體與虛擬環境及資產進行資產管理，包括：
  - 伺服器、路由器、交換器、安全性裝置、負載平衡器以及其他網路基礎結構。
  - 標準和專有自訂應用程式以及用於通訊的服務帳戶。將應用程式詳細目錄清單與要認可之應用程式的清單進行比較。

    著重於要允許的應用程式，因為允許清單安全性政策規則允許這些應用程式，並且依預設，會拒絕所有其他應用程式來減少攻擊面。將應用程式對映於業務要求。若應用程式未對映於業務要求，請評估您是否確實需要允許該應用程式。
  - 評估每個資產，協助對先要保護的內容設定優先順序。可以問自己這樣的問題：「是什麼定義和區分了我們的公司？」，「在日常運營中必須使用哪些系統？」以及「如果我失去了這項資產，會產生怎樣的後果？」
- 與應用程式、網路與企業架構設計師以及業務代表合作，共同描繪資料中心流量特徵，並瞭解一般基準線流量負載與模式，便於您瞭解正常的網路行為。使用應用程式控管中心 Widget 以及流量分析工具來確定流量基準線。

STEP 4 | 建立資料中心分割策略，可防止在資料中心獲得立足點的惡意軟體橫向移動以感染其他系統。

- 將防火牆用作分割閘道，以顯示資料中心流量與系統，使您可以精確控制哪些人員可以使用哪些應用程式來存取哪些裝置。對使用實體防火牆的非虛擬伺服器以及使用 VM 系列防火牆的虛擬網路進行分割，並保護其安全。
- 使用防火牆的靈活分割工具（比如區域、動態位址群組、App-ID 以及 User-ID）來設計精確分割策略，用以保護敏感伺服器與資料。
- 對執行類似功能且在同一區段中需要相同層次的安全性的資產進行分組。
- 若要分割資料中心應用程式，則可分割構成應用程式層的伺服器層（通常服務鏈包含 Web 伺服器層、應用程式伺服器層以及資料庫伺服器層），然後使用防火牆來控制並檢查各個層之間的流量。

- 考慮在資料中心內使用 SDN 解決方案，以實現靈活的虛擬化基礎結構，從而最大限度地提高資源利用率並簡化自動化和擴充。

STEP 5 | 計劃使用最佳做法方法學以檢查所有資料中心流量，使其完全可見，減少受攻擊面，並防止已知與未知威脅。

- 將實體或虛擬防火牆放置在可以查看所有資料中心網路流量的位置。
- 利用防火牆功能強大的工具集，建立與特定使用者群組相關之基於應用程式的安全性原則規則，且受安全性設定檔保護。將未知檔案轉送至 WildFire，然後部署解密，以防威脅以加密流量進入資料中心。
- 在內部模式下，使用 GlobalProtect 作為控制資料中心存取的閘道。
- 對使用者進行驗證，可防止未獲授權的存取，並設定多因素驗證以存取敏感應用程式、服務以及伺服器，特別是對於承包商、合作夥伴以及其他需要存取資料中心的協力廠商。
- 使用 Panorama 集中管理防火牆，以在整個實體與虛擬環境執行一致的原則，並實現集中顯示。
- 若有多個資料中心，請重複使用範本與範本堆疊，以在不同位置套用一致的安全性原則。

STEP 6 | 隨著時間的推移，逐步進行最佳做法部署；首先著重於業務與網路最有可能面臨的威脅，並先保護最有價值的資產。

考慮所有資料中心使用者、應用程式、裝置與流量，然後圍繞這些內容建立最佳做法安全性原則。若您嘗試一次完成所有操作，這可能看起來是一項艱鉅任務。但如果先保護最有價值的資產，然後規劃分階段的逐步實作，您便可以一種實用方式順利地從最理想的安全性原則轉換到最佳做法安全性原則，從而安全地啟用應用程式、使用者及內容。

部署資料中心最佳做法

在建立安全性設定檔、解密設定檔、安全性原則規則、驗證原則規則以及解密原則規則時，實作資料中心最佳做法。

對於安全性、驗證和 *DoS* 原則規則，請對 *Panorama* 或外部服務設定日誌轉送，以集中顯示日誌，方便透過通知來檢視及分析。

- 全域資料中心物件、政策和動作
- 使用者資料中心流量政策
- 網際網路至資料中心流量政策
- 資料中心至網際網路流量政策
- 內部資料中心流量政策
- 資料中心安全性政策規則庫順序

全域資料中心物件、政策和動作

確定您可以保護所使用的自訂應用程式。設定安全性設定檔和解密設定檔，並在所有資料中心端點上安裝 Cortex XDR 代理程式。

- 自訂應用程式
- 安全性設定檔
- 解密設定檔
- 流量封鎖規則
- 在端點上安裝 Cortex XDR 代理程式

STEP 1 | 若資料中心應用程式詳細目錄包含專有自訂應用程式，則為其建立自訂應用程式，以便您可以在安全性原則中指定這些應用程式。

STEP 2 | 設定嚴格的資料中心最佳做法安全性設定檔，以防威脅中斷資料中心網路。

- ❑ 若要設定最佳做法防毒軟體設定檔，則可複製預先定義的設定檔，並在 Action（動作）及 WildFire Action（WildFire 動作）欄中將 imap、pop3 及 smtp 解碼器值變更為 **reset-both**（重設兩者）。
- ❑ 透過複製預先定義的嚴格設定檔來設定最佳做法反間諜軟體設定檔。對於記錄的流量，在 **Rules**（規則）頁籤上，對嚴重性層級分別為中、高及重要的威脅啟用單一封包擷取。（對於未記錄的流量，套用單獨的設定檔而不啟用封包擷取。）

  若防火牆看不到 DNS 查詢的發起者（通常，當防火牆位於本機 DNS 伺服器北方時），則在 DNS Signatures（DNS 特徵碼）頁籤上，將 DNS 查詢的 **Action**（動作）變更為 **sinkhole**，方便您識別受感染的主機。可能遭入侵的主機會試圖存取可疑網域，而 DNS sinkhole 會對這些主機進行識別並追蹤，以防其存取這些網域。對遭到 sinkhole 攻擊的流量啟用延伸封包擷取。
- ❑ 若要設定最佳做法漏洞保護設定檔，則可複製預先定義的嚴格設定檔，並將每個規則（**simple-client-informational**（簡單用戶端資訊）與 **simple-server-informational**（簡單伺服器資訊）除外）的「封包擷取」設定變更為 **single-packet**（單一封包）。若防火牆識別大量漏洞威脅並影響效能，則對嚴重性層級為低的事件停用封包擷取。
- ❑ 預先定義的嚴格檔案封鎖設定檔便為最佳做法設定檔。若支援重要的應用程式可防止您封鎖所有檔案類型，則會封鎖嚴格的設定檔（您可以在 **Monitor**（監控）> **Logs**（日誌）> **Data Filtering**（資料篩選），從資料篩選日誌中識別資料中心內所使用的檔案類型），以及複製嚴格的設定檔並根據需要加以修改。若檔案不需要在兩個方向流動，則使用 **Direction**（方向）設定將檔案類型限制為僅所需的方向。
- ❑ 預先定義的WildFire 分析設定檔便為最佳做法設定檔。WildFire 針對不明威脅與進階持續威脅 (ATP) 提供了最佳防禦措施。

STEP 3 | 設定嚴格的資料中心最佳做法解密設定檔，以防止不明流量進入資料中心。

- 執行 CRL/OCSP 檢查，以確保 SSL 解密期間所示的憑證有效。
- SSL 通訊協定設定：將 **Min Version**（最低版本）設定為 **TLSv1.2**，**Max Version**（最高版本）設定為 **Max**（最高），然後取消核取 **SHA1** 驗證演算法。（弱 3DES 與 RC4 加密演算法會在您選取 TLSv1.2 時自動取消核取。）請針對支援 TLSv1.3 的流量使用 TLSv1.3（許多行動應用程式都會使用固定憑證，這會防止在使用 TLSv1.3 時解密，因此對於這些應用程式，使用 TLSv1.2）。
- SSL 正向 Proxy：對於 **Server Certificate Verification**（伺服器憑證驗證），封鎖具有過期憑證、不受信任的簽發者以及不明憑證狀態的工作階段，並限制憑證延伸。對於 **Unsupported Mode Checks**（不受支援的模式檢查），封鎖具有不受支援版本、不受支援的密碼套件以及用戶端驗證的工作階段。對於 **Failure Checks**（失敗檢查），在資源無法使用時封鎖工作階段則是使用者體驗（封鎖可能會對使用者體驗產生負面影響）與可能允許危險連線之間的權衡。若必須考慮此權衡，還應考慮增加部署中的可用解密資源。
- SSL 輸入檢查：對於 **Unsupported Mode Checks**（不受支援的模式檢查），封鎖具有不受支援版本以及不受支援密碼的工作階段。對於 **Failure Checks**（失敗檢查），權衡類似於 SSL 正向 Proxy。
- SSH Proxy：對於 **Unsupported Mode Checks**（不受支援的模式檢查），封鎖具有不受支援版本以及不受支援演算法的工作階段。對於 **Failure Checks**（失敗檢查），權衡類似於 SSL 正向 Proxy。
- 將不解密設定檔套用至因法規、合規性規則或業務原因而選擇不解密的流量，TLSv1.3 流量除外（TLSv1.3 會加密憑證資訊，因此防火牆無法根據憑證資訊來封鎖流量）。以過期憑證封鎖工作階段與不信任的發布者。

STEP 4 | 設定流量封鎖規則，即可拒絕已知的惡意流量或業務目的不需要的流量。

記錄並監控封鎖規則可能會顯示網路上存在您不知道的使用者與應用程式，這可能是合法的，也可能指示存在攻擊。安全性原則規則庫中的規則順序對於防止產生影響至關重要（流量符合允許或封鎖規則，然後可以比對您希望與之相符的規則）。某些規則幾乎相同，但可為標準及非標準連接埠或其他來源的使用者應用程式與應用程式啟用單獨報告。對於每個規則，請在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄），然後設定日誌轉送以追蹤及分析規則違規。

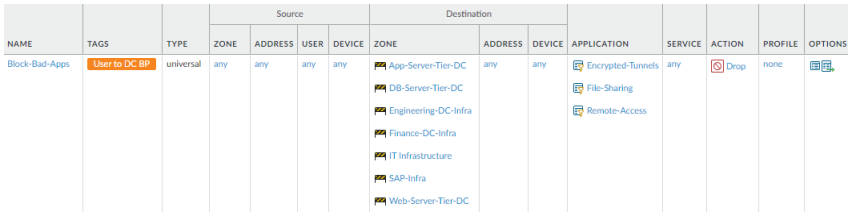
- 封鎖 **application-default**（應用程式預設）連接埠上使用者區域中的所有應用程式。將此規則置於允許使用者區域中合法應用程式流量的規則之後，可識別標準連接埠上的不明或非預期使用者應用程式。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-User-Zone	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

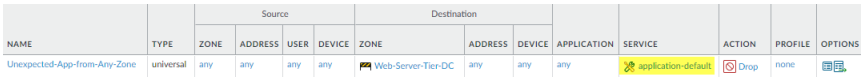
- 封鎖 **any**（任意）連接埠上使用者區域中的所有應用程式，即可捕捉試圖使用非標準連接埠的使用者流量。將此規則置於之前的 **application-default**（應用程式預設）封鎖規則之後，即可識別非標準連接埠上的不明或非預期使用者應用程式（可能是自訂應用程式或規避應用程式）。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-User-App-Any-Port	User to DC BP	universal	Contractors Engineering-Users Finance-Users IT-Users	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

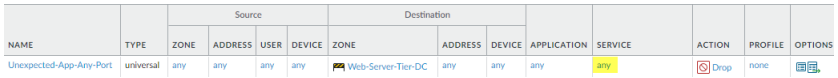
- 封鎖您從未想要在資料中心內允許的應用程式（比如規避應用程式與容易被入侵的應用程式）以及非業務所需的應用程式。將此規則置於應用程式允許規則之後，（舉例來說）可在 **Filesharing**（檔案共用）應用程式篩選器封鎖所有其他檔案共用應用程式之前允許認可的檔案共用應用程式。



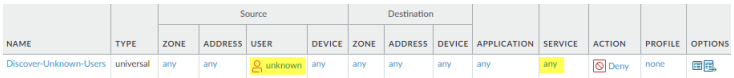
- 封鎖 **application-default**（應用程式預設）連接埠上 **any**（任意）區域中的所有應用程式，即可識別標準連接埠上的非預期應用程式。規則相符項可能指示潛在威脅或需要修改允許規則的應用程式變更。將此規則置於應用程式允許規則與前述封鎖規則之後。



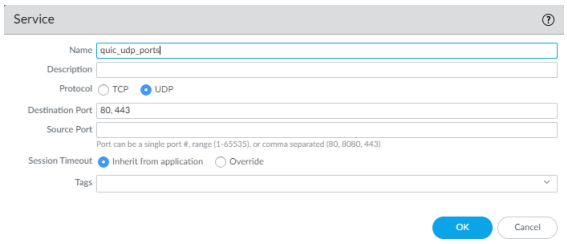
- 封鎖 **any**（任意）連接埠上任意區域中的所有應用程式，即可識別非標準連接埠上的非預期應用程式。請勿允許不明的 TCP 流量、不明的 UDP 流量或非同步 TCP 流量。將此規則置於應用程式允許規則與前述封鎖規則之後。



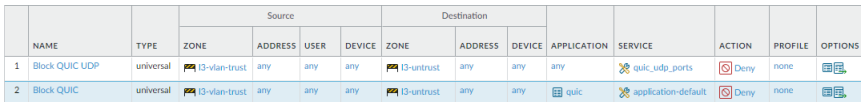
- 封鎖試圖在任意連接埠上執行應用程式的不明使用者，即可發現不明使用者（User-ID 覆蓋範圍內的漏洞或攻擊者）並識別遭入侵的裝置（包含內嵌裝置，如列印機、讀卡機以及攝影機）。將此規則置於應用程式允許規則與前述封鎖規則之後。



- 除了封鎖不想要的潛在惡意流量之外，請封鎖快速 UDP 網際網路連線 (QUIC) 通訊協定，除非基於業務原因，您想要允許加密瀏覽器流量。Chrome 以及其他一些瀏覽器會使用 QUIC 而非 TLS 建立工作階段，但 QUIC 使用防火牆無法解密的專用加密手法，因此潛在危險的流量可能會如加密流量般進入網路。同時封鎖 QUIC 應用程式以及 UDP 連接埠 80 和 443，以強制瀏覽器使用 TLS。先建立一個包括 UDP 連接埠 80 和 443 的服務（**Objects**（物件）> **Services**（服務））：



使用該服務指定 UDP 連接埠以封鎖 QUIC。在第二個規則中，封鎖 QUIC 應用程式，讓規則庫中的前兩個規則封鎖 QUIC：



STEP 5 | 在所有資料中心端點上安裝 Cortex XDR 代理程式，以抵禦端點上的惡意軟體和入侵。

Cortex XDR 代理程式保護所有端點的方式都相同，因此，對於資料中心與任何其他網路區域，部署處理程序與惡意軟體保護政策最佳做法相同。

使用者資料中心流量政策

為需要存取資料中心的使用者設定安全性政策、驗證政策和解密政策。

- 使用者安全性政策規則
- 使用者驗證政策規則
- 使用者解密政策規則

STEP 1 | 為使用者流量建立應用程式允許清單安全性政策規則以允許適當的存取。

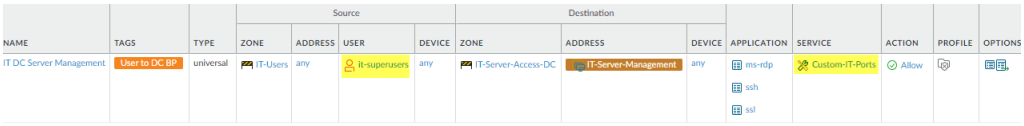
將使用者存取的允許規則置於規則庫頂端、封鎖規則之前，以防意外封鎖合法流量。對於每個規則，請在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄），然後設定日誌轉送以追蹤及分析規則違規。

- 允許員工使用者存取內部公司 DNS 伺服器。此規則允許任何使用者，因為使用者會在登入之前存取 DNS 服務。該規則會嚴格控制來源區域、目的地伺服器以及應用程式，並將安全性設定檔套用至流量。

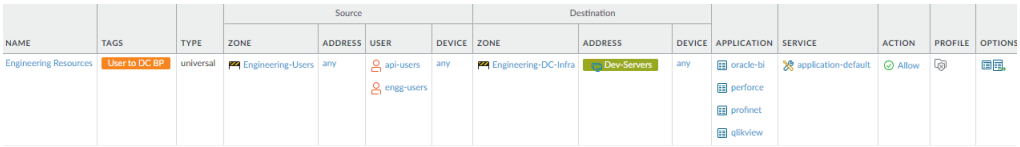
  封鎖對網際網路閘道處之外部 *DNS* 伺服器的存取，以防 *DNS* 流量從網際網路流向公共伺服器。

- 允許 IT 人員在必要時安全地特許存取資料中心管理介面。將規則限制為管理介面（在此範例中，會使用位址群組識別裝置，以及使用自訂服務識別管理連接埠），以及必要的應用程式（在此範例中為 RDP、SSH 及 SSL）。使用專用 VLAN 將管理流量與其他流量進行區分，並將管理介面置於相同的子網路上。

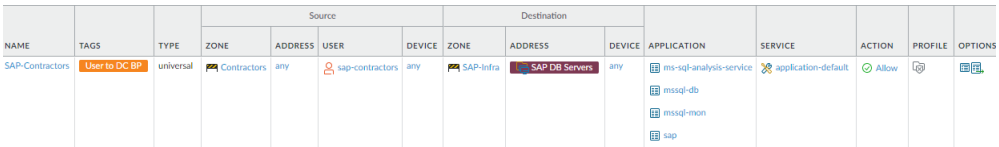
  若相同 *IT* 使用者群組還管理交換器、路由器以及其他資料中心裝置，請將其新增至目的地，並將其連接埠新增至自訂服務，從而確保規則可以保護與其管理介面之連線的流量。若不同 *IT* 群組管理不同的資料中心資源，請為每個群組建立單獨的安全性原則規則及相應的解密與驗證原則規則。



- 允許員工使用者群組進行必要的存取。這些規則限制每個使用者群組（或使用者）對必要應用程式與伺服器的存取。在此範例中，將限制工程使用者群組僅存取其開發伺服器與應用程式。



- 允許有針對性的有限存取承包商、合作夥伴、客戶及其他協力廠商。在此範例中，將限制 SAP 承包商群組的存取權限，使該群組只能使用適當的應用程式存取相應的 SAP 資料庫伺服器。

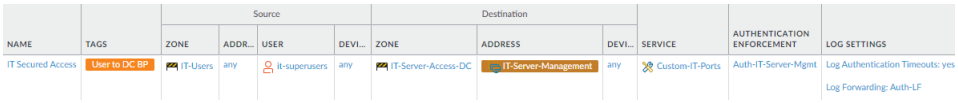


STEP 2 | 為使用者流量建立驗證原則規則，即可驗證資料中心存取權限。

對於您為其建立應用程式允許規則的每個使用者群組或使用者，建立類似的驗證規則（DNS 允許規則除外，因為 DNS 出現在使用者驗證登入之前）。對於每個規則，請在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄），然後設定日誌轉送以追蹤及分析規則違規。

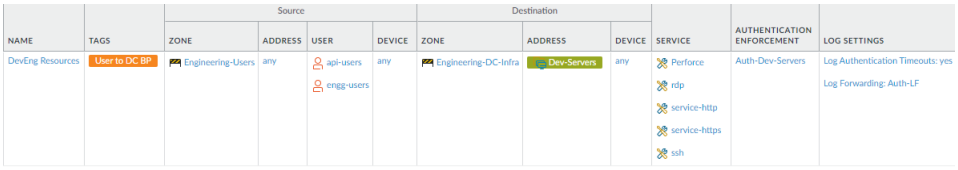
- 對需要專用存取權限的使用者進行驗證。在此範例中，會對需要安全特許存取權限的 IT 人員進行驗證，以根據前述步驟的允許規則管理資料中心伺服器。由於特許使用者憑證遭入侵會將資料中心王國的金鑰交給攻擊者，需要多因素驗證 (MFA)，以防遭竊取的憑證。

  若相同 *IT* 使用者群組還管理交換器、路由器以及其他資料中心裝置，請將其新增至目的地，並將其連接埠新增至自訂服務，從而確保規則可以驗證與其管理介面之連線的流量。若不同 *IT* 群組管理不同的資料中心資源，請為每個群組建立單獨的安全性原則規則及相應的解密與驗證原則規則。



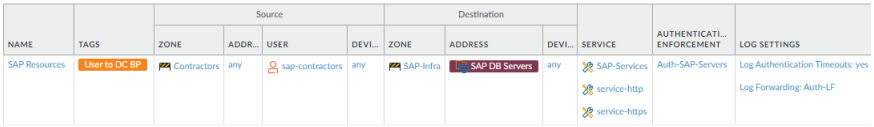
NAME	TAGS	Source ZONE	Source ADDR...	Source USER	Source DEVI...	Destination ZONE	Destination ADDRESS	Destination DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
IT Secured Access	User to DC BP	IT-Users	any	it-superusers	any	IT-Server-Access-DC	IT-Server-Management	any	Custom-IT-Ports	Auth-IT-Server-Mgmt	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

- 對以合法業務原因存取資料中心的員工進行驗證。在此範例中，會根據前述步驟的允許規則驗證工程開發使用者群組。



NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

- 驗證承包商、合作夥伴、客戶以及其他非員工群組。要求對非員工群組使用 MFA 來防止協力廠商公司的憑證被竊取。在此範例中，會根據前述步驟的允許規則驗證 SAP 開發人員。



NAME	TAGS	Source ZONE	Source ADDR...	Source USER	Source DEVI...	Destination ZONE	Destination ADDRESS	Destination DEVI...	SERVICE	AUTHENTICATI... ENFORCEMENT	LOG SETTINGS
SAP Resources	User to DC BP	Contractors	any	sap-contractors	any	SAP-Infra	SAP DB Servers	any	SAP-Services service-http service-https	Auth-SAP-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

STEP 3 | 為使用者流量建立解密原則規則，即可對允許的流量進行解密，使防火牆可以看到、檢查流量並對其套用安全性原則。

對於每個解密原則規則，套用適當的最佳做法解密設定檔（SSL 輸入檢查、SSL 正向 Proxy、SSH Proxy 或無解密，包含用於 SSL 輸入檢查與 SSL 正向 Proxy 規則的最佳做法 SSL 通訊協定設定），以封鎖弱通訊協定與演算法並驗證伺服器憑證。對於每個 SSL 輸入檢查規則，匯入使用解密保護之資料中心伺服器的憑證。

將流量排除在解密之外的原因只有兩個：

- 因技術原因（比如釘選憑證或相互驗證）而中斷解密的流量。將技術排除項新增至 *Device*（裝置）> *Certificate Management*（憑證管理）> *SSL Decryption Exclusion*（*SSL* 解密排除項）清單。
- 出於業務、法規、符合性或其他原因，選擇不解密的流量，比如財務、健康或政府流量。為您選擇不解密的流量建立基於原則的解密排除項。

- 從之前建立的安全性原則規則中，解密允許 IT 人員特許存取管理伺服器的流量。解密原則規則與其相關聯的解密設定檔有所不同，具體視 IT 群組是使用 SSL（SSL 正向 Proxy 解密設定檔）還是 SSH（SSH Proxy 解密設定檔）來存取管理連接埠而定。

  若相同 *IT* 使用者群組還管理資料中心交換器、路由器以及其他裝置，請將其新增至目的地，並新增伺服器憑證，從而確保規則可以解密與其管理介面之連線的流量。若不同 *IT* 群組管理不同的資料中心資源集，請為每個群組建立單獨、嚴格的安全性原則規則及相應的解密與驗證原則規則。

  對於 SSL 特許存取權限：

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

對於 SSH 特許存取權限：

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

- 設定 SSL 輸入檢查以解密來自員工使用者群組的允許流量。在此範例中，會解密來自類似工程開發使用者群組允許規則的流量。

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- 設定 SSL 輸入檢查以解密來自承包商、合作夥伴、客戶以及其他協力廠商的允許流量。在此範例中，會解密來自類似 SAP 承包商使用者群組允許規則的流量。

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

- 套用無解密設定檔，以便為以下流量設定伺服器驗證：出於業務、法規、符合性或其他原因，選擇不解密的流量，比如財務、健康或政府流量。在此範例中，會顯示兩組財務使用者在存取 **Fin Servers**（**Fin** 伺服器）位址群組中的伺服器時，系統如何將其排除在解密之外。

請不要將不解密設定檔套用至 *TLSv1.3* 流量，因為已加密憑證資訊，讓防火牆無法根據憑證資訊來封鎖工作階段。

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

網際網路至資料中心流量政策

設定從網際網路至資料中心之流量的安全性政策、解密政策和拒絕服務 (DoS) 保護政策。

- 網際網路至資料中心安全性政策
- 網際網路至資料中心解密政策
- 網際網路至資料中心 DoS 保護政策

STEP 1 | 為網際網路至資料中心流量建立應用程式允許清單安全性政策規則，以控制並保護合作夥伴、承包商和客戶的存取權限。

防止從受感染的外部用戶端下載惡意軟體或從受感染的資料中心伺服器將惡意軟體置於外部伺服器上。建立業務目的所需之應用程式的允許規則，並建立外部動態清單 (EDL) 來封鎖錯誤的 IP 位址。對於每個規則，請在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄），然後設定日誌轉送以追蹤及分析規則違規。

在此範例中，會限制網際網路至資料中心的流量的應用程式與目的地，並使用 **Negate**（否定）選項來防止與 **Bad IPs List**（錯誤 **IP** 清單）EDL 進行通訊。

NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
			ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Web Server Inbound	Internet to DC	universal	L3-External	~~Bad IPs List~~	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

為網際網路至其他伺服器群組（若允許）以及其他應用程式的流量建立類似的規則。將每個規則具體化，以限制僅存取必要的應用程式與伺服器。

STEP 2 | 為網際網路至資料中心的流量建立解密原則規則，以解密允許的流量。

為網際網路至資料中心的流量設定 SSL 輸入檢查（並將目的地伺服器憑證匯入防火牆），以解密安全性原則規則允許的合作夥伴、承包商以及客戶流量。此範例顯示前述安全性原則規則的解密原則。

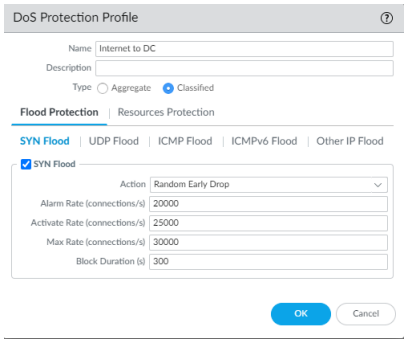
		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

建立解密規則，以符合網際網路至資料中心的安全性原則規則允許的流量。

STEP 3 | 若要建立網際網路至資料中心的 DoS 保護原則規則來保護敏感伺服器免遭「拒絕服務 (DoS)」攻擊，則可限制防火牆允許送達伺服器的每秒連線數 (CPS) 來防止 SYN 爆流攻擊。

若攻擊者將 Web 伺服器層關閉，則會阻止對資料中心的大多數合法存取，因此 Web 伺服器層便成為其攻擊目標。套用具有 DoS 保護設定檔的分類 DoS 保護原則規則，可限制傳入的 CPS，以防流量突增進而影響伺服器效能及可用性。

- 建立分類 DoS 保護設定檔，可保護 Web 伺服器層並防止 SYN 爆流攻擊。設定的 CPS 臨界值取決於基準線尖峰 CPS 速率。



- 建立 DoS 保護原則規則，可指定要保護的 Web 伺服器並對其套用分類 DoS 保護設定檔。

		Source			Destination				Protection		
NAME	TAGS	ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS	SERVICE	ACTION	AGGREGATE	CLASSIFIED	LOG FORWARDING
DC Web Server Protection	Internet to DC BP	L3-External	Bad-IPs-List	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

若要防止外部來源的 SYN 洪水攻擊，請建立單獨的 DoS 保護原則規則，將您的內部區域指定為來源區域，而不是 **L3-External**。針對外部和內部攻擊來源的單獨規則提供單獨的報告，可讓您更輕鬆地調查試圖進行的攻擊。

- 此外，還需為每個資料中心區域設定封包緩衝保護，以保護防火牆免遭單一工作階段 DoS 攻擊，從而避免丟棄合法流量。

資料中心至網際網路流量政策

設定從資料中心到網際網路之流量的安全性政策和解密政策。

- 資料中心至網際網路安全性政策
- 資料中心至網際網路解密政策

STEP 1 | 建立資料中心至網際網路允許規則，以保護與外部伺服器的連線。

資料中心伺服器可從網際網路上的伺服器中獲取軟體更新或憑證狀態。最大的風險在於連接錯誤的伺服器。為更新建立嚴格的允許規則，以限制可存取的外部伺服器數量以及允許的應用程式數量（僅在預設

連接埠上）。這會防止受感染的資料中心伺服器進行回撥，並防止在非標準連接埠上使用 FTP、HTTP 或 DNS 等合法應用程式來洩漏資料。此外，使用檔案封鎖設定檔的 **Direction**（方向）控制來封鎖輸出更新檔案，以便僅允許下載軟體更新檔案。

對於每個規則，套用最佳做法安全性設定檔並在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄）。

與更新軟體的工程群組和其他群組合作，可記錄和分析 *Web* 瀏覽工作階段，以定義開發人員為獲取更新而連接的 *URL*。

- 在這些範例中，允許工程伺服器與下列伺服器進行通訊：使用 **yum** 應用程式的 CentOS 更新伺服器（**CentOS-Update-Servers**（**CentOS** 更新伺服器）自訂 URL 類別），以及使用 **ms-update** 應用程式的 Microsoft 更新伺服器（**Win-Update-Servers**（**Win** 更新伺服器）自訂 URL 類別）（您還必須允許 **ssl**，因為 **ms-update** 在 SSL 上具有相依性）。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

- 允許存取 DNS 與 NTP 更新（**NTP DNS Update Servers**（**NTP DNS** 更新伺服器）自訂 URL 類別）。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

- 允許連線至網際網路線上憑證狀態通訊協定 (OCSP) 回應程式，以檢查驗證憑證的撤銷狀態，並確保其是否有效。當您在防火牆上設定憑證設定檔時，若 OCSP 回應程式無法存取，請將 CRL 狀態驗證設定為 OCSP 的回復方法。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Cert Update	DC to Internet BP	universal	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	Allow		

STEP 2 | 建立資料中心至網際網路的解密原則規則，便可對之前的安全性原則規則內允許的流量進行解密。

遭入侵的更新伺服器可能會下載惡意軟體並在軟體更新過程中加以傳播，因此解密流量以獲取可見性至關重要。由於只有服務帳戶啟動更新流量且更新流量沒有個人或敏感資訊，因此不存在隱私權問題。

請勿解密流向 *OCSP* 憑證撤銷伺服器的流量，因為該流量通常使用 *HTTP*，而沒有進行加密。此外，*SSL* 正向 *Proxy* 解密可能會中斷更新過程，因為防火牆可充當 *Proxy*，並將用戶端憑證更換為 *Proxy* 憑證，而 *OCSP* 回應程式可能無法將其作為有效憑證予以接受。

- 解密資料中心和更新伺服器之間的流量。在這兩個範例中，會解密前述步驟中類似安全性原則規則允許的 CentOS 與 Windows 更新流量。

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

NAME	TAGS	Source ZONE	Source ADDRESS	Destination ZONE	Destination ADDRESS	URL CATEGORY	Decrypt Options ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- 解密資料中心伺服器和 NTP 與 DNS 更新伺服器之間的流量。在此範例中，會解密前述步驟中類似安全性原則規則允許的更新流量。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

內部資料中心流量政策

設定資料中心伺服器與應用程式層間之流量的安全性政策和解密政策。

- 內部資料中心安全性政策
- 內部資料中心解密政策

STEP 1 | 建立內部資料中心應用程式允許規則，即可保護資料中心伺服器免受其他可能遭入侵之資料中心伺服器的攻擊。

常見的應用程式架構包含三個伺服器層：Web 伺服器、應用程式伺服器以及資料庫伺服器。將最佳做法安全性設定檔套用至伺服器層間的大多數流量來抵禦威脅。請勿將安全性設定檔套用至低價值、大容量的流量（如郵箱複製與備份流量）—防火牆已檢查原始流量，因此在其上花費 CPU 週期亦不會產生額外的價值。為這些應用程式建立允許規則以防誤用。對於每個規則，請在 **Actions**（動作）頁籤上設定 **Log at Session End**（工作階段結束時記錄），然後設定日誌轉送以追蹤及分析規則違規。

在此範例中，會對以下兩個已為其建立自訂應用程式之專用內部財務應用程式設定規則，以允許應用程式伺服器層之間的流量：**Billing-App** 和 **Payment-App**。

- 允許 Web 伺服器層和應用程式伺服器層之間的財務應用程式流量。

			Source			Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web to App Server	Intra DC BP	universal	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	Allow		

- 允許應用程式伺服器層與資料庫伺服器層之間的財務應用程式流量。

			Source			Destination						
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	ZONE	ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
App to DB Server	Intra DC BP	universal	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	Allow		

STEP 2 | 建立內部資料中心解密政策規則，便可對之前的安全性政策規則內允許的流量進行解密。

資料中心是攻擊者藏身的理想場所，因為許多人認為資料中心很安全，而不會尋找入侵者。但網路其他部分的基本原理也同樣適用於資料中心：您不能防止自己免受您看不見的威脅的攻擊。解密經加密的資料中心流量，使防火牆能夠檢查流量、控制存取、使威脅可見，並保護您的寶貴資產。

並不會加密所有資料中心流量。請不要將資源用在解密未加密（純文字）流量。

- 此規則解密財務部帳單伺服器的 Web 伺服器層和應用程式伺服器層之間流動的流量。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

- 此規則解密財務部帳單伺服器的應用程式伺服器層與資料庫伺服器層之間流動的流量。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

資料中心安全性政策規則庫順序

在安全性政策規則庫中正確地排序規則，確定您只允許您要允許的應用程式和流量，這樣就沒有規則會影響另一個規則。

對資料中心安全性政策規則庫進行排序，會以正確的順序顯示之前範例（允許和封鎖規則）中的完整規則庫，並對每個規則的位置進行說明。

遵循部署後資料中心最佳做法

開始部署資料中心最佳做法之後，監控網路可確保安全性與存取能按預期進行，然後在環境變更時維護規則庫。

STEP 1 | 檢查預先定義的應用程式報告（**Monitor**（監控）> **Reports**（報告）> **Application Reports**（應用程式報告）> **Applications**（應用程式）），確認僅有安全性政策規則中允許的應用程式正在執行。

如果發現非預期應用程式，請檢閱安全性原則規則並對其進行調整，以刪除非預期應用程式或容納合法應用程式。

STEP 2 | 記錄所有資料中心流量。

使用 Palo Alto Networks 的廣泛監控工具、記錄工具、預先定義報告以及自訂報告，以擷取並監控非預期應用程式、使用者、流量及行為的活動。

STEP 3 | 建立自訂報告來監控封鎖規則，這些規則用於防禦潛在的攻擊，還可識別原則漏洞以及非預期行為，因此您可以調整規則庫。

STEP 4 | 建立自訂報告，以記錄符合規則庫底部之預先定義區域內預設允許規則的資料中心內的流量。依預設，該規則會允許相同區域內的所有流量。

STEP 5 | 對符合規則庫底部之預先定義的區域間預設規則的資料中心流量啟用日誌記錄並為其建立自訂報告。依預設，該規則會拒絕區域間的所有流量。

STEP 6 | 傾聽並回應使用者回饋。

使用者投訴無法存取應用程式，這可在應用程式允許清單阻止使用規則庫或已在網路中使用之具風險的應用程式之前，識別其內存在的漏洞。

STEP 7 | 定期將您在規劃階段進行的基準線測量與現行測量進行比較，以評估進度，確定變更並找到需要改進的領域。

同時，重新審視網路之理想未來狀態的目標，以評估進度。若用 Panorama 管理防火牆，監控防火牆健康以將裝置與其基準線效能進行比較，並相互比較，以確定與正常行為的偏差。

STEP 8 | 隨著時間推移，應用程式允許規則會發生變化，因為應用程式發展、使用者要求變更以及內容更新會修改現有的 App-ID 並引進新的 App-ID。

在安裝新內容版本之前，維護資料中心最佳做法規則庫並檢閱新的及修改過的 App-ID，以便在變更影響原則時修改規則庫。

STEP 9 | 使用 Palo Alto Networks 評估及檢閱工具，以評估現行防禦狀態以及最佳做法的採用情況。

STEP 10 | 如需每個規劃、部署及後置部署步驟及其實現效果的相關詳細資料，請參閱完整的資料中心最佳做法安全性原則。

資料中心最佳做法安全性原則

您企業最寶貴的資產儲存於資料中心內，包括專有源代碼、智慧財產及敏感的公司和客戶資料。您的客戶和員工相信您會對其敏感資料保密，並希望可隨時存取資料中心，因為他們希望可隨時使用自己的資料。實施資料中心最佳做法安全性原則來保護您的資料並防止有效攻擊，對於業務的完整性和成功至關重要。

下列方法和建議為資料中心最佳做法安全性原則按優先次序的階段式規劃、設計和實施提供了一個藍圖。如果您嘗試一次性在所有網路區域實現各種保護措施，那麼建立資料中心最佳做法安全性原則可能是一項艱巨的任務。但是，如果您要評估哪些資料是最重要、最需要保護的，並在開始實施資料中心最佳做法安全性原則時先保護最寶貴的資產，則可逐漸轉過渡到允許您安全啟用應用程式、使用者和內容的安全性原則，而不必承擔過高的風險。

資料中心安全性原則最佳做法檢查清單提供了預先部署、部署和部署後最佳做法的概觀，如果您不需要詳細說明，還可提供快速實施最佳做法的方式。

- 什麼是資料中心最佳做法安全性原則？
- 為何需要資料中心最佳做法安全性原則？
- 資料中心最佳做法方法
- 為何部署資料中心最佳做法安全性原則？
- 如何存取您的資料中心
- 如何部署資料中心流量
- 建立資料中心分割策略
- 如何建立資料中心最佳做法安全性設定檔
- 使用 Cortex XDR 代理程式保護資料中心端點
- 建立資料中心流量封鎖規則
- 定義初始使用者至資料中心流量安全性原則
- 定義初始網際網路至資料中心流量安全性原則
- 定義初始資料中心至網際網路流量安全性原則
- 定義初始內部資料中心流量安全性原則
- 對資料中心安全性原則規則庫進行排序
- 記錄和監控資料中心流量
- 維護資料中心最佳做法規則庫
- 使用 Palo Alto Networks 評估與檢閱工具

什麼是資料中心最佳做法安全性原則？

資料中心最佳做法安全性原則可保護您自己公司的寶貴資料，保護您的客戶、合作夥伴及供應商的機密性，保護網路與業務運營的完整性，並有助於確保網路的持續可用性。它還可沿著所有攻擊載體抵禦來自網路內外的攻擊。

資料中心最佳做法安全性原則可保護四種流量（啟動連線的來源區域）：

1. 流向資料中心的本機使用者流量。
2. 從網際網路流向資料中心的流量。
3. 從資料中心流向網際網路的流量。
4. 伺服器或 VM 間流動的資料中心內的流量，也稱為東西向流量。

資料中心最佳做法安全性原則可防止攻擊者在您的資料中心獲得立足點，並防止任何設法入侵資料中心的攻擊者洩露資料或在網路內橫向移動以破壞重要的伺服器。它透過實作安全性原則規則來實現符合您的業務要求的最佳做法目標，從而防止已知與未知的威脅。作用：

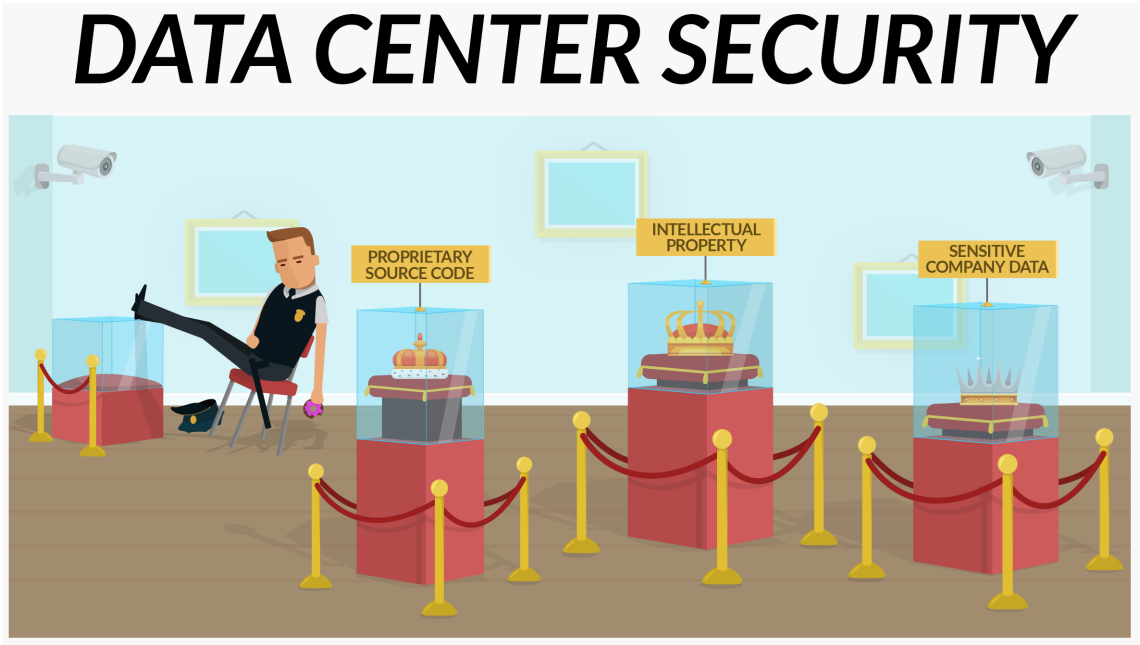
- 識別應用程式，無論連接埠、通訊協定或規避技術如何，包括透過解密加密流量。
- 識別並控制所有 IP 位址、位置或裝置的使用者。
- 提供保護，抵禦已知及未知的應用程式所攜帶的威脅及漏洞。
- 偵測可能指示攻擊進行中的異常行為。

資料中心最佳做法安全性原則還會在入侵者違反原則規則時將其捕獲。違反規則即會停止攻擊，因為違規會使新世代防火牆拒絕存取並記錄此違規，方便您調查問題並採取適當動作。

為何需要資料中心最佳做法安全性原則？

保護網路的可用性、機密性和完整性，使您可以安全執行業務，而不會中斷，並符合有關保護敏感資料的法規，這一點至關重要。強化網路外部且允許網路內部保持柔軟（因為內部受信任）的想法已經過時，並會使網路更容易遭到來自內部的攻擊，亦沒有考慮到資源豐富的持久攻擊者堅定決心地在周邊內尋找立足點的情況。這就是您為何需要像保護企業網路周邊一樣強有力地保護資料中心周邊和內部。

內部攻擊可能來自當前員工或現場承包商等來源。內部攻擊的常見執行緒是攻擊來自合法使用者或應用程式來源。外部攻擊可能來自網路犯罪分子、駭客行為主義者和國家支持的攻擊者，也可能來自不太明顯的攻擊途徑，例如遭入侵的合作夥伴或供應商系統，或者知道網路的前僱員。外部攻擊者的第一步是在網路中獲得立足點，將攻擊轉換為內部攻擊。本質上，所有入侵皆為內部攻擊，即使它們來自外部，因為一旦攻擊者獲得網路的存取權限，攻擊者就可以在整個網路中漫遊。



若攻擊者竊取合作夥伴的合法存取認證，則攻擊者可能會偽裝成合法使用者存取資料中心。然後，從網路「軟而耐嚼的內部」，攻擊者可以使用內部伺服器與端點在網路中橫向移動並危及到重要的系統。外部攻擊者入侵網路後，您會依賴網路及使用者分割以及網路內的分層防禦來保護資料，就像攻擊來自內部時一樣。

制定最佳做法安全性原則有助於保護資料中心免遭攻擊（無論其來源如何），並以分階段和優先順序的方式，首先保護最有價值的資產，然後逐步採取其他保護措施。從最理想的安全性原則逐步轉換到最佳做法安全性原則，可實際確保資料的機密性、組織的完整性以及資料中心的可用性。用於設計及實作資料中最佳做法安全性原則的下列建議，向您顯示如何透過對所有流量、所有時間進行分類來安全地啟用應用程式、使用者及內容，同時最大程度地減少對一般使用者的干擾。

資料中心最佳做法方法

以下最佳做法方法可確保在攻擊生命週期的多個階段進行偵測和防禦。

最佳做法方法	這為何如此重要？
檢查所有流量獲得全面的可視性	查看網路流量讓您能夠確定攻擊者的存在情況。檢查流量以查看流入、通過及流出資料中心的使用者、應用程式和內容。 ❑ 在可以檢查所有網路流量的位置部署下一代防火牆。在未部署防火牆檢查流量的情況下，不要允許流量流入資料中心或在網路段之間流動。 ❑ 除非法規或合規性規則要求您排除諸如健康、財務、政府或軍事等類別的流量，否則在所有進入或流出資料中心的流量上啟用 SSL 解密。您必須要看到威脅才能保護網路免受威脅攻擊。由於超過 50% 的典型網路流量都經過加密，而且這一比例還在上升，如果不解密流量，您便無法全面保護網路。 ❑ 使用 App-ID 識別應用程式，並為專有應用程式建立自訂應用程式，以便防火牆能夠正確識別這些應用程式並對其分類，及套用正確的安全性原則規則。這對於舊版應用程式尤其重要，因為它們經常被分類為「web-browsing」或「unknown-tcp」，而未正確分類。 如果您有單獨用於定義一組連接埠的自訂工作階段逾時而建立的現有「應用程式定覆寫」政策，請透過設定基於服務的工作階段逾時，將現有的「應用程式覆寫」政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時，然後將規則移轉為基於應用程式的規則。「應用程式覆寫」政策以連接埠為基礎。當您使用「應用程式覆寫」政策維持一組連接埠的自訂工作階段逾時時，您會失去對那些流動的應用程式可見度，因此您不知道也無法控制由哪些應用程式使用連接埠。基於服務的工作階段逾時達到自訂逾時，同時又能維持應用程式的可見度。 ❑ 在所有進入或流出資料中心的流量上啟用 User-ID，以將應用程式流量及其內容中的相關威脅對應至使用者和服務。您在網路段（區域）上啟用了 User-ID，因此必須分割網路才能啟用 User-ID。分割網路是取得可視性和縮小攻擊面的最佳做法。 ❑ 在內部模式下部署 GlobalProtect，將其作為控制存取資料中心的閘道。GlobalProtect 可以檢查使用者資訊以驗證使用者，及透過檢查主機資訊，並將主機資訊與您定義的 HIP 物件和設定檔進行比較，來確認主機安全性資訊是否為最新。這可確保連接至網路的主機維持您安全性等級標準。 ❑ 在所有安全性原則規則上啟用「在工作階段結束時記錄」。 流量可視性讓防火牆能夠使用其原生 App-ID、Content-ID 和 User-ID 技術將應用程式、威脅和內容與使用者綁定，而不受使用者位置或裝置類型、連接埠、加密或規避技術影響。
減少攻擊面	攻擊面指硬體和軟體進行網路互動的所有點，包括應用程式、內容、使用者，及伺服器、交換器、路由器和其他實體與虛擬設備。縮小攻擊面可以減少攻擊者攻擊的漏洞。攻擊面越小，入侵網路就越困難。 ❑ 評估您的資料中心，以便您瞭解網路上的應用程式、內容及使用者。 ❑ 使用積極的安全性強制措施，方法是建立基於應用程式的安全性原則規則，在網路和規則中僅允許具有合法商業用途的應用程式，以封鎖所有沒有合法使用案例的高風險應用程式。 ❑ 使用環境評估資訊建立一個策略，以根據業務需求、常用功能及全域原則需求將網路分割為不同區域，以便每個區域的資源具有相同的安全性等級需求。在資料中心內，將諸如資料庫、Web 伺服器、應用程式伺服器、開發伺服器和生產伺服器的應用程式層分割到不同區域。網路分割讓您能夠查看不同應用程式層之間的流量，因為流量在各區域之間流動時，必須通過防火牆。

最佳做法方法	這為何如此重要？
	精細分割讓您能夠建立關注每個區域業務需求，並為每個區段提供適當保護的安全性原則規則。分割還有助於阻止惡意軟體在資料中心之間及內部的橫向移動，因為將 App-ID、Content-ID（威脅防禦）與 User-ID 相結合，您可識別應該允許存取的流量並拒絕其他流量。 ❑ 在內部模式下部署 GlobalProtect，將其作為控制存取資料中心的閘道。 ❑ 若要進一步縮小攻擊面，在允許應用程式流量的安全性原則規則上，套用檔案封鎖設定檔以封鎖惡意和高風險的檔案類型。透過使用防火牆的驗證原則啟用多重要素驗證，防止認證被竊取，這樣即使攻擊者成功竊取認證，也無法成功存取資料中心網路。
預防已知威脅	附加至安全性政策原則的安全性設定檔允許規則掃描已知威脅（例如病毒、間諜軟體、應用層漏洞利用、惡意檔案等）的流量。防火牆會根據安全性設定檔設定對這些威脅套用一個動作，如允許、警告、丟棄、封鎖 IP 或連線重設。 遵循內容更新最佳做法並在下載內容更新後儘快安裝，以更新安全性設定檔並套用最新的保護措施至資料中心。安全性設定檔是基本的保護措施，極易套用至安全性原則規則。 外部動態清單 (EDL) 還能防禦已知威脅。EDL 會將惡意和高風險 IP 位址、URL 或網域清單匯入至防火牆以防禦已知威脅。EDL 來自信任的第三方、在防火牆上預先定義的 EDL 及您建立的自訂 EDL。EDL 無需提交即可在防火牆上自動更新。 防禦已知威脅是啟用解密之所以如此重要的另一個原因。如果看不到威脅，您是否瞭解它並不重要，但因為看不到，因此您仍有可能受到它的侵害。
防禦未知威脅	您要如何偵測從來沒有人見過的威脅呢？答案是將所有未知檔案轉送至 WildFire 進行分析。 WildFire 能夠識別未知或目標式惡意軟體。防火牆第一次偵測到一個未知檔案時，會將該檔案轉送至其內部目的地及 WildFire 雲端進行分析。WildFire 將對檔案（或電子郵件中的連結）進行分析，並在短短五分鐘內將分析結論傳回防火牆。WildFire 還包含標識檔案的簽章，將未知檔案轉換為已知檔案。如果檔案包含威脅，則該威脅現在變成了已知威脅。如果檔案可疑，則該檔案下次到達防火牆時，防火牆會將其封鎖。 您可在 WildFire 提交日誌（**Monitor**（監控）> **Logs**（日誌）> **WildFire Submissions**（**WildFire** 提交））中查看分析結論。設定 WildFire 設備內容更新以下載和每分鐘自動安裝，因此您一直能得到最新的支援。例如，Linux 和 SMB 檔案的支援在 WildFire 設備內容更新中第一次交付。

此外：

- 利用 Panorama 集中管理防火牆，以在各種實體和虛擬環境下一致地執行原則並提供集中的可視性。
- 使用積極的安全性強制措施允許您希望在資料中心網路上使用的流量，並拒絕其他流量。
- 建立您可在資料中心之間一致地複製和套用的標準化、可調式設計。
- 獲得管理人員、IT 和資料中心管理員、使用者及其他受影響方的支援。

透過關注對您的特定業務和網路最有可能的威脅，逐漸實施下一代安全防護，然後確定最重要的資產並首先為其提供保護。提出以下問題以幫助確定需要優先保護的資產：

1. 是什麼造就了我們公司？哪些屬性定義了您的公司並讓您的公司與眾不同，哪些資產與這些屬性相對應？與公司的專有競爭優勢相關的資產應當優先予以保護。例如，軟體開發公司會優先保護其源代碼發，製藥公司會優先保護其藥劑配方。
2. 什麼讓企業保持正常運營？您需要哪些系統和應用程式來支援公司的日常運營？例如，您的啟動目錄 (AD) 服務可為員工提供存取應用程式和工作站的權限。入侵您的 AD 服務讓攻擊者可以存取您企業內的所有帳戶，從而使攻擊者能夠完全存取您的網路。其他範例包括關鍵 IT 基礎結構，例如管理工具和驗證伺服器，以及儲存最重要的業務運營資料的伺服器。

3. 如果失去了此資產，會怎麼樣？失去一項資產的後果越嚴重，這項資產就越需要優先保護。例如，卓越的使用者體驗可以讓服務公司在競爭中脫穎而出，因此保護使用者體驗至關重要。專有工藝和設備可以讓製造公司與眾不同，因此保護智慧財產和專有設計是重中之重。建立優先次序清單以定義要優先保護的對像。

定義資料中心的理想未來狀態並逐步努力實現。定期重新審視您的定義以將業務、新的法律法規要求及新的安全性需求的變化納入考慮之中。

為何部署資料中心最佳做法安全性原則？

實作資料中心最佳做法安全性原則的工作流程是，瞭解資料中心網路、資料中心的資產及防火牆的威脅防禦能力，然後根據該資訊建立初始安全性原則規則，從而先保護最有價值的資產。

- 如何評估資料中心—確定要保護的資產、這些資產面臨的最大威脅以及允許進行存取的應用程式與使用者，並對其設定優先順序。
- 如何解密資料中心流量—無法保護網路免受看不見的威脅。加密流量是攻擊者帶來威脅的普通方法。
- 建立資料中心分割策略—分割資料中心可防止在資料中心獲得立足點的攻擊者橫向移動至其他區域。
- 如何建立資料中心最佳做法安全性設定檔—合法應用程式可以遞送命令與控制惡意軟體、通用漏洞暨披露 (CVE)、惡意內容偷渡式下載、網路釣魚攻擊以及 APT。最佳做法安全性設定檔保護所有四個資料中心流量中的允許流量不受已知與不明威脅的侵擾。
- 使用 Cortex XDR 代理程式保護資料中心端點—防火牆抵禦周遊網路的威脅。但在端點上執行的威脅沒有穿過網路，因此其並未周遊防火牆。在每個端點上安裝 Cortex XDR 代理程式，防止端點本身受到威脅。
- 建立資料中心流量封鎖規則—封鎖資料中心內的已知惡意 IP 位址、攻擊者常入侵的應用程式、設計用於規避或繞過安全性的應用程式，以及非業務目的所需的應用程式。
- 定義初始使用者至資料中心的流量安全性原則—未獲授權的存取會對資料中心內有價值的資訊構成巨大風險。由於內部企業網路上的員工和其他使用者經常受到信任，因此可能會鬆懈安全性預防措施。使用者群體與資料中心甚至可位於一個平面網路上。嚴格控制可存取資料中心的人員、不同使用者群組可以存取的資產，以及不同使用者群組對應用程式所具有的存取層次。
- 定義初始網際網路至資料中心的流量安全性原則—保護資料中心伺服器免受惡意網際網路流量攻擊。利用伺服器端漏洞會使資料中心受到攻擊，並使合作夥伴面臨風險，因為遭入侵的資料中心伺服器可能會向協力廠商用戶端提供漏洞利用。
- 定義初始資料中心至網際網路的流量安全性原則—命令與控制惡意軟體隱藏於已連接網際網路的受感染伺服器上，並可使用合法應用程式下載更多的惡意軟體。防止應用程式使用非標準連接埠，僅允許傳輸每個應用程式應合法使用的檔案類型，並封鎖惡意軟體、網路釣魚、Proxy 匿名者、對等的 URL 類別和其他潛在惡意的 URL 類別。
- 定義初始資料中心內的流量安全性原則（東西向流量）—通常忽視來自資料中心內部的威脅，因為沒有使用者流量來自此處，而且資料中心內部被認為值得信任。然而，若攻擊者入侵資料中心伺服器，則伺服器與 VM 之間的通訊可能會傳播惡意軟體。最佳做法安全性原則可防止攻擊者在資料中心中橫向移動，還可防止危及更多系統或洩漏資料。
- 記錄並監控資料中心流量—記錄並監控允許及封鎖的流量，可在轉換到資料中心最佳做法安全性原則以及對其加以維護的所有階段中提供資訊。它可以顯示網路上的應用程式、使用者及流量模式，包括您可能不知道的應用程式、使用者及流量模式。此資訊有助於您調查潛在的安全性問題。
- 維護資料中心最佳做法規則庫—持續監控應用程式允許清單，以便您可以調整規則以適應新認可的應用程式，並確定新的或已修改的 App-ID 如何影響您的政策。

對資料中心安全性原則規則庫進行排序彙總了安全性原則規則庫。

如何存取您的資料中心

為了實現零信任安全性模型，您必須瞭解資料中心內的資產並對其進行評估，以便您可以對先要保護最有價值的資產設定優先順序，確定誰應該有權存取這些資產，並瞭解這些資產面臨的主要風險。瞭解存取資產的使用者、允許的應用程式以及網路本身，可讓您對所需及所信任的內容進行評估，進而建立資料中心最佳做法安全性原則，以僅允許使用者存取與網路上具有合法業務目的的應用程式。

1. 對資料中心環境進行資產管理—對實體與虛擬資料中心環境進行資產管理，包括伺服器、路由器、交換器、安全性裝置以及其他網路基礎結構，並對資料中心應用程式（包括內部開發的自訂應用程式）與服務帳戶進行資產管理。

   - 根據每個系統在網路中的角色及其對業務的重要性評估每個系統，以對先要保護的實體及虛擬基礎結構部分設定優先順序。例如，如果您的業務涉及信用卡交易，則處理信用卡交易的伺服器與隨附有信用卡資訊之流量的通訊路徑均為極其寶貴的資產，應對其保護設定優先順序。
   - 檢查至少 90 天的流量日誌，以對資料中心網路上的應用程式進行資產管理。根據資料中心的應用程式資料庫建立自訂報告，幫助識別現有的資料中心應用程式。使用資料中心應用程式詳細目錄制定您希望在資料中心網路上認可或容忍的允許應用程式清單，包括內部開發的自訂應用程式。

     透過監控為資料中心最佳做法安全性規則庫設定的封鎖規則，您會發現尚未識別的應用程式，因此初始應用程式詳細目錄並不需要識別每個應用程式。著重於對您想要允許的應用程式及應用程式類型進行資產管理。在制定應用程式允許清單完成之後，會拒絕所有您未明確允許的應用程式。

     將應用程式對映於業務要求。若應用程式未對映於業務要求，請評估是否應在網路上允許該應用程式。不符合明顯業務需求的應用程式會增加受攻擊面，並且可能是攻擊者工具集的一部分。即使不需要的應用程式是無害的，也應將其移除，此為最佳做法，這樣攻擊者就少了一個可以利用的受攻擊面。若多個應用程式執行相同功能（例如，檔案共用或即時傳訊），請考慮將一個或兩個應用程式標準化以減少受攻擊面。

     若任何內部自訂應用程式不使用應用程式預設連接埠，請注意支援自訂應用程式所需的連接埠與服務。請考慮重新撰寫內部自訂應用程式，以使用應用程式預設連接埠。

     為需要在網路上進行類似處理的應用程式建立群組，以便有效地將安全性原則套用至應用程式群組，而不是個別應用程式。應用程式群組可以更輕鬆地設計及實作安全性原則，因為您可以同時將原則套用於群組內的所有應用程式，變更整個群組的原則，新增應用程式至群組以將群組的原則套用於新應用程式，以及重複使用多個安全性原則規則內的應用程式群組。例如，為資料中心儲存應用程式設計的應用程式群組可包含諸如 crashplan、ms-ds-smb 以及 NFS 之類的應用程式。
   - 對服務帳戶進行資產管理，應用程式可用這些帳戶在資料中心內的伺服器之間以及伺服器內進行通訊。最佳做法是為每個功能使用一個服務帳戶，而不是將一個服務帳戶用於多個功能。這將限制服務帳戶的存取權限，並更容易理解系統遭入侵時服務帳戶的使用方式。另一個最佳做法是識別已硬編碼至應用程式的服務帳戶，使您可以針對這些帳戶撰寫 IPS 特徵碼，並監控帳戶的使用情況。
2. 描繪資料中心流量特徵—描繪資料中心流量特徵並對資料中心流量進行繪製，瞭解資料如何在整個網路中以及使用者與資源之間流動。加入的跨職能團隊成員包括應用程式架構設計師、網路架構設計師、企業架構設計師與業務代表。描繪流量特徵可告知您網路流量來源與目的地、一般流量模式與負載，並助您瞭解網路上的流量以及為要保護之最重要的流量設定優先順序。使用應用程式控管中心 Widget、Panorama 的防火牆健康監控功能以及其他方法來瞭解正常（基準線）流量模式，有助於您瞭解可能指示攻擊的異常流量模式。
3. 評估資料中心分割—分割資料中心伺服器層，使不同伺服器層之間的通訊必須通過新世代防火牆，以根據最佳做法安全性原則進行解密、檢查並受到保護，還可使使用者群體或網際網路的通訊通過新世代防火牆。在資料中心外部，瞭解哪些區域可以與每個資料中心區域進行通訊，然後判定應允許哪些區域與每個資料中心區域進行通訊。
4. 評估使用者群體分割並判定哪些人員應有權存取資料中心—將使用者對映於群組以對使用者群體進行分割，使您可以更輕鬆地控制對敏感系統的存取。例如，「產品管理」群組內的使用者不應存取財務或人力資源系統。在 Active Directory（或您使用的任何系統）中，根據使用者出於合法業務目的所需的存取

層次建立細化的使用者群組，方便您控制對系統與應用程式的存取。這包括不同的員工群組以及不同的承包商、合作夥伴、客戶與供應商群組，其皆按所需的存取層次進行分組。

透過根據存取要求而不只是功能建立使用者群組來減少受攻擊面，並且僅向每個群組授與適當層次的應用程式存取權限。在「行銷」或「承包商」等職能領域內，建立對映至應用程式存取要求的多個使用者群組。

5. 持續監控資料中心網路—記錄並監控資料中心流量，可揭示資料中心最佳做法安全性原則中存在的漏洞，暴露可能指示攻擊的異常流量模式或非預期存取嘗試，以及診斷應用程式問題。

評估資產的實用方法便是對資產進行分組。確定最有價值的資產，首先對其提供保護，然後確定在保護這些資產後可以疊代的資產。為每個類別中的資產設定保護優先順序。以最適合特定業務的方式組織資產。下表顯示了一些可能性，但並不全面。為需要優先保護的資產設定優先順序時，還需考慮法律符合性要求，以保護諸如密碼、個人資訊以及財務資訊之類的資料。

表 **1:** 資產類別示例

最有價值的資產	其他有價值的資產	剩餘資產（疊代）
• 專利 • 原始碼 • 機密資料（如產品設計、藥物配方或使用者資料）。 • 專有演算法 • 程式碼簽署憑證與 PKI（這些均為加密項目的金鑰） • AD 網域伺服器（AD 遺失可讓攻擊者建立認證，進而無限制地存取網路） • 其他極為珍貴的資產，可區分貴企業與其他企業	• 重要的 IT 基礎結構（如路由器與防火牆介面） • 驗證服務 • 電郵 • VPN，尤其適用於高度分散的企業 • 重要的業務應用程式 • 檔案共用伺服器 • 資料庫	• 網路實驗室設備 • IT 管理系統 • 其他資產

每個企業都有獨一無二的資產優先順序。對於服務公司而言，使用者體驗便可區分該企業與其他企業，因此最有價值的資產可能是能確保最佳使用者體驗的資產。對於製造公司而言，最有價值的資產可能是專有流程和設備設計。考慮資產遺失的後果可以很好地確定首先要保護的資產。

如何部署資料中心流量

您無法保護您的網路遠離看不見的威脅，並進行檢查。解密流量來暴露惡意軟體至關重要，因為大部分一般網路流量已加密，而且數量還在上升。較大百分比的惡意軟體活動會隱藏網路入侵、安裝命令和控制惡意軟體，以及洩漏資料使用加密。

若要公開加密的應用程式與威脅，請妥善放置實體或虛擬新世代防火牆，確保它們可以看到所有資料中心流量。盡可能解密所有流量，尤其是高風險流量類別、預期送達重要伺服器的流量和業務重要流量。解密流量會識別該流量，使防火牆可以適當地套用防毒、漏洞保護、WildFire 和其他威脅保護。

若要將解密套用至流量，請建立解密設定檔，以指定如何處理 TLS 與 SSH 流量以及您選擇不解密或無法解密的流量。解密設定檔會為流量設定允許的通訊協定、演算法、模式和工作階段特性。您可以將解密設定檔套用於解密原則規則，用於指定防火牆套用解密設定檔的流量。

防火牆支援兩種類型的 SSL/TLS 解密以及 SSH 解密：

- SSL 正向 Proxy（輸出流量）
- SSL 輸入檢查（輸入流量）
- SSH Proxy（通常可供管理網路裝置的管理員進行安全存取）

在資料中心內，盡可能解密東西向流量。如果由於不正確的防火牆大小而導致的效能考慮因素阻止您解密所有流量，請為最重要的伺服器、風險最高的流量類別以及不太信任的區段及 IP 子網路設定優先順序，並在保持可接受效能的同時解密盡可能多的流量。要問的關鍵問題是：「如果此伺服器遭到入侵該怎麼辦？」、「每個流量類別代表的風險程度如何？」「對於我想在資料中心內達到的效能層級，我願意承擔多大的風險？」

對於從資料中心流向網際網路的流量，解密必須為其建立例外項的流量之外的所有內容。解密所提供的可見性尤為重要，因為您不希望資料中心內的伺服器連線至惡意網站、傳輸惡意檔案或易受惡意軟體下載的攻擊。

當您規劃解密原則時，請考慮貴公司的安全性符合性規則及定位。對於從使用者至資料中心的流量，儘管嚴格的解密原則最初可能會引起一些投訴，但這些投訴可能會讓您注意到那些非認可或不適當的網站，這些網站因使用弱演算法或存在憑證問題而被封鎖。將投訴用作一種工具，可以更好地瞭解網路上的流量。

此外，在解密政策中啟用解密記錄，並在資源允許時，同時記錄成功和不成功的 SSL 交握。利用所有解密監控和疑難排解工具，以檢查部署與調整政策和設定檔。

解密流量會耗用防火牆資源。每個資料中心需解密的流量每各不相同。若在支援解密的同時調整防火牆部署的大小以保持可接受的效能，請考慮預期解密的流量（某些應用程式必須解密，而其他應用程式未加密且不需要解密）、解密密碼（更強、更複雜的密碼需要更多的處理能力來解密）、金鑰的大小（金鑰越大，耗用的解密資源越多）、金鑰交換的類型（例如，*RSA* 金鑰交換比 *PFS* 金鑰耗用更多的處理資源），以及防火牆的容量。與您的 *Palo Alto Networks* 銷售團隊與代表合作，為您的特定網路適當調整防火牆部署的大小，使您可以解密流量並暴露威脅。

擁有銀行業等業務的公司，為確保其私密金鑰具有極為強大的安全性，可使用協力廠商硬體安全性模組 (HSM) 來保護並管理公司的私密金鑰，而不是將其儲存在防火牆上。

- 建立資料中心最佳做法解密設定檔
- 從資料中心解密中排除不合適的流量

建立資料中心最佳做法解密設定檔

解密設定檔可指定防火牆檢查解密流量及您無法解密或選擇不解密之流量的方式。防火牆檢查協定、伺服器憑證、工作階段特徵及密碼（金鑰交換演算法、加密演算法和驗證演算法）。您可以將解密設定檔（**Objects**（物件）> **Decryption Profile**（解密設定檔））套用至解密政策規則（**Policies**（政策）>

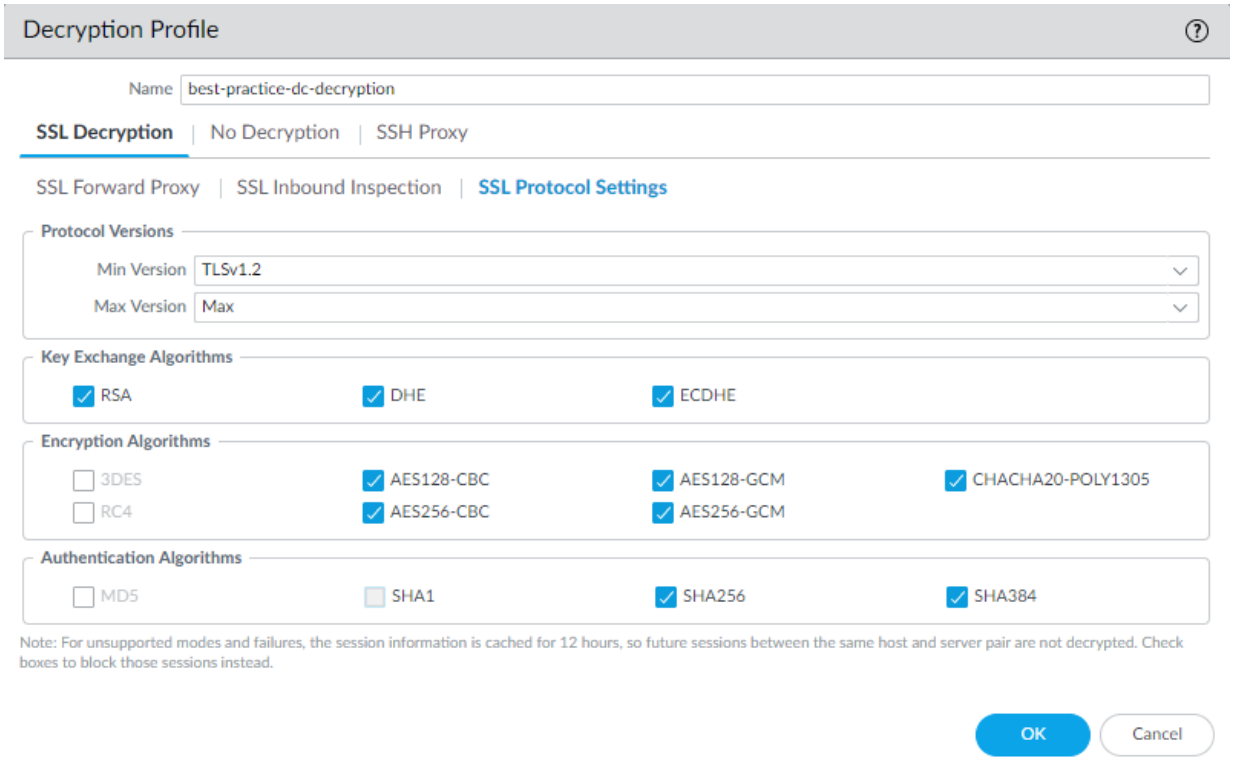
Decryption（解密））。解密原則規則使用來源、目的地、服務類別及 URL 類別作為比對準則，定義要檢查的流量，以便您對套用解密設定檔的流量進行精確的控制。您也可以在政策規則中設定解密記錄和日誌轉送。

若要解密輸出流量，防火牆將充當內部用戶端與外部伺服器之間的正向 Proxy 裝置。為檢查輸入流量，防火牆將複製傳入工作階段流量並對其進行解密和檢查。

STEP 1 | 設定防火牆以執行 CRL/OCSP 檢查，確保解密期間提供的憑證有效。

STEP 2 | 設定 **SSL Decryption**（**SSL** 解密）> **SSL Protocol Settings**（**SSL** 通訊協定設定）以封鎖易受攻擊的 SSL/TLS 版本，如 TLSv1.0、TLSv1.1 和 SSLv3，並避免使用弱加密演算法（如 RC4 和 3DES）和弱驗證演算法（如 MD5 和 SHA1）。

SSL 協定設定適用於所有解密流量。



將通訊協定 **Min Version**（最低版本）設定為 **TLSv1.2**，並將 **Max Version**（最高版本）設定為 **Max**（最高），以封鎖弱通訊協定。使用您可以使用的最強 TLS 通訊協定。建立單獨解密政策和設定檔，以將安全性最大化。例如，如果您因業務目的而需要的傳統網站僅支援較弱的通訊協定，則請建立允許較弱通訊協定的單獨解密設定檔，並僅在解密政策中將它套用至不支援至少 TLSv1.2 的網站。這也套用至不支援強演算法的必要業務網站和不同的 URL 類別，以對安全性和效能進行微調。

如果網站不包含合法的業務應用程式，則請不要降低安全性等級來支援網站—弱通訊協定（和密碼）包含攻擊者可以利用的已知漏洞。如果網站屬於出於業務目的而不需要的某類網站，請使用 URL 篩選來封

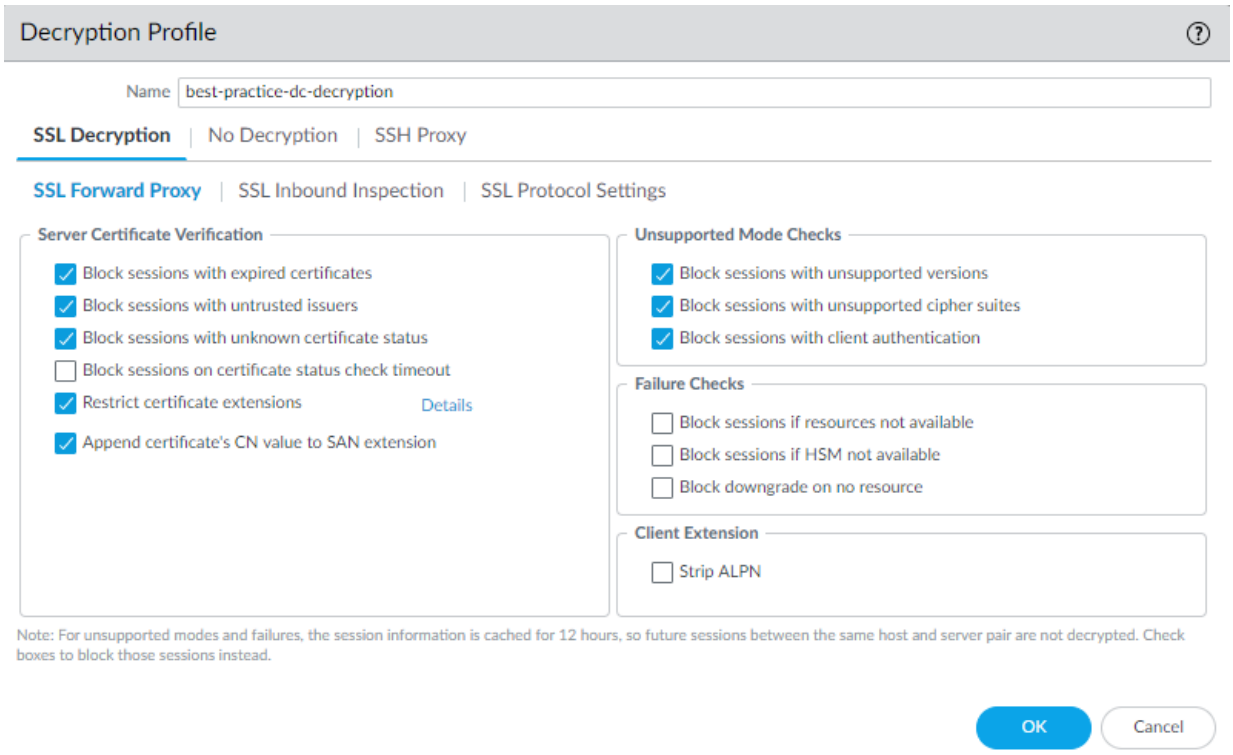
鎖對整個類別的存取權限。除非必須如此才能支援重要的舊版網站，否則請不要支援弱通訊協定或是弱加密或驗證演算法。

將 **Max Version**（最高版本）設定為 **Max**（最高）而不是特定版本，以便通訊協定可以改進，防火牆自動支援最新與最佳的通訊協定。無論您打算將解密設定檔附加到管理輸入（SSL 輸入檢查）還是輸出（SSL 轉送 Proxy）流量的解密原則規則，都要避免允許採用弱演算法。

許多行動應用程式都使用固定的憑證。因為 *TLSv1.3* 會加密憑證資訊，所以防火牆無法將這些行動應用程式自動新增至 *SSL* 解密排除清單。對於這些應用程式，確定解密設定檔 *Max Version*（最高版本）設定為 *TLSv1.2*，或將不解密政策套用至流量。

STEP 3 | 設定輸出流量的 **SSL Decryption**（**SSL** 解密）> **SSL Forward Proxy**（**SSL** 正向 **Proxy**）設定以封鎖 TLS 交涉期間的例外狀況並封鎖無法解密的工作階段。

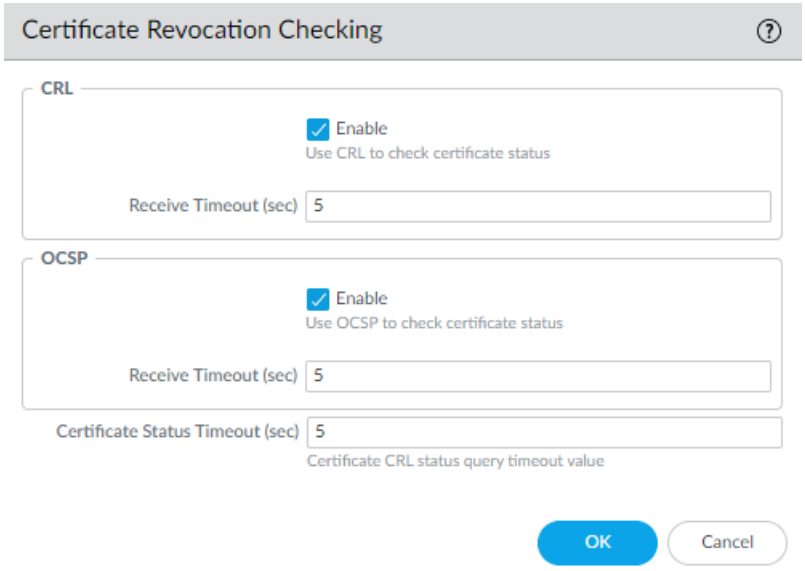
在某些情況下，最佳做法設定取決於公司的安全性合規性規則。將 SSL 轉送 Proxy 解密設定檔套用至控制輸出流量的安全性原則規則。



封鎖 TLS 交涉期間的例外狀況，並封鎖無法解密的工作階段。

- 伺服器憑證驗證—是否勾選封鎖憑證狀態檢查逾時的工作階段方塊取決於您公司的安全性合規性立場，因為這需要在更高的安全性和更好的用戶體驗之間進行權衡。憑證狀態驗證檢查撤銷伺服器上的憑證撤銷清單 (CRL)，或使用線上憑證狀態通訊協定 (OCSP) 以確定簽發的 CA 是否已撤銷憑證，並且該憑證不應受信任。然而，撤銷伺服器可能回應速度緩慢，導致工作階段逾時，以及防火牆即使在憑證可能有效的情況下也會封鎖工作階段。如果您 **Block sessions on certificate status check timeout**（封鎖憑證狀態檢查逾時的工作階段）且撤銷伺服器回應速度慢，您可使用 **Device**（裝置）

> **Setup**（設定）> **Session**（工作階段）> **Decryption Settings**（解密設定），並按一下 **Certificate Revocation Checking**（憑證撤銷檢查）以將預設逾時值由五秒變更為其他值。



由於伺服器憑證可能包含 CRL 分佈點 (CDP) 延伸內的 CRL URL 或授權資訊存取 (AIA) 憑證延伸內的 OCSP URL，同時啟用 CRL 和 OCSP 憑證撤銷檢查。

雖然最佳做法是使用適當的憑證，但部分憑證會將主體別名（Subject Alternate Name，SAN）欄位留空，從而導致防火牆拒絕這些憑證。如果 SAN 欄位為空，則勾選將憑證的 **CN** 值附加到 **SAN** 擴充功能以自動複製憑證編號到 SAN 欄位，以便您在與未填寫憑證 SAN 欄位的網站進行交易時，可以接受其憑證。否則，這些網站需要重新產生憑證才符合適當的做法並填寫 SAN 欄位。

封鎖所有其他伺服器憑證驗證例外狀況。

- 不支援模式檢查—如果您不封鎖採用不支援版本和不支援密碼套件的工作階段，則使用者會收到一則表示其按一下就會進入高風險網站的警告訊息。您設定嚴格 SSL 協定設定的原因是，封鎖使用這些弱（高風險）協定版本和演算法的伺服器，保護您免受其攻擊。此外，使用不支援模式檢查功能封鎖工作階段可以保護您免受惡意後門及其他使用自訂和非標準加密來使其活動具有迷惑性的威脅的攻擊。

  封鎖使用用戶端驗證的工作階段可讓您選擇允許還是封鎖使用用戶端驗證的工作階段。雖然伺服器驗證可以用於建立工作階段的唯一驗證方法，但一些網站使用相互驗證，即同時使用伺服器和用戶端驗證來建立工作階段。使用 X.509 數位憑證的用戶端驗證與伺服器驗證類似，因為這兩種驗證方法均使用由信任的憑證授權單位簽發的數位憑證來驗證工作階段。用戶端憑證充當用戶端的數位識別碼，位於用戶端裝置上，不能移植到其他裝置。但是，用戶端驗證會防止防火牆解密工作階段，因為防火牆需要用戶端和伺服器憑證才能執行雙向解密，但防火牆只知道伺服器憑證。防火牆會中斷用戶端驗證工作階段的解密。

  如果您未啟用封鎖用戶端驗證的工作階段，則在防火牆試圖解密使用用戶端驗證的工作階段時，防火牆會容許該工作階段，並新增一個項目至其本機解密排除快取（包含伺服器 URL/IP 位址、應用程式以及解密設定檔）。項目在快取中保留 12 小時，然後過時。若同一使用者或其他使用者嘗試使用用戶端驗證在 12 小時內存取伺服器，則防火牆會將工作階段與解密排除快取項目比對，但不會嘗試解密流量，並允許加密工作階段。

  若排除快取已滿，則防火牆會在新項目抵達時清除最舊的項目。若變更解密原則或設定檔，則防火牆會清除排除快取，因為變更原則或設定檔可能會變更工作階段的分類結果。

  如果您啟用封鎖使用用戶端驗證的工作階段，則防火牆會封鎖使用用戶端驗證的工作階段，但 SSL 解密排除清單（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（**SSL** 解密排除））上網站中的工作階段除外。

除了 SSL 解密排除項清單中預先定義的網站之外，您可能還需要允許來自使用用戶端驗證的其他網站的網路流量。建立的解密設定檔容許用戶端驗證的工作階段。將其新增到僅適用於包含該應用程式之伺服器的解密原則規則。為了進一步增強安全性，您可以要求多因素驗證來完成使用者登入過程。

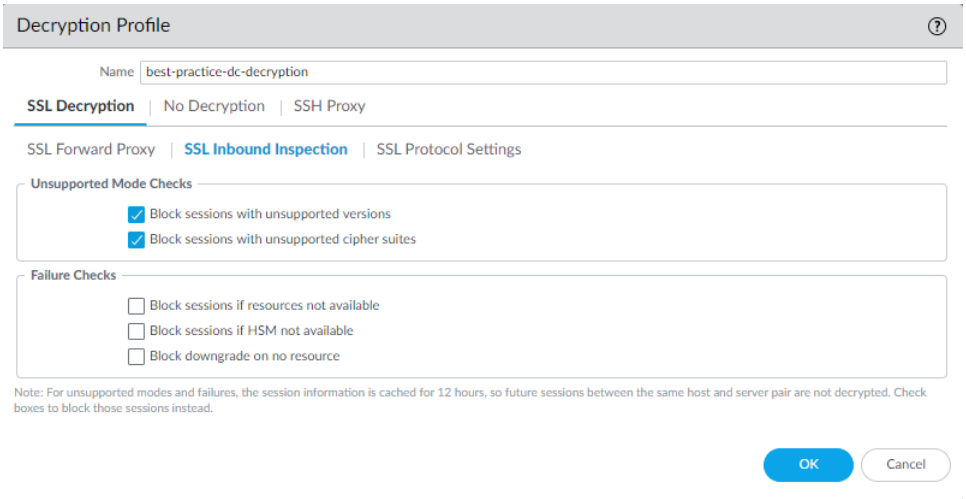
對於所有其他流量，則可套用封鎖使用用戶端驗證的工作階段之解密設定檔。

- 故障檢查—如果您沒有 **Block sessions if resources not available**（封鎖資源不可用的工作階段），存在的風險是，處理資源不足可能會允許建立具有潛在危險的連線。如果您封鎖了資源不可用的工作階段，則可能影響使用者體驗。是否實作失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗對您的業務的重要性（與更嚴格的安全性權衡利弊）。

  如果您使用硬體安全模組 (HSM) 儲存私人金鑰，則是否勾選 **Block sessions if HSM not available**（**HSM** 不可用時封鎖工作階段）取決於當 HSM 不可用時，關於私人金鑰來源及您希望如何處理加密流量的合規性規則。例如，如果貴公司強制使用 HSM 進行私密金鑰簽署，則會在 HSM 不可用時封鎖工作階段。然而，如果貴公司對此並不嚴格，則在 HSM 不可用時可以考慮不封鎖工作階段。（如果 HSM 關閉，則防火牆可以針對其已快取來自 HSM 之回應的網站處理解密，但不會處理其他網站的解密。）這種情況下的最佳做法取決於貴公司的原則。如果 HSM 對您的業務至關重要，則可在高可用性 (HA) 配對中執行 HSM（PAN-OS 8.0 支援 HSM HA 配對中的兩個成員）。
- 無資源時封鎖降級—防止當防火牆沒有可用的 TLSv1.3 處理資源時從 TLSv1.3 降級到 TLSv1.2。如果封鎖降級，則當防火牆用盡 TLSv1.3 資源時，即會丟棄使用 TLSv1.3 的流量，而不是將其降級至 TLSv1.2。如果不封鎖降級，則當防火牆用盡 TLSv1.3 資源時，即會降級至 TLSv1.2。但是，若在防火牆處理資源不可用時封鎖降級，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於公司的安全性合規性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。對於不想要降級 TLS 版本的敏感流量，您可能想要建立單獨的解密原則和設定檔來控管其解密。

STEP 4 | 設定 **SSL Decryption**（**SSL** 解密）> **SSL Inbound Inspection**（**SSL** 輸入檢查）設定以檢查從外部用戶端到內部伺服器的流量並封鎖可疑工作階段。

將 SSL 輸入檢查解密設定檔套用至控制輸入流量的安全性原則規則。



- 不支援模式檢查—防火牆無法解密防火牆不支援的工作階段版本和密碼。若要防止攻擊者使用不支援的版本和密碼潛入網路，可以封鎖防火牆不支援的工作階段版本和密碼套件。此外，使用不支援模式檢查功能封鎖工作階段可以保護您免受惡意後門及其他使用自訂和非標準加密來使其活動具有迷惑性的威脅的攻擊。

  在伺服器上，僅啟用防火牆支援的密碼。確保這一相容性可以使用戶端和伺服器之間的交涉更加順利。
- 故障檢查—如果您沒有 **Block sessions if resources not available**（封鎖資源不可用的工作階段），存在的風險是，處理資源不足可能會允許建立具有潛在危險的連線。如果您封鎖了資源不可用的工作階

段，則可能影響使用者體驗。是否實作失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗對您的業務的重要性（與更嚴格的安全性權衡利弊）。

如果您使用硬體安全模組 (HSM) 儲存私人金鑰，則是否勾選 **Block sessions if HSM not available**（**HSM** 不可用時封鎖工作階段）取決於當 HSM 不可用時，關於私人金鑰來源及您希望如何處理加密流量的合規性規則。例如，如果貴公司強制使用 HSM 進行私密金鑰簽署，則會在 HSM 不可用時封鎖工作階段。然而，如果貴公司對此並不嚴格，則在 HSM 不可用時可以考慮不封鎖工作階段。（如果 HSM 關閉，則防火牆可以針對其已快取來自 HSM 之回應的網站處理解密，但不會處理其他網站的解密。）這種情況下的最佳做法取決於貴公司的原則。如果 HSM 對您的業務至關重要，則可在高可用性 (HA) 配對中執行 HSM（PAN-OS 8.0 支援 HSM HA 配對中的兩個成員）。

- 無資源時封鎖降級—防止當防火牆沒有可用的 TLSv1.3 處理資源時從 TLSv1.3 降級到 TLSv1.2。如果封鎖降級，則當防火牆用盡 TLSv1.3 資源時，即會丟棄使用 TLSv1.3 的流量，而不是將其降級至 TLSv1.2。如果不封鎖降級，則當防火牆用盡 TLSv1.3 資源時，即會降級至 TLSv1.2。但是，若在防火牆處理資源不可用時封鎖降級，則會讓使用者無法存取通常可臨時存取的網站，從而影響使用者體驗。是否實作此失敗檢查取決於公司的安全性合規性立場，以及使用者體驗的重要性（與更嚴格的安全性權衡利弊）。對於不想要降級 TLS 版本的敏感流量，您可能想要建立單獨的解密原則和設定檔來控管其解密。

STEP 5 | 對於 SSH 流量，請設定 SSH Proxy 解密設定檔設定。

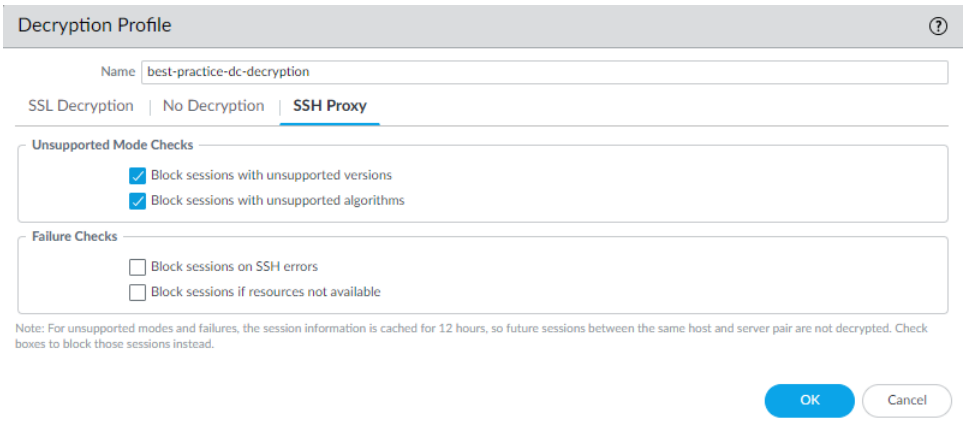
SSH 解密允許正常路由的 SSH 流量，拒絕 SSH 通道（SSH 連接埠轉送）流量，但不會在 SSH 流量上執行內容或威脅檢查。SSH 通道作業工作階段可發掘 X11 Windows 封包和 TCP 封包。一個 SSH 連線可能包含多個通道。當您將 SSH 解密設定檔套用至流量時，對於連線中的每個通道，防火牆都會檢查流量的 App-ID 並識別通道類型。通道類型可以是：

- 工作階段
- X11
- forwarded-tcpip
- direct-tcpip

當通道類型是工作階段時，防火牆會將流量識別為允許的 SSH 流量，如 SFTP 或 SCP。當通道類型是 X11、forwarded-tcpip 或 direct-tcpip 時，防火牆會將流量識別為 SSH 通道流量並將其封鎖。

對於大多數使用者群組，您可能不會在資料中心允許 SSH 流量。SSH 通常用於遠端存取伺服器，而您不會希望所有使用者都具有此能力，因為這使其能夠存取 Linux 伺服器並進行檔案傳輸，從而將您的資料中心伺服器置於較大的風險之中。您無法解密 SSH 流量，因此使用 SSH 存取資料中心資源的任何人都必須值得信任—即使如此，也應將所有威脅設定檔附加至允許進行 SSH 存取的任何規則，以掃描惡意軟體、病毒、間諜軟體等。

SSH 的一個範例使用案例是負責管理和維護資料中心伺服器的 IT 人員使用 SSH 進行遠端存取。



- 不支援模式檢查—防火牆無法解密防火牆不支援的工作階段版本和密碼，且不支援的版本和密碼可能易於受到攻擊。若要防止攻擊者使用不支援的版本和密碼潛入網路，可以封鎖防火牆不支援的工作階

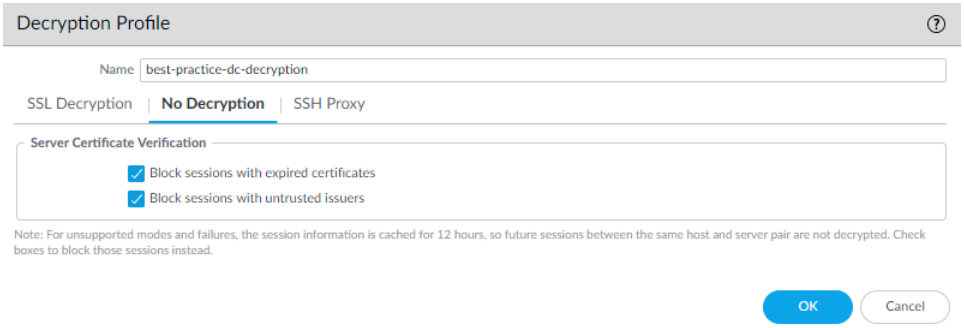
段版本和密碼套件。此外，使用不支援模式檢查功能封鎖工作階段可以保護您免受惡意後門及其他使用自訂和非標準加密來使其活動具有迷惑性的威脅的攻擊。

- 故障檢查—如果您沒有 **Block sessions if resources not available**（封鎖資源不可用的工作階段），存在的風險是，處理資源不足可能會允許建立具有潛在危險的連線。如果您封鎖了資源不可用的工作階段，則可能影響使用者體驗。是否實作失敗檢查取決於貴公司的安全性符合性立場，以及使用者體驗對您的業務的重要性（與更嚴格的安全性權衡利弊）。

STEP 6 | 對於您選擇不解密的流量，可設定 **No Decryption**（不解密）設定以封鎖目的地為憑證過期或簽發者不可信的網站的加密工作階段。

僅將不解密設定檔套用至為符合法規或合規性規則而選擇不解密的流量，而不是套用至因固定憑證這類技術問題而無法解密的流量（將該流量新增至 [SSL Decryption Exclusion List（SSL 解密排除清單）]）。最佳做法是儘量解密更多資料中心流量。

對於不解密的 *TLSv1.3* 流量，不要將不解密設定檔附加至解密原則。與以前的版本不同，*TLSv1.3* 會加密憑證資訊，防火牆無法查看憑證資料，因此無法封鎖具有過期憑證或不受信任簽發者的工作階段，這樣，設定檔便沒有效果（防火牆可以使用 *TLSv1.2* 及早前版本執行憑證檢查，因為這些通訊協定不會加密憑證資訊，您應將「不解密」設定檔套用至其流量）。 但是，您應為不解密的 *TLSv1.3* 流量建立解密原則，因為除非解密原則控制未解密的流量，否則防火牆不會記錄該流量。



從資料中心解密中排除不合適的流量

兩種類型的流量不適合解密：

- 因技術原因（如使用用戶端憑證驗證、固定憑證或不完整的憑證鏈）而中斷解密的流量。
- 選擇不解密的流量。

防火牆為因技術原因而中斷解密的常用網站提供預先定義的 SSL 解密排除項清單（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（SSL 解密排除項））。若要從清單中移除預先定義的網站，則可按一下網站主機名稱旁邊的核取方塊，然後按一下 **Disable**（停用），您還可以將網站新增至清單。僅對因技術原因而中斷解密的網站使用解密排除項清單，請勿對選擇不解密的網站使用該清單。如果解密中斷一個重要的應用程式，則將其新增至解密排除項清單，以便為與應用程式相關聯之憑證中的特定 IP 位址、網域或通用名稱建立一個例外。若進行解密，則某些內部自訂應用程式可能會中斷。

如果解密設定檔允許 **Unsupported Modes**（不受支援的模式）（具有用戶端驗證、不受支援版本或不受支援加密套件的工作階段），防火牆會自動將使用允許的受支援模式的伺服器和應用程式新增至其本機 SSL 解密排除快取（**Device**（裝置）> **Certificate Management**（憑證管理）> **SSL Decryption Exclusion**（SSL 解密排除）> **Show Local Exclusion Cache**（顯示本機排除快取））。當您封鎖不受支援的模式時，會增加安全性，但同時也封鎖與使用那些模式的應用程式進行通訊。

如果將網站排除在解密之外的技術原因是憑證鏈不完整，則您可以使用解密日誌中的資訊來修復不完整憑證鏈，讓您可以允許、解密和檢查流量。

出於諸如法規與法律符合性之類的原因，您可以選擇不解密流量。例如，歐盟 (EU) 一般資料保護法規 (GDPR) 將要求對所有個體的所有個人資料進行強有力的保護。GDPR 影響了所有收集或處理歐盟居民個人資料的公司（包括外國公司）。不同的法規和符合性規則可能意味著，您在不同的國家或地區對相同資料的處理方式會有所不同。由於企業擁有其公司資料中心中的個人資訊，企業通常可解密該資訊。最佳做法是盡可能多地解密流量，以便您可以瞭解流量並對其套用安全性保護。

對於您選擇不解密的流量，請確保它確實是您不想解密的流量，然後建立基於政策的排除項，以指定應用程式、使用者群組、來源與目的地、URL 類別及/或服務，以盡可能限制每個排除項。解密排除項越具體越好，這樣您就不會意外將應進行解密的流量排除在解密之外。

建立資料中心分割策略

扁平化、未分割的網路很難防禦，因為如果攻擊者獲得了網路的存取權，攻擊者便可橫向移動並破壞重要系統。在資料中心內部尤其如此，因為各公司在那裡保存其最有價值的資產。舊的分割方法，如 VLAN，不能很好地擴展，難以進行自動化，並且不會考慮使用者、內容或應用程式，因此幾乎無法控制或洞察流量。

建立一個分割策略，對資料中心資源進行更精細的存取控制，讓您更好地洞察流量。分割策略越精細，流量的可視性就越高，因為流量在區段之間流動時必須穿過防火牆（區段閘道）。分割還使合規性與合規性稽核變得更容易，因為除必要時外，您可防止對所有個人資訊的存取，從而保護資料並縮小稽核範圍。

您的資料中心分割策略取決於您的架構和業務目標，因此不存在「通用型」實作。但是，學習通用指南可讓您設計並實現分割策略以保護您的資料中心網路。

- 如何分割資料中心
- 如何分割資料中心應用程式

如何分割資料中心

如何分割資料中心取決於業務要求以及資料中心網路架構，包括可能指示分割方法的 SDN 解決方案。例如，vwire 介面控制 NSX 主機上的防火牆連線。vwire 介面不在 NSX 主機上遞送或切換流量，它們必須屬於同一個區域，因此特定租戶（部門、客戶或應用程式層）的所有資源都存留在一個區域中，防火牆會使用動態位址組來分割該區域內的應用程式流量。每個租戶都有一個具有自己的 vwire 介面的獨立區域。對於其他 SDN 解決方案，單獨的虛擬防火牆實例可能會分割流量。

Palo Alto Networks 的新世代防火牆提供了分割流量的靈活工具：

- 區域—穿過區域的流量會通過防火牆進行檢查。所有允許的資料中心通訊應該周遊防火牆，並進行完整的威脅檢查（對於離開企業的資料中心流量以及由客戶租戶管理的應用程式，則進行以下檢查：防毒軟體、反間諜軟體、漏洞保護、檔案封鎖、WildFire 分析以及 URL 篩選）。依預設，防火牆會拒絕區域之間的所有流量（區域間流量）。您必須撰寫特定的安全性原則規則，以允許流量在區域之間通過，因此只有明確允許的流量才能在兩個區域之間移動。如何使用區域來分割資料中心取決於您需要與其他資產區分的資產。例如，常見的架構包含用於開發伺服器與生產伺服器的單獨區域。您可以使用區域分割包含極為敏感的資訊（如付款卡資訊 (PCI) 或個人可識別資訊 (PII)）的伺服器，分割不同的公司內部部門（如行銷部門、工程部門及人力資源部門），以及分割客戶資源與客戶管理的應用程式。

  考慮使用區域保護設定檔，即可保護區域免受爆流、偵察活動（連接埠掃描與主機掃描）、第三層基於封包的攻擊以及非 IP 通訊協定 (第二層) 基於封包的攻擊。
- 動態位址群組—為此，動態位址群組為 IP 位址清單，防火牆會在安全性政策中匯入並使用該清單來動態而非靜態定義伺服器群組。在動態位址群組中新增與移除 IP 位址會自動更新安全性原則，而不需在防火牆上執行提交動作。在區域內，若於安全性政策允許規則中使用動態位址群組，則會在所指定應用程式和服務中啟用伺服器至伺服器互動。例如，在 NSX 中，使用動態位址群組來分割應用程式層內的伺服器層。
- User-ID—啟用 User-ID 即可根據使用者群組建立應用程式允許規則，以分割來自應用程式與伺服器群組的使用者。

設計資料中心分割計劃後，時刻謹記以下一般準則：

- 如何評估資料中心，可讓您在各個階段對其進行分割，並首先保護最有價值及敏感的資產。
- 在資料中心內使用 SDN 解決方案（比如 NSX、ACI、OpenStack），可提供一個可調式而又敏捷的虛擬化基礎結構。使用 SDN 可最佳地集中管理資料中心網路，最大限度地提高計算資源利用率，擴充與自動化網路以及控制和保護虛擬化網路的流量。儘管您可以建立一個基本上複製 SDN 架構的非 SDN 架構，但這種操作既困難又耗時，且容易出現導致中斷的錯誤，因此不將其視為最佳做法。SDN 解決方案可最大限度地利用基礎資料中心計算資源，而不會犧牲安全性。
- 使用實體新世代防火牆，可對非虛擬化舊式伺服器進行分割與保護，而使用 VM 系列防火牆，可對虛擬資料中心網路進行分割與保護。

- 對執行類似功能且在同一資料中心區段中需要相同層次的安全性的資產進行分組。例如，在同一區段中放置連接至網際網路的伺服器。

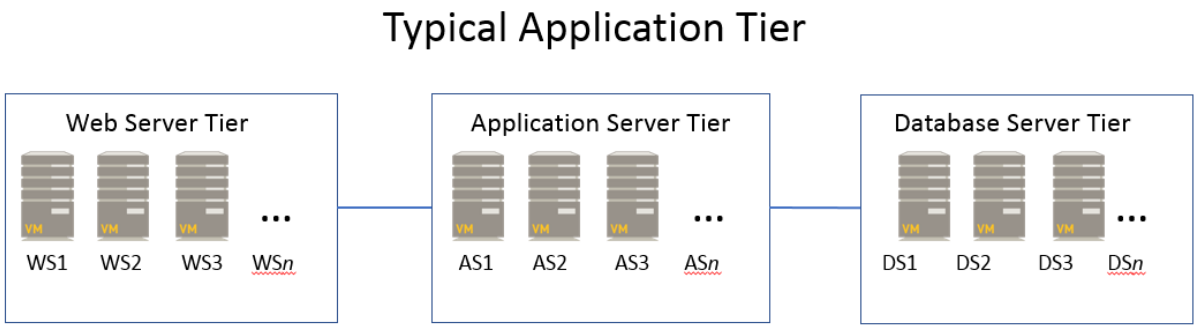
將根據多個準則確定分割計劃，以制定正確的計劃來保護業務。

如何分割資料中心應用程式

分割資料中心應用程式，可防止惡意軟體在應用程式之間移動，還可安全地為使用者啟用這些應用程式。應用程式層提供了資料中心應用程式所需的資源與功能。應用程式層包含了多個伺服器層，而這些伺服器層可共同完成與特定應用程式相關的要求和命令。通常，應用程式層包含三個伺服器層：

- *Web* 伺服器層—面向使用者的應用程式介面。
- 應用程式伺服器層—從 Web 伺服器層獲取要求以處理及產生應用程式功能。
- 資料庫伺服器層—包含應用程式運行所需的資料。

每個伺服器層包含可協同工作且功能相似的伺服器，以便應用程式層可以向使用者顯示應用程式。



每個應用程式層中的伺服器層建立 VM 的服務鏈。服務鏈透過虛擬資料中心設備引導流量以提供應用程式服務。在應用程式層內，Web 伺服器可與包含應用程式碼的應用程式伺服器通訊，並且該應用程式伺服器可與包含內容的資料庫伺服器通訊。三個伺服器位於應用程式層內不同的伺服器層中，其間的通訊為服務鏈。

資料中心包含許多應用程式層，其可專用於特定部門、客戶、承包商或其他群組。分割資料中心應用程式基礎結構，可防止應用程式資源中未獲授權與不必要的通訊，還可檢查應用程式流量。

應用程式分割	如何分割應用程式
應用程式層	若要分割每個應用程式層內的伺服器層，請為每個伺服器層設定單獨的防火牆區域，以便您可以控制每組伺服器的存取權限，並在每個伺服器層之間流動的流量周遊防火牆時檢查該流量。例如，將 Web 伺服器、應用程式伺服器及資料庫伺服器放在單獨的區域中，使伺服器層之間的流量一律通過新世代防火牆以進行完全檢查。 根據業務要求，您可能需要為每個應用程式層建立多個區域，以分隔租戶，載入平衡，將應用程式層用於不同用途，提供不同層次的安全性或連接至不同的伺服器組。若要分割資料中心以減少每個應用程式層的受攻擊面，則只需將需要類似層次的信任且需要與類似應用程式層進行通訊的伺服器分組到同一區域內。
Web 伺服器層	流量通常經由 Web 伺服器進入資料中心，但有一些特殊情況，例如 IT 設定資料中心伺服器的直接安全存取權限以用於管理用途。與其他伺服器層一樣，為 Web 伺服器層建立單獨的區域，使您可以對其套用精確的安全性原則。 由於 Web 伺服器層與資料中心之外的裝置通訊，對於攻擊者而言它是一個吸引力十足的目標。將 Web 伺服器層放置於單獨的網路中，例如，使用 VLAN。進出 VLAN 的所有流量 - 進出資料中心的所有流量 - 應該周遊新世代防火牆。若要完成此作業，則您可以將新世代防火牆設定為預設閘道，或使用 NSX 等 SDN 解決方案來引導流量。

應用程式分割	如何分割應用程式
	分割 Web 伺服器層中的伺服器，可防止其彼此通訊，例如，透過使用 *NSX* 分散式防火牆 *(DFW)* 等傳統規則來開啟連接埠或封鎖層內的流量。
基礎結構服務應用程式伺服器	分割用於提供重要的基礎結構服務（如 DNS、DHCP 與 NTP）的伺服器，並僅使用適當的應用程式僅允許存取其特定的 IP 位址。
應用程式	使用 App-ID 建立基於應用程式的允許清單安全性政策規則，用以透過控制可以存取每個應用程式的人員以及伺服器組（使用動態位址群組）來分割應用程式。App-ID 可讓您將精確安全性原則規則套用於應用程式，而這些應用程式可位於相同計算資源上，但需要不同層次的安全性與存取控制。 建立自訂應用程式以唯一識別專有應用程式與區段存取。如果您有單獨用於定義一組連接埠的自訂工作階段逾時而建立的現有「應用程式定覆寫」政策，請透過設定基於服務的工作階段逾時，將現有的「應用程式覆寫」政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時，然後將規則移轉為基於應用程式的規則。「應用程式覆寫」政策以連接埠為基礎。當您使用「應用程式覆寫」政策維持一組連接埠的自訂工作階段逾時時，您會失去對那些流動的應用程式可見度，因此您不知道也無法控制由哪些應用程式使用連接埠。基於服務的工作階段逾時達到自訂逾時，同時又能維持應用程式的可見度。 若要從具有自訂應用程式逾時之基於連接埠的安全性原則移轉到基於應用程式的原則，請勿使用應用程式覆寫規則來維持自訂逾時，因為您將無法看到應用程式。而是定義基於服務的工作階段逾時以維持每個應用程式的自訂逾時，然後將規則移轉到基於應用程式的規則。

請勿使用新世代防火牆來分割特定伺服器層內的伺服器：若您必須防止伺服器層內的伺服器進行相互通訊，請使用 NSX DFW 等傳統規則來開啟連接埠或封鎖層內的流量。然而，伺服器層內的伺服器通常需要相互通訊。例如，資料庫伺服器層可能是伺服器叢集，要求相互通訊自由。

如何建立資料中心最佳做法安全性設定檔

安全性設定檔透過對網路上允許的流量進行威脅檢查來提供基本保護。安全性設定檔提供了一套完整的協同威脅防禦工具，用以封鎖對等式命令與控制 (C2) 應用程式流量、危險的檔案類型、利用漏洞的嘗試以及防毒軟體特徵碼，還會識別新惡意軟體與不明惡意軟體。

由於 Palo Alto Networks 提供了您可以簡單地新增到安全性原則允許規則的預先定義設定檔，套用安全性設定檔所花費的精力相對較少。您可以複製預先定義設定檔然後加以編輯，因此自訂安全性設定檔過程很簡單。當然，您也可以在防火牆或 Panorama 上建立全新的安全性設定檔。

若要偵測網路流量中的已知與不明威脅，請將安全性設定檔附加到網路上允許之流量的所有安全性原則規則，以便防火牆可檢查所有允許的流量。防火牆對符合安全性原則允許規則的流量套用安全性設定檔，根據安全性設定檔設定掃描流量，然後採取適當動作來保護網路。除非另有說明，否則最佳做法安全性設定檔的建議會套用於所有四個資料中心流量。

自動下載內容更新，並盡快進行安裝，這樣您在防火牆上便擁有最新的威脅防禦特徵碼與內容（防毒軟體、反間諜軟體、漏洞、惡意軟體等）並封鎖最新的威脅。

- 建立資料中心最佳做法防毒設定檔
- 建立資料中心最佳做法反間諜軟體設定檔
- 建立資料中心最佳做法漏洞保護設定檔
- 建立資料中心最佳做法檔案封鎖設定檔
- 建立資料中心最佳做法 WildFire 分析設定檔

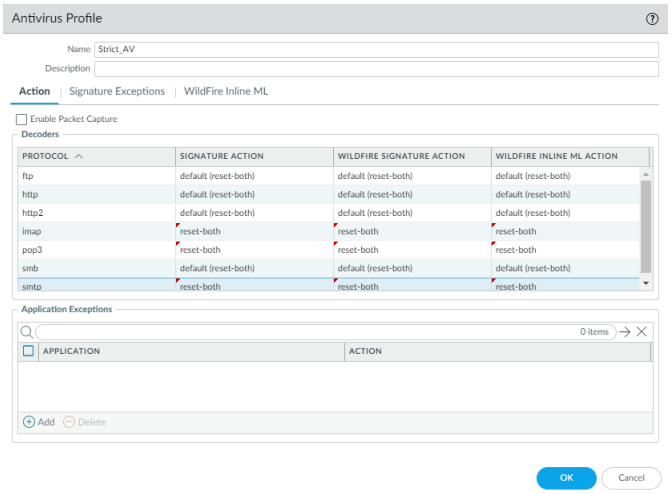
建立一或多個安全性設定檔群組，讓您一次可以將所有設定檔套用至安全性政策規則，而不是個別指定它們。

若不存在與網際網路的直接輸出連線，則無需為資料中心防火牆訂閱URL 篩選。未直連線至網際網路的防火牆不需要 PAN-DB URL 篩選解決方案，因為該解決方案會識別網際網路 URL，而不是專用資料中心 URL，因此不會針對資料中心流量匯入 PAN-DB 資料庫並檢查 URL。若您不確定防火牆是否具有 URL 流量，請訂閱 URL 篩選試用服務，並將設定檔設為針對所有 URL 類別發出警示以識別任何 URL 流量。否則，URL 篩選應在使用者流量進出網路之網路周邊（而不是資料中心周邊）的防火牆上進行。考慮建立自訂 URL 類別（**Objects**（物件）> **Custom Objects**（自訂物件）> **URL Category**（**URL** 類別）），以識別並控制對內部資料中心 Web 服務的存取。

建立資料中心最佳做法防毒設定檔

複製預設防毒設定檔並進行編輯。若要確保業務關鍵性應用程式的可用性，當您從現行狀態移至最佳做法設定檔時，請採取安全移轉步驟。若要完成最佳做法設定檔，按如下所示對預設設定檔進行修改，並將其附加至所有允許流量的安全性原則規則。防毒設定檔有通訊協定解碼器，可偵測和防止超過七個通訊協定傳輸的病毒和惡意軟體：FTP、HTTP、HTTP2、IMAP、POP3、SMB 以及 SMTP。您可以設定所有七個通訊協定的 WildFire 動作，因為防毒設定檔也會根據 WildFire 特徵碼和內嵌機器學習來執行動作。

設定複製的最佳做法防毒設定檔，重設用於七個通訊協定解碼器和 WildFire 動作的用戶端和伺服器，然後將設定檔附加至四個資料中心流量流程的允許規則。



儲存格左上角的紅色三角形表示動作已經過修改（從預設值修改），修改後的設定檔名稱為 **Strict_AV**。

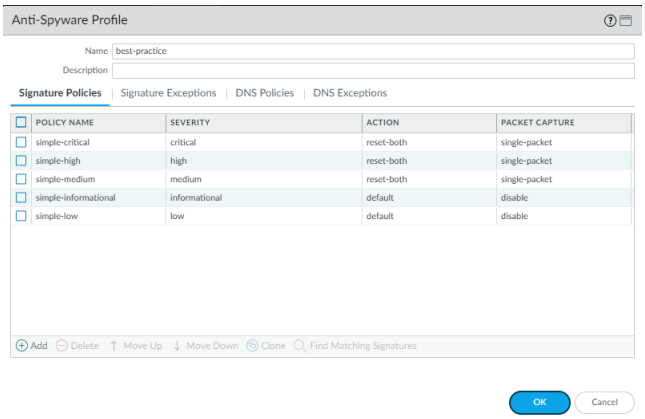
將最佳做法防毒設定檔附加至所有允許流量的安全性政策規則，以在已知惡意檔案（惡意軟體、勒索軟體機器人和病毒）試圖進入網路時將其封鎖。例如：

- 內部資料中心流量—防毒設定檔及漏洞保護設定檔有助於防止攻擊者利用漏洞，在資料中心網路內的伺服器之間橫向傳播惡意軟體和駭客工具。
- 從資料中心到網際網路的流量—防毒設定檔及反間諜軟體設定檔有助於識別和封鎖命令與控制流量及惡意軟體和駭客工具的初始下載。

建立資料中心最佳做法反間諜軟體設定檔

附加反間諜軟體設定檔至所有允許資料中心流量的安全性原則規則。反間諜軟體設定檔可以偵測命令與控制 (C2) 流量，這些流量來自安裝在伺服器或端點上的間諜軟體，包括廣告軟體、後門、瀏覽器劫持、資料竊取及鍵盤記錄等類別，並可防止受到攻擊的系統從網路建立輸出連線。

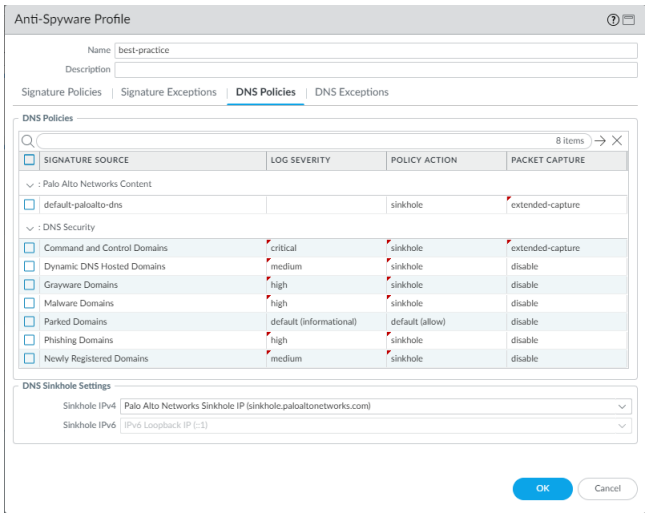
複製預先定義的嚴格反間諜軟體設定檔並進行編輯。若要確保業務關鍵性應用程式的可用性，當您從現行狀態移至最佳做法設定檔時，請採取安全移轉步驟。如果您設定了可以向其傳送流量進行分析的沉洞，請啟用具有封包擷取功能的 DNS 沉洞，以幫助您追蹤試圖解析惡意網域的端點。最佳做法反間諜軟體設定檔保留預設的 **Action (動作)**，以在防火牆偵測到中、高或重大嚴重的威脅時重設連，並啟用針對這些威脅的單一封包擷取 (PCAP)。



切勿要啟用用於資訊活動的 PCAP，因為會產生相對大量的該流量，而且與潛在威脅相較之下不是特別有用。套用延伸的 PCAP（跟單一 PCAP 相反）到您套用 **alert (警示)** 活動的高價值流量中。使用相同的邏輯套用 PCAP以決定記錄哪些流量—採用您記錄的流量的 PCAP。套用單一 PCAP 至您封鎖的流量。延伸 PCAP

記錄然後傳送到管理面的預設封包數目是五個封包，也就是建議的值。在大多數情況中，擷取五個封包提供充份的資訊以分析威脅。如果傳送太多 PCAP 流量到管理面，則擷取超過五個封包可能導致 PCAP 下降。

最佳做法 **Action on DNS Queries**（**DNS** 查詢動作）是封鎖 DNS 查詢或將其設為沉洞，並在您無法看到 DNS 查詢時啟用 PCAP。



啟用 DNS sinkhole 可找出嘗試透過追蹤主機和防止它們存取這些網域，以進入可疑網域的可能遭到入侵的主機/。在防火牆看不到 DNS 查詢的建立者時（通常在防火牆位於本機 DNS 伺服器的北邊時）啟用 DNS sinkhole，這樣您可以找出遭到感染的主機。在防火牆可以看到 DNS 查詢的建立者（通常在防火牆位於本機 DNS 伺服器的南邊時。在此情況中，防火牆的封鎖規則和記錄可提供對流量的可見度）或在您封鎖的流量上時，不要啟用 DNS sinkhole。

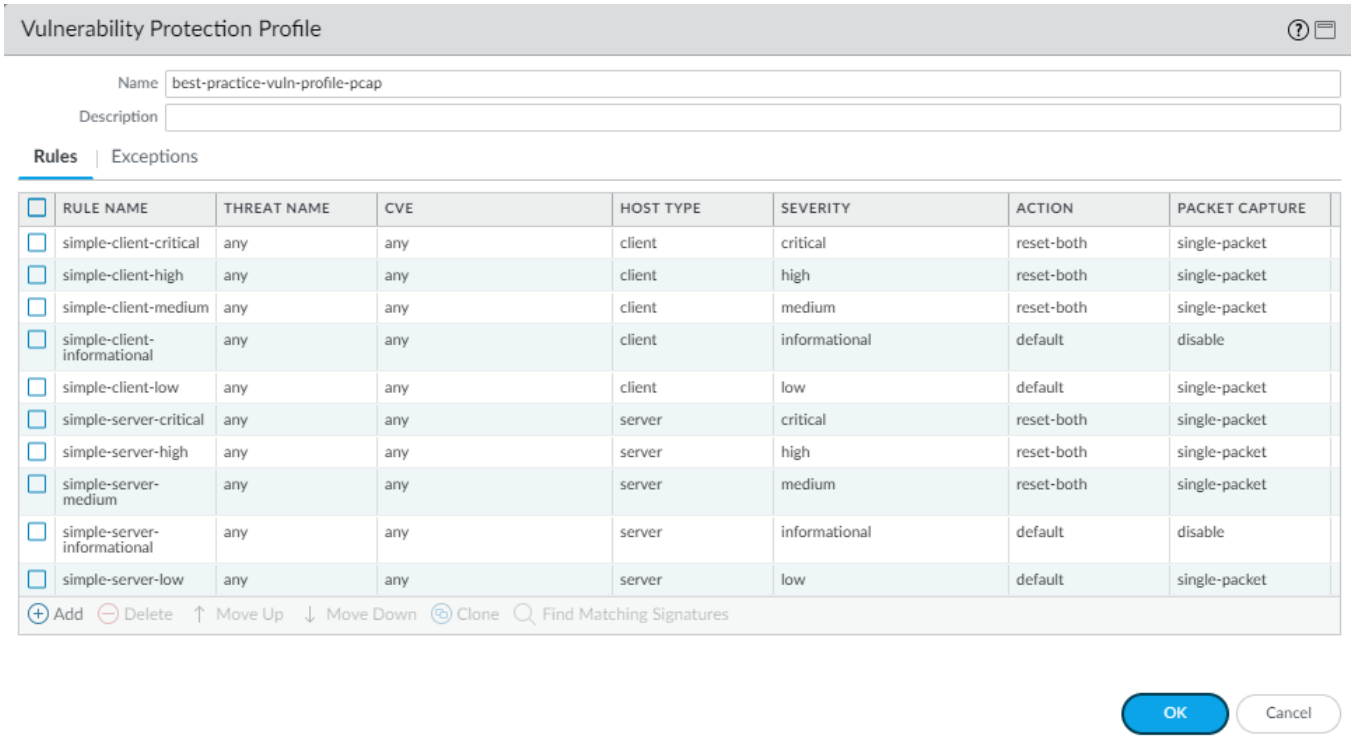
除了使用 DNS 沉洞技術保護主機之外，還可以將最佳做法反間諜軟體設定檔附加至所有安全性原則規則，這些規則允許流量在流量離開網路時識別受感染的主機，並透過防止受到攻擊的系統與惡意 C2 網路通訊來阻止攻擊者。如果一個系統無法與 C2 網路通訊，則 C2 網路將無法控制該系統。例如：

- 從使用者到資料中心的流量、內部資料中心流量及從網際網路到資料中心的流量—反間諜軟體設定檔封鎖點對點 C2 流量。
- 從資料中心到網際網路的流量—反間諜軟體設定檔及防毒設定檔有助於識別和封鎖 C2 流量及惡意軟體和駭客工具的初始下載。

建立資料中心最佳做法漏洞保護設定檔

附加漏洞保護設定檔至所有允許流量的安全性原則規則。漏洞保護設定檔可以防止緩衝區溢位、非法代碼執行及其他試圖利用用戶端和伺服器端漏洞之行為透過資料中心網路造成破壞或進行橫向移動。

複製預先定義的嚴格漏洞保護設定檔。若要確保業務關鍵性應用程式的可用性，當您從現行狀態移至最佳做法設定檔時，請採取安全移轉步驟。針對最佳做法設定檔，對於 **simple-client-informational** 和 **simple-server-informational** 以外的每個規則，按兩下 **Rule Name**（規則名稱）並將 **Packet Capture**（封包擷取）從 **disable**（停用）變更為 **single-packet** 來啟用每個規則的封包擷取 (PCAP)，以追蹤潛在攻擊的來源。不要變更其他設定。自動下載內容更新並儘快安裝，使簽章集始終保持最新。



切勿要啟用用於資訊活動的 PCAP，因為會產生相對大量的該流量，而且與潛在威脅相較之下不是特別有用。套用延伸的 PCAP（跟單一 PCAP 相反）到您套用 **alert (警示)** 活動的高價值流量中。使用相同的邏輯套用 PCAP以決定記錄哪些流量—採用您記錄的流量的 PCAP。套用單一 PCAP 至您封鎖的流量。延伸 PCAP 記錄然後傳送到管理面的預設封包數目是五個封包，也就是建議的值。在大多數情況中，擷取五個封包提供充份的資訊以分析威脅。如果傳送太多 PCAP 流量到管理面，則擷取超過五個封包可能導致 PCAP 下降。

將最佳做法漏洞保護設定檔附加到所有允許流量的安全性原則規則的原因是，如果您沒有實施嚴格的漏洞保護，攻擊者便可利用用戶端或伺服器端的漏洞來攻擊資料中心。例如：

- 內部資料中心流量—嚴格的漏洞保護設定檔及防毒設定檔有助於防止攻擊者利用漏洞，在資料中心網路內的伺服器之間橫向傳播惡意軟體和駭客工具。
- 從資料中心到網際網路的流量—漏洞保護有助於防止受感染的資料中心伺服器攻擊網際網路伺服器。
- 從網際網路到資料中心的流量—嚴格的漏洞保護設定檔可以封鎖試圖使用伺服器端漏洞攻擊資料中心伺服器的行為。如果伺服器受到攻擊，漏洞保護有助於防止受感染的伺服器向用戶端傳遞漏洞利用程式，隔離感染，並保護您的合作夥伴和客戶免受水坑攻擊。漏洞保護還可以使用封鎖 IP 動作阻止暴力攻擊。當暴力攻擊簽章觸發該動作時，防火牆會在設定的時間內封鎖攻擊者的 IP 位址。如果暴力攻擊在設定的時間後繼續，簽章會再次觸發封鎖動作。暴力攻擊可能會繼續進行，但永遠都不會成功。

建立資料中心最佳做法檔案封鎖設定檔

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

在有些情況中，支援重要應用程式的需求可能妨礙您封鎖所有嚴格設定檔的檔案類型。遵循安全移轉建議以協助判斷您是否需要在網路的不同區域建立例外情況。檢閱資料篩選日誌（*Monitor*（監控）> *Logs*（日誌）> *Data Filtering*（資料篩選））以識別資料中心使用的檔案類型，並與業務關係人討論其應用程式需要的檔案類型。根據這些資訊，必要時複製嚴格

的設定檔並視需要修改，以便僅允許您需要支援的重要應用程式的其他檔案類型。您還可使用方向設定來限制檔案類型在兩個方向的傳輸，或封鎖檔案在一個方向的傳輸，但不封鎖在另一個方向傳輸。

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

將最佳做法檔案封鎖設定檔附加到所有允許流量的安全性原則規則的原因是，幫助防止攻擊者透過檔案共享應用程式和漏洞利用套件，或透過感染存取資料中心的使用者，或感染 USB 隨身碟，向資料中心傳遞惡意檔案。

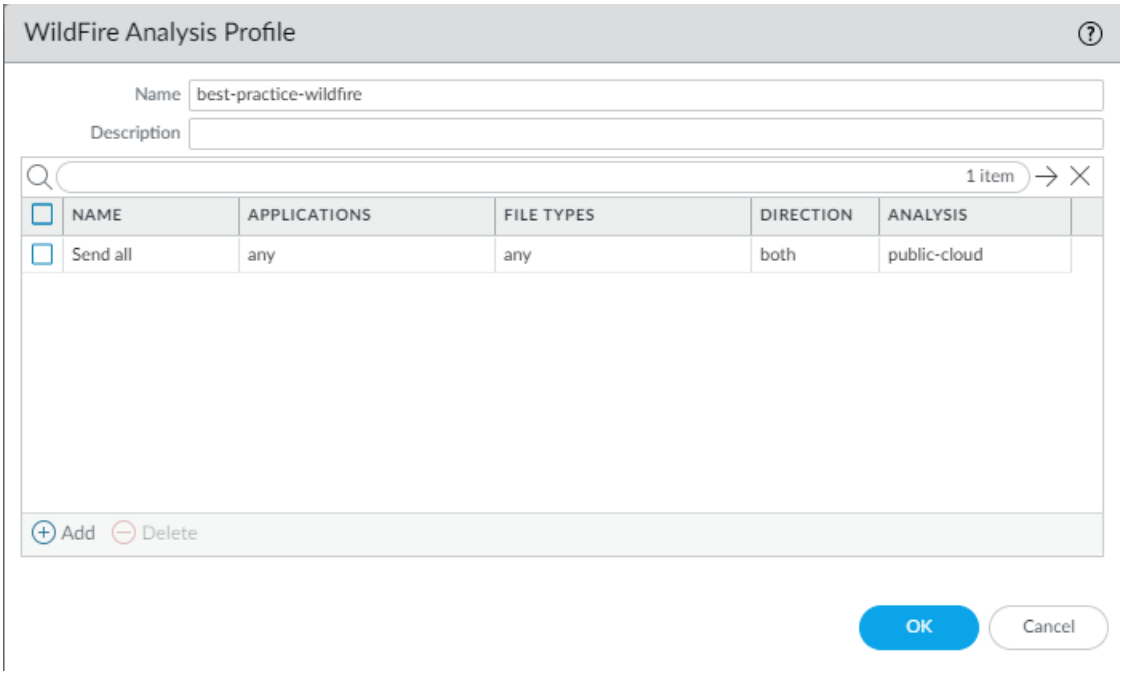
- 從使用者到資料中心的流量—將嚴格的檔案封鎖設定檔附加至安全性原則規則，以便無需進行檔案共享或共同作業的應用程式封鎖可能傳遞漏洞利用套件和惡意軟體的危險檔案類型。
- 內部資料中心流量—將嚴格的檔案封鎖設定檔附加至安全性原則規則，以防止受到攻擊的伺服器與資料中心的其他伺服器共享惡意檔案。這可以隔離感染並防止惡意軟體透過資料中心進行傳播。
- 從資料中心到網際網路的流量—將檔案傳輸限制在使用中的應用程式所需的檔案類型中。

如果您不封鎖所有 Windows PE 檔案，則須向 WildFire 傳送所有未知檔案進行分析。對於使用者帳戶，請將 **Action**（動作）設定為 **continue**（繼續）以幫助防止路過式下載，路過式下載是指惡意網站、電子郵件或快顯視窗讓使用者在無意中下載惡意檔案的行為。告訴使用者，對於在其不知情的情況下進行的檔案傳輸，如果出現 continue（繼續）提示，則表示其可能在下載惡意檔案。

建立資料中心最佳做法 WildFire 分析設定檔

其他安全性設定檔可偵測並封鎖已知威脅。WildFire 可保護資料中心免受未知威脅攻擊。設定防火牆以使用預先定義的預設設定檔轉送所有未知檔案至 WildFire 進行分析。未知威脅可能隱藏在許多不同的檔案類型中，成功的攻擊可能在造成破壞很久之後才會被發現。例如，WildFire 可以在攻擊者造成破壞之前識別載入登台伺服器的惡意軟體，並在攻擊者達到目的之前找到漏洞掃描器和橫向移動協助工具。在過去幾年裡，大量大型企業發生的駭客攻擊事件本可使用 WildFire 來避免。任何用於控制已在進行、即將進行或可能進行檔案傳輸活動的流量的安全性原則規則都應包含已啟用的 WildFire 分析設定檔。

設定 WildFire 設備內容更新以時時刻刻自動進行下載和安裝，以便您隨時能取得最新支援。例如，對 *Linux* 檔案和 *SMB* 檔案的支援首先在 *WildFire* 設備內容更新中提供。



將預設 WildFire 分析設定檔附加到所有允許流量的安全性原則規則的原因是，WildFire 可以提供對未知威脅和進階持續性威脅 (APT) 的最好防禦。例如：

- 從使用者到資料中心的流量—WildFire 可以識別諸如 Confluence 或 SharePoint 的資料中心內的未知惡意軟體。
- 內部資料中心流量—WildFire 可以識別在資料中心之間傳播的未知惡意軟體，透過在惡意軟體未造成任何損害之前發現它來防止資料洩露。
- 從資料中心到網際網路的流量—由於此類流量會下載用於軟體和作業系統更新的可執行檔，因此其對於在所有應用程式上執行 WildFire 以識別惡意行為至關重要。

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

如有必要，您可以根據流量方向限制傳送進行分析的應用程式與檔案類型。

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

使用 Cortex XDR 代理程式保護資料中心端點

Cortex XDR 代理程式可保護伺服器與 VM 這類資料中心端點免遭其本身的惡意軟體和入侵，而新世代防火牆則會抵禦跨網路（因此必須周遊防火牆）到達端點的威脅。當惡意軟體或漏洞已在端點上或進入端點時，若端點執行威脅（例如，透過 .exe 或 .dll 檔案），則防火牆不會看到威脅，因為該攻擊是在端點上進行的，且沒有流量穿過防火牆，防火牆也就看不到任何內容。然而，Cortex XDR 代理程式會在每個端點上看到可執行檔中的威脅、文件中的巨集以及動態連結程式庫檔等等。當這些威脅試圖執行時，陷阱會對端點本身採取動作並保護端點。

Cortex XDR 代理程式與新世代防火牆為資料中心端點提供雙層保護，以便防火牆保護端點免受網路威脅侵擾，而 Cortex XDR 代理程式監控並保護端點免受存留在端點上的威脅侵擾。您在 Endpoint Security Manager (ESM) 上為端點設定的安全性原則以及您在 Panorama 或防火牆上設定的安全性原則不會發生衝突，因為它們管理不同位置的不同事件。Cortex XDR 代理程式控制每個個別端點的安全性。防火牆控制周遊防火牆之流量的安全性。

在每個資料中心端點上安裝 Cortex XDR 代理程式。資料中心內 Cortex XDR 代理程式的最佳做法與任何端點上 Cortex XDR 代理程式的最佳做法相同，因為內容一律為端點本身，所以「資料中心內」的內容或「使用者群組內」的內容無關緊要—Cortex XDR 代理程式會以相同的方式保護所有端點。因此，對於資料中心與網路的任何其他區域，惡意軟體保護政策最佳做法等皆是相同。

建立資料中心流量封鎖規則

在您為四種資料中心流量建立應用程式允許規則之前，建立封鎖和記錄規則以封鎖您不會在資料中心使用的應用程式、封鎖已知不良應用程式，並發現網路中您可能不知道的應用程式。記錄被封鎖的流量可提供關於潛在攻擊的資訊，以幫助您進行研究。

當您發現未知應用程式時，判斷應當允許這些應用程式，還是它們代表著潛在威脅。如果這些規則發現應該允許的應用程式，則相應地調整應用程式允許規則。如果這些規則發現了不合法的應用程式，則其可能代表著潛在威脅，您可使用日誌資訊對其進行研究。不要套用安全性設定檔來封鎖規則，因為其控制的流量絕不會進入您的網路。

如果您發現的未知應用程式為內部專有應用程式或其他類型的合法應用程式，則為每個未知應用程式建立自訂應用程式，以便您識別並對其套用安全性原則。

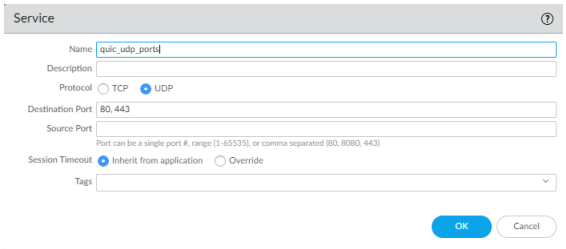
對資料中心安全性原則規則庫進行排序向您展示如何利用我們為四個資料中心流量建立的所有其他規則對這些規則進行排序，如此便不會有規則影響其他規則。

若要在多個資料中心之間套用一致的安全性原則，您可重複使用範本和範本堆疊，以便相同的原則適用於每個資料中心。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

STEP 1 | 封鎖快速 UDP 網際網路連線 (QUIC) 通訊協定。

Chrome 以及其他一些瀏覽器會使用 QUIC 而非 TLS 建立工作階段，但 QUIC 使用防火牆無法解密的專用加密手法，因此潛在危險的流量可能會如加密流量般進入網路。封鎖 QUIC 會強制瀏覽器回退到 TLS，並讓防火牆可以解密流量。

建立建立安全性原則規則以在其 UDP 服務連接埠（80 和 443）封鎖 QUIC，並建立單獨的規則以封鎖 QUIC 應用程式。對於封鎖 UDP 連接埠 80 和 443 的規則，建立包含 UDP 連接埠 80 和 443 的服務（**Objects**（物件）> **Services**（服務））：



使用該服務指定 UDP 連接埠以封鎖 QUIC。在第二個規則中，封鎖 QUIC 應用程式，讓規則庫中的前兩個規則封鎖 QUIC：

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

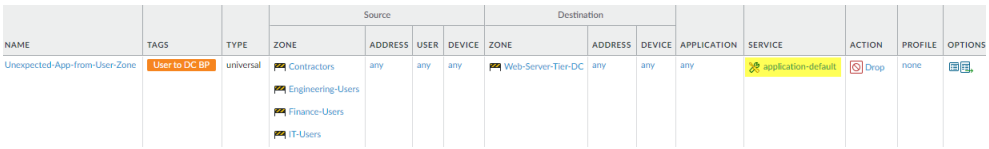
STEP 2 | 從應用程式預設連接埠上的使用者區域封鎖所有應用程式以識別意外應用程式。

此規則可發現使用者正在嘗試使用的應用程式及在資料中心執行而您並不知道的應用程式。監控與此規則相符的流量，以確定其為潛在威脅還是您需要修改允許規則來啟用應用程式的存取。請確保將此規則置於允許流量的規則之後，否則此規則將封鎖您打算允許的流量。

在此規則後面顯示的規則與此規則類似，但其適用於任何來源的流量，而不僅限於來自使用者區域的流量。建立單獨規則的原因是，違反使用者區域規則可能表示您封鎖部分使用者需要用於處理業務的合法應用程式，因此您可能需要修改規則以針對特定一組使用者

允許應用程式。違反非使用者區域規則可能表示應用程式發生變更或存在潛在攻擊。為其餘流量建立單獨規則可讓您檢視使用者流量和試圖進入資料中心之所有其他流量的單獨日誌，這讓調查和應對潛在問題變得更容易。

此規則必須在下一個規則之前，後者適用於所有流量，因此您可在首次記錄使用者區域違規情況後記錄和監控應用程式預設連接埠上使用意外應用程式的嘗試，而不考慮來源。



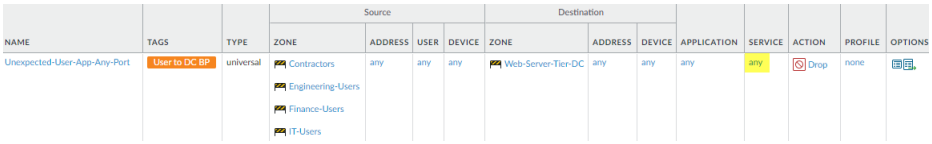
若要建立此規則：

- 來源區域包括所有使用者區域與使用者（部署的使用者區域數目可能多於此範例中顯示的使用者區域數目）。
- 目的地區域為資料中心周邊的資料中心 Web 伺服器層 (**Web-Server-Tier-DC**)。
- 將應用程式設定為 **any**（任何）並將服務設定為 **application-default**（應用程式預設），使規則適用於在其標準連接埠上執行的所有應用程式。
- 將動作設定為 **Drop**（丟棄）以在不向用戶端或伺服器傳送訊號的情況下安靜地丟棄流量。

STEP 3 | 從任何連接埠上的使用者區域封鎖所有應用程式以識別正在執行但不應在此執行的應用程式。

此規則可識別使用者試圖在非標準連接埠上執行的合法、已知應用程式以及您可能需要為其建立自訂應用程式的未知應用程式。調查與此規則相符的任何流量之來源，以確保您未允許 unknown-tcp、unknown-udp 或 non-syn-tcp 流量。請確保將此規則置於允許流量的規則之後，否則此規則將封鎖您打算允許的流量。

我們稍後還會在此區段中建立與此規則 *(Unexpected-App-from-Any-Zone)* 類似的不同封鎖規則，但其適用於任何來源的流量，而不僅限於來自使用者區域的流量。建立單獨規則的原因是，違反使用者區域規則可能表示部分使用者需要用於處理業務的合法應用程式未正確設計，因此您可能需要修改應用程式。為其餘流量建立單獨規則可讓您檢視使用者流量和試圖進入資料中心之所有其他流量的單獨日誌，這讓調查和應對潛在問題變得更容易。



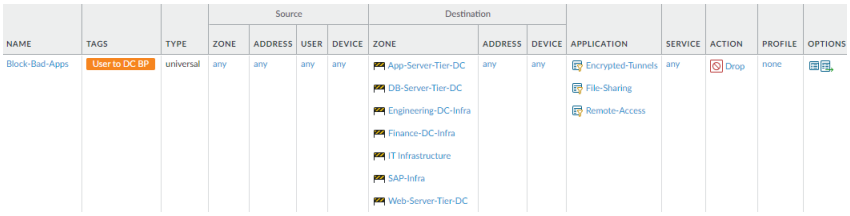
若要建立此規則：

- 來源區域包括所有使用者區域與使用者（部署的使用者區域數目可能多於此範例中顯示的使用者區域數目）。
- 目的地區域為資料中心周邊的資料中心 Web 伺服器層 (**Web-Server-Tier-DC**)。
- 將應用程式設定為 **any**（任何）並將服務設定為 **any**（任何），使規則適用於在任何連接埠上執行的所有應用程式。
- 將動作設定為 **Drop**（丟棄）以在不向用戶端或伺服器傳送訊號的情況下安靜地丟棄流量。

STEP 4 | 封鎖應用程式設計成規避或避開安全性問題，比如攻擊者通常導致破壞或資料中心不需要應用程式等問題。

此規則可保護資料中心免受您在網路中不需要的應用程式的影響。雖然最佳做法安全性政策的目標是使用應用程式允許規則進行積極執行，但明確封鎖和記錄潛在的危險應用程式活動，如未認可的檔案共用應用程式、遠端存取應用程式或加密通道，可提供對潛在攻擊的可視性及其相關資訊。即使在您建立可靠的應用程式允許清單之後，也要在規則庫中保留此應用程式封鎖規則，因為違規嘗試日誌有助於您對潛在的攻擊展開調查。

使用此規則僅封鎖您在資料中心永遠不需要的應用程式。



NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Block-Bad-Apps	User to DC BP	universal	any	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	

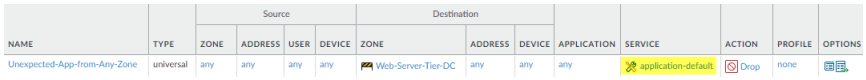
若要建立此規則：

- 將來源區域、位址、使用者和裝置設定為 **any**（任何），因為您將封鎖不允許任何人在資料中心使用的應用程式。
- 在目的地區域指定所有資料中心區域以保護所有資料中心伺服器免受不良應用程式影響。
- 為您想要封鎖的每種類型（類別）的應用程式建立應用程式篩選器並指定任何其他應用程式。此範例包含加密通道、遠端存取和檔案共享的應用程式篩選器。去除不需要的應用程式來封鎖您不會在資料中心使用的應用程式以減少攻擊面，這同時也會降低風險。使用應用程式篩選器取代應用程式群組或列出個別應用程式的優點是，篩選器可自動更新，因此出現新的應用程式時無需維護。
- 將服務設定為 **any**（任何）以在非標準連接埠及預設連接埠上擷取不需要的應用程式。
- 將動作設定為 **Drop**（丟棄）以在不向用戶端或伺服器傳送訊號的情況下安靜地丟棄流量。

範例規則中顯示的應用程式篩選器清單不全面。根據如何評估您的資料中心對您建立的應用程式清單進行評估並新增您不想允許此規則使用的應用程式。將此封鎖規則置於允許規則之後，以允許規則例外。例如，IT 人員需要使用遠端存取應用程式來管理資料中心裝置，因此您必須先允許其使用遠端存取應用程式，然後才能對所有其他使用者封鎖遠端存取應用程式。另一個範例是，您可能會在此封鎖規則之前的允許規則中認可一個或兩個檔案共用應用程式，然後此規則中的應用程式篩選器會封鎖所有其他應用程式。如果有您在網路中永遠都不需要的多組應用程式或個別應用程式，且沒有例外情況，您可以建立特定封鎖規則以僅封鎖這些應用程式，並將其置於規則庫頂部，位於應用程式允許規則之上。不過，如果您執行此操作，則必須確保封鎖的應用程式不具備合法的業務用途，因為使用者將無法存取它們。

STEP 5 | 從應用程式預設連接埠上的任何區域封鎖所有應用程式以識別意外應用程式。

此規則可從任何區域發現在資料中心執行而您並不知道的應用程式。違反此規則可能表示應用程式發生了變更或可能表示存在潛在威脅。監控與此規則相符的流量，以確定其為潛在威脅還是您需要修改應用程式允許規則。請確保將此規則置於允許流量的允許規則之後，否則此規則將封鎖您打算允許的流量，並置於步驟 1 中的規則之後，這樣它就不會從使用者區域擷取流量。



NAME	TYPE	Source ZONE	Source ADDRESS	Source USER	Source DEVICE	Destination ZONE	Destination ADDRESS	Destination DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Unexpected-App-from-Any-Zone	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	application-default	Drop	none	

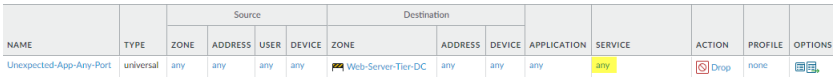
若要建立此規則：

- 將來源設定為 **any**（任何）以涵蓋試圖進入資料中心的所有剩餘流量（步驟 1 中的規則將在流量與此規則相符之前封鎖並識別意外的使用者應用程式）。
- 目的地區域為資料中心周邊的資料中心 Web 伺服器層 (**Web-Server-Tier-DC**)。
- 將應用程式設定為 **any**（任何）並將服務設定為 **application-default**（應用程式預設），使規則適用於在其標準連接埠上執行的所有應用程式。
- 將動作設定為 **Drop**（丟棄）以在不向用戶端或伺服器傳送訊號的情況下安靜地丟棄流量。

STEP 6 | 從任何連接埠上的任何區域封鎖所有應用程式以識別正在執行但不應在此執行的應用程式。

此規則可識別試圖在非標準連接埠上執行的合法、已知應用程式以及您可能需要為其建立自訂應用程式的未知應用程式。調查與此規則相符的任何流量之來源，以確保您未允許 unknown-tcp、unknown-udp

或 non-syn-tcp 流量。請確保將此規則置於允許流量的允許規則之後，否則此規則將封鎖您打算允許的流量，並置於前一個規則之後，這樣它就不會從使用者區域擷取流量。



NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Unexpected-App-Any-Port	universal	any	any	any	any	Web-Server-Tier-DC	any	any	any	any	Drop	none	

若要建立此規則，請使用與規則 **Unexpected-App-from-User-Zone** 相同的設定，但其不是在來源中指定使用者區域，而是指定 **any**（任何）區域以涵蓋試圖進入資料中心的所有剩餘流量，並將服務設定為 **any**（任何）以涵蓋非標準連接埠。

STEP 7 | 在任何連接埠上發現試圖執行任何應用程式的未知使用者。

此規則可透過查找未知使用者識別 User-ID 範圍內的漏洞。它還可識別使用者社群中試圖存取您的資料中心的受攻擊或內嵌裝置。（內嵌裝置無使用者介面，例如印表機、讀卡機和相機，但攻擊者可在攻擊時入侵並使用這些裝置。）

NAME	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
		ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
Discover-Unknown-Users	universal	any	any	unknown	any	any	any	any	any	any	Deny	none	

此規則與阻止區域間通訊的區域間預設規則幾乎相同（除非另一個規則允許流量），但其不會丟棄所有使用者的流量，而只丟棄未知使用者的流量。這讓您能夠分別記錄規則相符情況並更輕鬆地調查試圖存取資料中心的未知使用者。

定義初始使用者至資料中心流量安全性原則

為流向資料中心的使用者流量定義初始最佳做法安全性政策，即可開始制定資料中心應用程式允許清單。最終目標在於，透過明確控制可以存取資料中心的人員，他們可以存取的資料中心應用程式以及他們可在資料中心內存取的資源，使用積極安全性實施以零信任架構保護資料中心。最佳做法安全性原則制定完成後，任何未知使用者皆將無法存取資料中心，且資料中心內不應存在任何未知應用程式或資源。

- 使用者至資料中心流量安全性方法
- 建立使用者至資料中心應用程式允許規則
- 建立使用者至資料中心驗證原則規則
- 建立使用者至資料中心解密原則規則

使用者至資料中心流量安全性方法

使用傳統舊方法保護流向資料中心的使用者流量，會使有價值的資產面臨風險，而最佳做法方法則會保護有價值的資產。

傳統方法	風險	最佳做法方法
基於連接埠的規則提供足夠的安全性，因為資料中心位於受信任網路中。	惡意應用程式透過以下方式存取網路來避免偵測：偽造連接埠號碼、透過連接埠執行通道作業或使用連接埠跳躍。	應用程式允許規則與應用程式、使用者及伺服器相結合，確保只有使用認可應用程式的合法使用者才能存取正確的資料中心伺服器集。 當您從基於連接埠的規則轉換到基於應用程式的規則時，請在規則庫中將基於應用程式的規則置於其將取代之基於連接埠的規則之上。為這兩種規則重設原則規則命中計數器。若流量符合基於連接埠的規則，則其原則規則命中數會增加。調整基於應用程式的規則，直至在一段時間內沒有任何流量符合基於連接埠的規則，然後移除基於連接埠的規則。
信任內部使用者並允許使用者存取的應用程式根據認證以及可能的 IP 位址規則確定是否允許存取。	攻擊者可以存取資料中心端點，然後橫向移動至任何其他資料中心端點，以利用竊取的認證或伺服器端漏洞。不明使用者可以存取資料中心端點。	啟用 User-ID、封鎖不明使用者，以及允許認可使用者的存取權限。為員工、合作夥伴及承包商建立單獨的身分網域。將多因素驗證 (MFA) 用於合作夥伴、承包商以及敏感伺服器存取。
由於資料中心位於受信任的網路中，無需對不明檔案進行分析。	使用者可能會意外地從檔案共用及其他雲端應用程式中下載惡意軟體。	將所有不明檔案傳送至 WildFire 進行分析，即可識別新惡意軟體及不明惡意軟體並加以抵禦。
將來自多個供應商的威脅防禦設定檔相結合。	個別工具的結合為攻擊者留下了安全性漏洞，可能無法很好地協同工作。	Palo Alto Networks 協同安全性工具套件協同工作，可以堵住安全性漏洞並防止攻擊。

建立使用者至資料中心應用程式允許規則

當您評估資料中心時，將取得一些資訊，以便您根據哪些使用者應該有權限存取在哪些伺服器組上執行的哪些應用程式的明確決策，建立一組應用程式允許規則。制定應用程式安全性政策規則（**Policies**（政策）> **Security**（安全性）），以便只有您明確允許的使用者才能僅在合適的伺服器組上使用僅與其工作相關的應用程式。不允許不必要的存取、未知使用者及未知應用程式。

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

對資料中心安全性原則規則庫進行排序向您展示如何利用我們為其他三個資料中心流量建立的所有其他規則和封鎖規則對這些規則進行排序，如此便不會有規則影響其他規則。

若要在多個資料中心之間套用一致的安全性原則，您可重複使用範本和範本堆疊，以便相同的原則適用於每個資料中心。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

下列所有允許規則：

- 附加最佳做法安全性設定檔群組，其包含最佳做法安全性設定檔。使用安全性設定檔群組可讓您一次將所有最佳做法設定檔都套用至規則，而不是個別指定每個設定檔。安全性設定檔群組會更快速且更輕鬆地設定防止惡意軟體、漏洞、C2 流量以及已知和未知威脅的攻擊。
- 記錄流量（在工作階段端），讓您可以追蹤和分析規則違規，以及包含日誌轉送。將日誌轉送至日誌伺服器，並在適用時，將日誌電子郵件轉送給適當的管理員。

STEP 1 | 讓適當的使用者能夠存取您的公司內部 DNS 伺服器（不允許存取外部 DNS 伺服器）。

此規則限制了對公司 DNS 伺服器的存取，縮小了攻擊面，有助於保護關於內部主機和服務的 DNS 項目。為防止被公共 DNS 查詢發現，DNS 項目不會儲存在公開的 DNS 伺服器中，因此攻擊者瞭解這些項目的唯一方法是攻擊公司 DNS 伺服器，如此您的 DNS 伺服器便成了極具吸引力的目標。

在網際網路閘道上（網路周邊），封鎖所有流入公共 *DNS* 伺服器的 *DNS* 流量。不要允許 *DNS* 流量流入網際網路。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
DNS Services	User to DC BP	universal	any	any	any	any	IT Infrastructure	DNS-Servers	any	dns	application-default	Allow		

對於不在政策規則中允許「任何」使用者的最佳做法（因為使用者需要存取 DNS 服務才能登入）來說，此規則屬於例外情況。此規則可以保護對 DNS 服務的存取。若要建立此規則：

- 限制對資料區域中適當目的地區域 **IT infrastructure**（**IT** 基礎結構）的存取。
- 設定 **DNS Servers**（**DNS** 伺服器）的位址群組並限制僅對該群組的存取。
- 防止使用除 **dns** 之外的任何應用程式進行存取。
- 將最佳做法安全性設定檔群組套用至 DNS 流量特別重要，因為如果攻擊者劫持您的 DNS 伺服器，就可以將流量重新導向至看起來與使用者試圖存取的合法網站類似的網路釣魚網站。

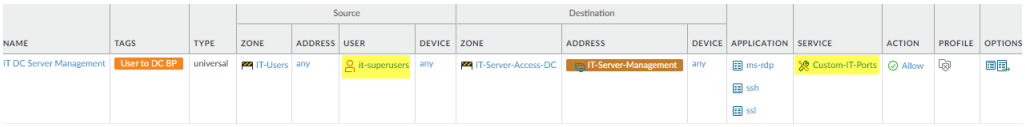
STEP 2 | 允許必要 IT 人員利用特權安全存取資料中心伺服器以便進行管理和維護。

此規則展示了如何保護擁有特權帳戶的使用者對重要系統的存取。特權帳戶要求使用者具有較高的信任度並會授予其存取包含公司最寶貴資料的重要系統的管理存取權限，因此您必須嚴格控制和監控特權帳戶。利用 App-ID 僅指定 IT 使用者管理資料中心裝置所需的應用程式，以便防火牆拒絕所有其他應用程式的存取。在此範例中，一組 IT 使用者需要管理存取權限來管理資料中心伺服器。

為便於管理資料中心伺服器的 *IT* 特權存取應僅限於在管理介面上進行，且應當在專用 *VLAN* 上進行，以便分隔伺服器管理流量與其他流量。管理介面應該在相同子網路上。不

要允許在資料介面上進行此類存取。如果 *IT* 群組使用 *SSH* 或 *RDP* 進行管理存取，則不要允許使用 *SSH* 或 *RDP* 進行其他目的的存取。

您 *IT* 網路團隊的組織將決定允許哪些人員進行 *IT* 特權存取。對於每種類型的特權存取，伺服器和其他裝置將按其存取需求進行分組。只允許必要的 *IT* 使用者僅使用進行裝置管理所需的應用程式存取每組伺服器。



若要建立此規則：

- 由於只有一部分 IT 使用者可能會管理資料中心伺服器，因此可利用 User-ID 來特別為需要該等級特權存取權限的 IT 使用者建立一個群組（本範例中為 **it-superusers**）。
- 建立一個靜態位址群組 (**IT-Server-Management**)，其中包含您希望 **it-superusers** 管理並將目的地限制到 **IT-server-access-DC** 區域中該位址群組的伺服器管理介面位址。
- 僅允許預設連接埠上 IT 超級使用者履行其工作職責所需的應用程式。在此範例中，規則允許 **ssl**、**ssh** 和 **ms-rdp** 應用程式。

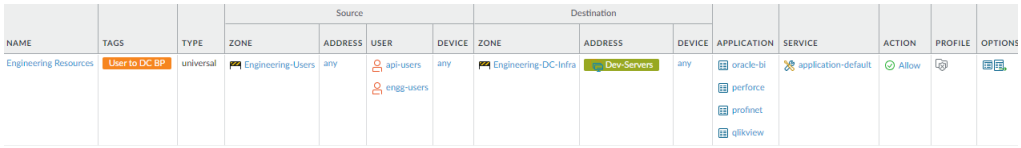
允許的應用程式即為範例。允許您的 *IT* 部門用於管理資料中心伺服器的應用程式。在某些情況下，透過 *SSL* 連線的應用程式可能需要新增特定應用程式以便由 *App-ID* 正確識別。

IT 還會管理資料中心的交換器、路由器及其他裝置。如果相同的 IT 使用者群組使用相同應用程式管理這些資源，則您可將其新增至目的地區域和位址，以便規則允許 IT 超級使用者存取這些裝置的管理介面。如果不同的 IT 使用者群組管理不同的資料中心資源組或使用不同應用程式，則為每個使用者群組和每組應用程式建立單獨、嚴格的安全性原則規則。

由於擁有特權帳戶的使用者群組可以存取重要系統，因此如果攻擊者入侵了他們的認證，您需要在建立使用者至資料中心驗證原則規則時要求 MFA 阻止其進行存取。為所有特權存取規則建立對應的驗證原則和解密原則規則。

STEP 3 | 允許具有合法商業理由的員工使用者群組與資料中心伺服器進行通訊。

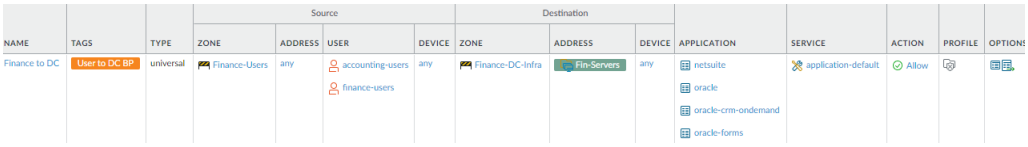
此規則展示了如何限制每個使用者群組（某些情況下為個別使用者）的存取權限，僅允許其存取必要的應用程式和伺服器。例如，需要在資料中心存取開發伺服器的工程師。若要建立安全性原則規則，請建立一個動態位址群組，其中包含該群組使用的所有資料中心開發伺服器的 IP 位址，識別工程師需要在這些伺服器上使用的應用程式，並根據這些群組建立規則。



若要建立此規則：

- 指定需要在資料中心存取工程伺服器的工程使用者群組，本範例中為 **api-users** 和 **engg-users**。
- 透過為資料中心開發伺服器建立動態位址群組 (**Dev-Servers**) 並將其設定為目的地位址來限制對它們的存取。
- 僅限存取預設連接埠上用於商業目的的應用程式。

使用相同方法為每個使用者群組建立細微允許規則（必要時，您也可為個別使用者執行此操作），以便每個群組僅可使用在預設連接埠上執行的合法應用程式存取僅用於業務目的的伺服器組。例如，僅允許需要存取包含 PCI 的伺服器的財務使用者群組，使用實現商業目標所需的許可財務應用程式存取這些伺服器。



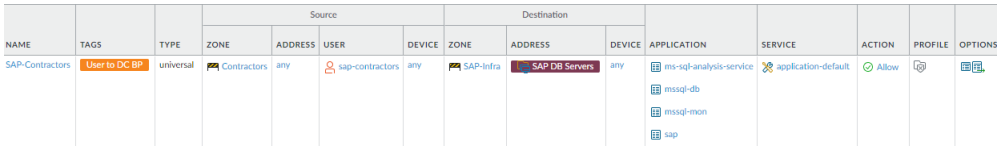
與工程使用者存取資料中心伺服器的允許規則類似，此規則允許 **finance-users** 和 **accounting-users** 群組中的使用者只能使用特定應用程式存取 **Fin-Servers** 動態位址群組中的伺服器。此規則會將最佳做法安全性設定檔套用至允許的流量和記錄活動。

STEP 4 | 允許承包商、合作夥伴、客戶及其他第三方有針對性地、有限制地存取資料中心。

此規則展示了如何嚴格控制第三方使用者的存取權限，使他們只能在需要的伺服器上使用需要的應用程式。例如，一家公司雇用了一組 SAP 開發人員承包商。SAP 開發人員需要在資料中心存取 SAP 資料庫並進行 SQL 查詢。但是，SQL 也會在 SAP 開發人員不應存取的生產資料庫中執行。該公司需要控制三個存取向量：

- 使用者群組—SAP 開發人員承包商。
- 應用程式—MS-SQL 和 SAP。
- 伺服器—僅 SAP 資料庫伺服器。拒絕所有其他資料中心伺服器存取。

User-ID 可隔離 SAP 承包商使用者群組，App-ID 可限制該群組只能使用必要的應用程式，而動態位址群組則可限制其只能存取資料中心的 SAP 資料庫伺服器，透過結合這三者，公司便可提供 SAP 承包商履行職責所需的存取權限，但僅此而已。



若要建立此規則：

- 指定來源區域與使用者，以限制來自 **Contractors**（承包商）區域的 **sap-contractors** 群組中使用者的存取權限。
- 將目的地限制為 **SAP-Infra** 區域的 SAP 資料庫伺服器（**SAP DB Server**（**SAP DB** 伺服器）動態位址群組）。
- 僅允許 SAP 承包商在預設連接埠上使用履行工作職責所需的應用程式。在此範例中，規則允許 **ms-sql-analysis-service**、**mssql-db**、**mssql-mon** 及 **sap** 應用程式。

細微安全性政策規則可以阻止業務目的以外的所有存取，並可透過縮小攻擊面而降低風險。為需要存取您的資料中心的所有第三方群組建立類似允許規則。

不要相信第三方使用者和公司能保障其認證的安全，而應要求進行多重要素驗證（MFA；建立使用者至資料中心驗證原則規則），以便在攻擊者竊取認證或攻擊第三方系統後阻止相關人員進行存取。過去幾年發生的幾起重大資料洩露事件本可利用 MFA 驗證來避免。

透過檢視預先定義的應用程式報告確認僅您在安全性政策規則中明確允許的應用程式正在執行（**Monitor**（監控）> **Reports**（報告）> **Application Reports**（應用程式報告）> **Applications**（應用程式））。如果您在報告中看到意外的應用程式，請檢閱應用程式允許規則並對其進行細化，使其不允許出現意外的應用程式。

建立使用者至資料中心驗證原則規則

驗證原則規則要求使用者必須先證明自己的身份，然後才能存取資料中心服務、應用程式及其他資源。驗證對於保護您最寶貴的資產尤其重要，因為如果攻擊者竊取了認證並利用防火牆進行了驗證，其便可能能夠存取並攻擊您資料中心的任何資產。

存取敏感伺服器及第三方使用者存取伺服器時（例如，SAP 開發承包商在資料中心存取 SAP 伺服器），請執行多重要素驗證 (MFA) 以防止攻擊者使用竊取的認證存取這些系統。過去幾年裡發生的若干重大成功駭客入侵事件本可利用採用 MFA 的驗證原則來避免。

在建立驗證政策規則之前（**Policies**（政策）> **Authentication**（驗證）），您必須設定驗證政策依賴關係，將驗證方法、驗證類型、驗證伺服器的存取方式以及驗證入口網站的使用綁定到驗證政策規則，該驗證政策規則將指定哪些人可以使用哪些服務在哪些伺服器上進行驗證。

STEP 1 | 對具有合法商業理由使用資料中心伺服器的員工使用者群組和個人進行驗證。

此規則展示了如何驗證使用者群組，以便其在必要的伺服器上存取商業活動所需的服務。例如，工程師需要進行驗證才能存取開發伺服器和應用程式。

		Source				Destination					
NAME	TAGS	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
DevEng Resources	User to DC BP	Engineering-Users	any	api-users engg-users	any	Engineering-DC-Infra	Dev-Servers	any	Perforce rdp service-http service-https ssh	Auth-Dev-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

若要建立此規則：

- 指定需要驗證才能在資料中心存取工程伺服器的工程使用者群組，本範例中為 **api-users** 和 **engg-users**。
- 透過為資料中心開發伺服器存取請求建立動態位址群組 (**Dev-Servers**) 並將其設定為目的地位址，來對其套用這些使用者群組的驗證。
- 將驗證規則套用至工程群組需要用於商業目的服務，本範例中為 **Perforce**、**rdp**、**service-http**、**service-https** 和 **ssh**（開發人員可能需要使用 SSH 和 RDP 來存取 Linux 伺服器並應進行驗證才允許存取這些伺服器）。您的驗證規則中的服務取決於群組需要使用的服務。
- 設定驗證強制物件 (**Auth-Dev-Servers**)，以指定驗證方法和驗證設定檔並將其新增至規則。
- 記錄活動，以便您追蹤和分析規則的違反情況，因為這些情況可能表示有人企圖發起攻擊。

另一個驗證使用案例是當群組需要存取一組特定服務時。例如，財務部使用者需要使用特定服務存取敏感的付款卡資訊 (PCI)，則應在獲得存取權限之前進行驗證。為驗證這些服務的使用者，此規則會使用一個自訂服務群組（**Objects**（物件）> **Service Groups**（服務群組）），其僅包含防火牆應驗證財務使用者的服務。

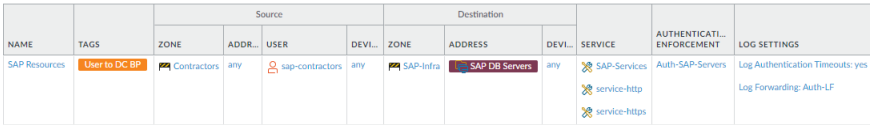
		Source				Destination					
NAME	TAGS	ZONE	ADDR...	USER	DEVI...	ZONE	ADDRESS	DEVI...	SERVICE	AUTHENTICATION ENFORCEMENT	LOG SETTINGS
Finance Servers	User to DC BP	Finance-Users	any	accounting-users finance-users	any	Finance-DC-Infra	Fin-Servers	any	Custom-Finance-Srvrs-Services service-http service-https	Auth-Finance-Servers	Log Authentication Timeouts: yes Log Forwarding: Auth-LF

若要建立此規則：

- 指定需要驗證才能在資料中心存取財務伺服器的使用者群組，本範例中為 **accounting-users** 和 **finance-users**。
- 透過為資料中心財務伺服器存取要求建立動態位址群組 (**Fin-Servers**)，並將其設定為目的地位址，來對其套用這些使用者群組的驗證。
- 將驗證規則套用至財務使用者需要用於商業目的的服務，本範例中為 **service-http**、**service-https**，及自訂服務群組 **Custom-Finance-Srvrs-Services** 中定義的服務，這樣使用者必須進行驗證才能存取這些服務。
- 設定驗證強制物件 (**Auth-Finance-Servers**)，以指定驗證方法和驗證設定檔並將其新增至規則。
- 記錄活動，以便您追蹤和分析規則的違反情況，因為這些情況可能表示有人企圖發起攻擊。

STEP 2 | 驗證需要存取資料中心的承包商、合作夥伴、客戶及其他非員工群組。

此規則要求諸如承包商、合作夥伴和客戶的第三方使用者群組進行 MFA 驗證，因為相較於您自己的員工，這類公司及其人員的商業和安全性做法更難控制。要求這類使用者至少使用兩種要素進行驗證，可以保護您的資料中心，以免認證在第三方公司被竊取。



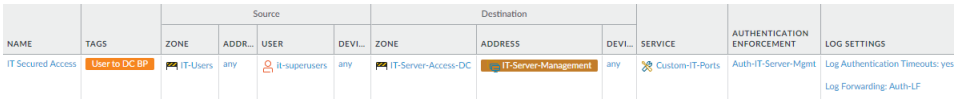
若要建立此規則：

- 將驗證規則套用至 SAP 承包商需要用於商業目的的服務。建立自訂服務群組 (**Sap-Services**) 以定義 SAP 承包商可以在其上進行驗證及新增必要服務的連接埠，此範例中為 **service-http** 和 **service-https**。
- 設定驗證強制物件 (**Auth-SAP-Servers**)，以指定驗證方法和驗證設定檔並將其新增至規則。在本例中，驗證類型必須支援 MFA，且您必須 **Add**（新增）MFA 伺服器設定檔至驗證設定檔（**Factors**（要素）頁籤）並執行設定 MFA 的其餘步驟。

  設定 MFA 驗證存取敏感系統的所有使用者和使用者群組，防止攻擊者利用竊取的認證入侵。
- 記錄活動，以便您追蹤和分析規則的違反情況，因為這些情況可能表示有人企圖發起攻擊。

STEP 3 | 驗證需要特殊存取權限的使用者，例如需要安全存取資料中心伺服器以便進行管理和維護的 IT 人員。

此規則展示了如何設定對具有特權帳戶的使用者進行驗證，而特權帳戶可以授予使用者對重要系統的管理存取權。由於洩露特權使用者的認證可讓攻擊者有權限存取您的資料中心及其寶貴資產，您必須要求使用者至少透過兩種要素進行驗證，確保只向合法使用者授予存取權限，從而防止認證被竊取。此範例展示了如何驗證 IT 使用者存取資料中心伺服器管理介面的權限。



若要建立此規則：

- 指定需要驗證才能存取資料中心伺服器管理介面的特權帳戶使用者，此範例中為 **it-superusers** 群組。
- 透過為資料中心管理介面存取請求建立動態位址群組（**IT-Server-Management** 靜態位址群組）並將其設定為目的地位址，來對其套用此使用者群組的驗證。
- 將驗證規則套用至特權 IT 人員需要用於業務目的的服務，本範例中為自訂服務群組 **Custom-IT-Ports**，其可以識別所有伺服器管理連接埠（應置於相同子網路上）。
- 設定並套用驗證強制物件（本範例中為 **Auth-IT-Server-Mgmt**），強制要求進行 MFA（雙重要素）驗證。**Add**（新增）MFA 伺服器設定檔至驗證設定檔（**Factors**（要素）頁籤）並執行設定 MFA 的其餘步驟。使用 MFA 至關重要，因為擁有特權帳戶的每位 IT 使用者都有權限存取裝置管理介面，因此您需要確定其身份。

  為進一步減少攻擊者利用竊取的認證攻擊資料中心的機會，或工作站無人值守但又未鎖定的情況，在設定 MFA 時，可為驗證要求設定驗證時間戳記。有寶貴的資料中心資產時，最好按優先次序為服務和應用程式提供保護。
- 記錄活動，以便您追蹤和分析規則的違反情況。

IT 還會管理資料中心的交換器、路由器及其他裝置。如果相同的 IT 使用者群組管理這些資源，則您可將其新增至目的地區域和位址，以便規則在 IT 超級使用者存取這些裝置的管理介面對其進行驗證。如果不同的 IT 使用者群組管理不同的資料中心資源組，則為每個使用者群組建立單獨、嚴格的安全性原則規則及對應的驗證原則和解密原則規則。

不要以明碼形式傳送認證。例如，如果您使用 *RADIUS*，則請使用支援的 EAP 方法在 TLS 內安全傳輸認證。

建立使用者至資料中心解密原則規則

為從使用者群體進入資料中心的流量建立解密原則規則，以提供可視性，以便您檢查流量並保護您最寶貴的資產。當您建立允許一組使用者（或特定使用者）存取一組資料中心伺服器的安全性原則規則時，請建立解密原則規則以解密該流量。

由於資料中心儲存著您最寶貴的資產，因此您需要解密可以解密的所有資料中心流量。開始解密進入重要伺服器的流量、高風險流量、來自可信度最低的網路段的流量（例如，優先解密來自合作夥伴、客戶或承包商等第三方的流量，而不是信任的內部網路段流量），然後繼續解密其他流量，直到對流入您所有資料中心資產的流量解密完成。解密儘可能多的流量，同時保持可接受的效能。

從資料中心解密排除不適當的流量。個人資訊的法規與合規性規則視乎國家和地區而異。不同公司的個人資訊合規規則可能有所不同。解密儘可能多的流量，但如果您的資料中心包含法規或公司規則要求免除解密的資訊，則不必解密該流量。

在建立使用者至資料中心應用程式允許規則中，我們已建立允許進行 DNS 存取的安全性政策規則，允許工程使用者存取工程開發伺服器、允許 SAP 承包商開發人員只能存取 SAP 開發伺服器，並允許一組特定的 IT 使用者進行資料中心伺服器管理存取。我們在此建立了解密原則規則（**Policies**（原則）> **Decryption**（解密））以解密這些規則允許的流量。

解密原則規則共享一些與這些流量相關的通用元素：

- 當您建立解密原則規則時，目的是解密流量，以便安全性原則規則檢查流量並根據原則允許或封鎖流量。為此，解密原則規則必須使用與類似安全性原則規則相同的來源區域和使用者，及相同的目的地區域和位址（通常由動態位址群組定義，以便您在新增或移除伺服器時，無需提交操作即可更新防火牆）。在安全性原則和解密原則中定義相同來源和目的地會將兩種原則套用至相同流量中。
- 所有這些規則的動作均為「解密」，但敏感個人資訊的情況除外，如步驟 4 所示。
- 對於每個規則，設定解密記錄和日誌轉送。請在防火牆資源允許時記錄最多的解密流量。
- 使用 SSL 輸入檢查來檢查傳入流量的解密規則需要適當的伺服器憑證。
- 所有這些解密規則都會使用建立資料中心最佳做法解密設定檔中顯示的最佳做法資料中心解密設定檔。

STEP 1 | 解密從員工使用者群組到資料中心伺服器的允許流量。

此規則展示了如何解密從使用者群組到資料中心伺服器的流量，允許該群組進行存取以提供對流量的可視性。例如，我們建立的應用程式允許規則包括允許工程使用者在資料中心存取開發伺服器的安全性政策規則。為保護開發伺服器，請解密傳入流量以便防火牆可檢查流量並套用威脅防禦設定檔。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Engg to Dev Servers	User to DC BP	Engineering-Users	api-users engg-users	Engineering-DC-Infra	Dev-Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

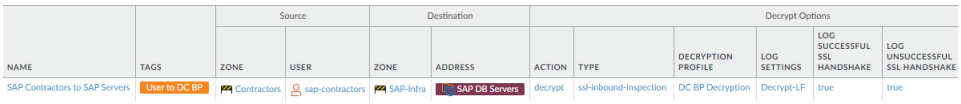
若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在本例中，來源使用者為 **Engineering-Users** 區域的 **api-users** 和 **engg-users**，目的地為 **Engineering-DC-Infra** 區域 **Dev-Servers** 動態位址群組中指定的伺服器。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Inbound Inspection**（**SSL** 輸入檢查）。為開發伺服器指定伺服器憑證，並套用資料中心最佳做法解密設定檔以對流量套用 SSL 輸入檢查和 SSL 通訊協定設定。

根據來源區域和使用者群組（或使用者）及目的地區域和伺服器區域（如動態位址群組成員資格所定義），為每個使用者群組（或個別使用者，如適用）允許的資料中心流量建立類似解密原則規則。

STEP 2 | 解密來自承包商、合作夥伴、客戶及其他第三方的允許流量。

此規則展示了如何解密從第三方群組到其允許存取的資料中心伺服器的流量。例如，允許規則包括允許 SAP 開發人員承包商在資料中心對 SAP 資料庫伺服器進行有限存取的安全性政策規則。解密傳入流量，以便防火牆檢查這些流量並對其套用威脅防禦設定檔，及保護 SAP 資料中心伺服器。



		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
SAP Contractors to SAP Servers	User to DC BP	Contractors	sap-contractors	SAP-Infra	SAP DB Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 為要解密的流量指定與類似安全性原則規則相同的來源和目的地。在本例中，來源使用者為**Contractors**（承包商）區域的 **sap-contractors** 使用者群組，目的地則為 **SAP-Infra** 區域的 **SAP DB Servers**（**SAP DB** 伺服器）動態位址群組中指定的伺服器。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Inbound Inspection**（**SSL** 輸入檢查）。為開發伺服器指定伺服器憑證，並套用資料中心最佳做法解密設定檔以對流量套用 SSL 輸入檢查和 SSL 通訊協定設定。

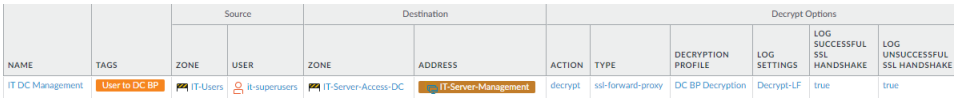
根據來源區域和使用者群組及目的地區域和伺服器區域（如動態位址群組成員資格所定義），為每個第三方群組允許的資料中心流量建立類似解密原則規則。

STEP 3 | 解密流量以允許對資料中心伺服器進行特權存取（法規或合規性規則禁止的個人資訊相關流量除外）。

此規則展示了如何為進行特權存取解密流量，因為無論您多麼任何使用者，都應該解密儘可能多的流量，以提供保護資料中心所需的可視性。如果您不解密允許的流量，將無法套用威脅防禦設定檔，且如果流量中隱藏了惡意軟體或其他威脅，您也無法看到。此範例參照我們先前建立的安全性政策允許規則，以便為 IT 超級使用者提供存取資料中心伺服器的管理介面。

如果管理和維護資料中心伺服器的 *IT* 群組使用 *SSH*，您將無法解密 *SSH* 流量。您可設定 SSH Proxy 以封鎖 *SSH* 通道並防止 *SSH* 傳輸潛在的惡意內容和應用程式。如果 *IT* 群組使用 *SSL*，則使用 *SSL* 轉送 *Proxy* 而非 *SSL* 輸入檢查來建立解密原則規則。這是因為 *SSL* 輸入檢查需要伺服器憑證才能執行解密。由於 *IT* 群組需要管理許多資料中心伺服器，因此為每個伺服器建立 *SSL* 輸入檢查規則既麻煩又難以管理。在此使用案例中，*SSL* 轉送 *Proxy* 解密更容易調整。

以下範例展示了 SSL 轉送 Proxy 使用案例的解密原則規則。



		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Management	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 為要解密的流量指定與類似安全性原則規則相同的來源和目的地。在本例中，來源使用者為 **IT-Users** 區域的 **it-superusers** 使用者群組，目的地則為 **IT-server-access-DC** 區域的 **IT-Server-Management** 靜態位址群組中指定的伺服器。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Forward Proxy**（**SSL** 轉送 **Proxy**）。套用資料中心最佳做法解密設定檔以對流量套用 SSL 轉送 Proxy 和 SSL 協定設定。

如果其他群組需要進行特權存取，則為每個群組建立類似類型的解密原則規則。

IT 還會管理資料中心的交換器、路由器及其他裝置。如果相同的 IT 使用者群組管理這些資源，則您可將其新增至目的地區域和位址，以便規則解密連線至這些裝置的管理介面的流量。如果不同的 IT 使用者群組管理不同的資料中心資源組，則為每個使用者群組建立單獨、嚴格的安全性原則規則及對應的解密和驗證原則規則。

下一個範例展示了 SSH Proxy 使用案例的解密原則規則。您也可以選擇不解密流量而使用 SSH Proxy 解密。

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
IT DC Mgmt-SSH	User to DC BP	IT-Users	it-superusers	IT-Server-Access-DC	IT-Server-Management	decrypt	ssh-proxy	DC BP Decryption	none	false	true

若要建立此規則：

- 流量來源和目的地與先前的 SSL 轉送 Proxy 使用案例範例規則相同。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSH Proxy**。套用資料中心最佳做法解密設定檔以對流量套用 SSH Proxy 和 SSL 協定設定。

  IT 人員還會管理資料中心的交換器、路由器及其他裝置。如果相同的 IT 使用者群組管理這些資源，則您可將其新增至目的地區域和位址，以便規則解密連線至這些裝置的管理介面的流量。如果不同的 IT 使用者群組管理不同的資料中心資源組，則為每個使用者群組建立單獨、嚴格的安全性原則規則及對應的解密和驗證原則規則。

STEP 4 | 如果法規或合規性規則禁止，則不要解密敏感的個人資訊。

此規則展示了當您出於法規或合規性原因需要免除流量解密時，如何建立基於原則的解密排除規則。此範例參照我們先前建立的安全性政策允許規則，以便為財務使用者提供財務伺服器存取權限。如果法則或合規性規則允許您解密此流量，則進行解密以便防火牆可以看到流量並防止威脅攻擊。

NAME	TAGS	Source		Destination		Decrypt Options					
		ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Finance PCI No Decrypt	User to DC BP	Finance-Users	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	no-decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 為要解密的流量指定與類似安全性原則規則相同的來源和目的地。在本例中，來源使用者為 **Finance-Users** 區域的 **accounting-users** 和 **finance-users**，目的地則為 **Finance-DC-Infra** 區域的 **Fin-Servers** 動態位址群組中指定的伺服器。
- 在 [Options（選項）] 頁籤上，將動作設定為 **No Decrypt**（不解密）。套用資料中心最佳做法不解密設定檔，以防止發生憑證問題。

  請不要將不解密設定檔套用至 TLSv1.3 流量，因為已加密憑證資訊，讓防火牆無法根據憑證資訊來封鎖工作階段。

定義初始網際網路至資料中心流量安全性原則

與其他資料中心流量一樣，根據應用程式允許安全性政策規則，嚴格控制從網際網路到資料中心的流量，以防使用未知或未認可的應用程式的流量進入資料中心。此外，透過將 DoS 保護原則規則（具有 DoS 保護設定檔）套用至預期送達資料中心 Web 伺服器層的外部流量，可保護資料中心 Web 伺服器免受「拒絕服務」(DoS) 攻擊。

- 網際網路至資料中心流量安全性方法
- 建立網際網路至資料中心應用程式允許規則
- 建立網際網路至資料中心 DoS 保護原則規則
- 建立網際網路至資料中心解密原則規則

網際網路至資料中心流量安全性方法

使用傳統舊方法保護從網際網路流向資料中心的資料中心流量，會使有價值的資產面臨風險，而最佳做法方法則會保護有價值的資產。流量進入資料中心的主要風險是意外地從受感染的外部伺服器下載惡意軟體，或者無意中將惡意軟體從遭入侵的資料中心伺服器放置在外部伺服器上。

傳統方法	風險	最佳做法方法
建立基本連接埠的安全性原則。	惡意應用程式透過以下方式存取網路來避免偵測：偽造連接埠號碼、透過連接埠執行通道作業或使用連接埠跳躍。	應用程式允許規則防止應用程式執行於非標準連接埠上。記錄和監控允許清單違規。 當您從基於連接埠的規則轉換到基於應用程式的規則時，請在規則庫中將基於應用程式的規則置於其將取代之基於連接埠的規則之上。為這兩種規則重設原則規則命中計數器。若流量符合基於連接埠的規則，則其原則規則命中數會增加。調整基於應用程式的規則，直至在一段時間內沒有任何流量符合基於連接埠的規則，然後移除基於連接埠的規則。
入侵防禦系統 (IPS) 通常部署為入侵偵測系統 (IDS)。	IPS 為頻內偵測以及防禦系統，而 IDS 為頻外偵測系統。將 IPS 部署為 IDS 會在來源與目的地之間的直接通訊路徑之外進行入侵偵測，因此無法進行即時防禦，威脅可能會進入資料中心。	在防火牆頻內，請使用 Palo Alto Networks App-ID、User-ID 和 Content-ID 建立嚴格控制存取權限的應用程式允許清單安全性政策。套用安全性設定檔以停止已知與新的威脅。
Web 應用程式防火牆保護資料中心綽綽有餘。	攻擊者將命令與控制 (C2) 軟體放置於遭入侵至資料中心端點，使網路更易遭受攻擊，並可能在水坑攻擊中為用戶端漏洞利用提供服務。	若要阻止攻擊者將 C2 軟體放置在資料中心端點上，只需將嚴格的反間諜軟體安全性設定檔指派給用於控制流量的安全性原則規則。此設定檔為防火牆內含的功能之一，因此套用此保護無需額外費用。

建立網際網路至資料中心應用程式允許規則

從網際網路進入資料中心之流量的最大風險是會在無意中從受感染的外部用戶端下載惡意軟體，或當用戶端在資料中心從受到攻擊的伺服器提取資料時無意中將惡意軟體置於外部伺服器上。保護從網際網路進入資料中心的流量，這樣您便不會在無意中下載利用伺服器漏洞的惡意軟體，或允許用戶端從可能感染合作夥伴、客戶，最後進入您所在行業網站的一個公司伺服器下載惡意軟體。

確保進入資料中心的流量來源不是惡意 IP 位址或其他存在潛在風險的來源，並僅出於商業目的允許必要應用程式。不允許在資料中心使用不必要（特別是未知）的應用程式。請執行以下操作：

- 建立允許規則，控制外部裝置可用於與您的資料中心通訊的認可和允許的應用程式。

  標記所有認可的應用程式，方法是採用預先定義的認可的標籤。*Panorama* 和防火牆將沒有「認可的」標籤的應用程式視為未認可的應用程式。
- 建立外部動態清單以識別不良 IP 位址並用其防止對資料中心的存取。
- 為任何專有應用程式建立自訂應用程式以便您識別應用程式並對其套用安全性原則。

  如果您有單獨用於定義一組連接埠的自訂工作階段逾時而建立的現有「應用程式定覆寫」政策，請透過設定基於服務的工作階段逾時，將現有的「應用程式覆寫」政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時，然後將規則移轉為基於應用程式的規則。「應用程式覆寫」政策以連接埠為基礎。當您使用「應用程式覆寫」政策維持一組連接埠的自訂工作階段逾時時，您會失去對那些流動的應用程式可見度，因此您不知道也無法控制由哪些應用程式使用連接埠。基於服務的工作階段逾時達到自訂逾時，同時又能維持應用程式的可見度。
- 套用最佳做法安全性設定檔群組，其包含最佳做法安全性設定檔，允許規則來防止惡意軟體、漏洞、C2 流量以及已知和未知威脅的攻擊。
- 記錄工作階段端的所有允許流量，以追蹤和分析規則違反。將日誌轉送至日誌伺服器，並在適用時，將日誌電子郵件轉送給適當的管理員。

對資料中心安全性原則規則庫進行排序向您展示如何利用我們為其他三個資料中心流量建立的所有其他規則和封鎖規則對這些規則進行排序，如此便不會有規則影響其他規則。

若要在多個資料中心之間套用一致的安全性原則，您可重複使用範本和範本堆疊，以便相同的原則適用於每個資料中心。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

僅允許廠商、承包商及客戶的認可應用程式流量進入必要應用程式。

此規則展示了如何透過嚴格控制允許的應用程式（僅允許其在預設連接埠使用），及使用外部動態清單識別已知不良 IP 位址並封鎖已知不良來源，來保護從外部來源進入資料中心的應用程式流量。

			Source				Destination							
NAME	TAGS	TYPE	ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
Web Server Inbound	Internet to DC	universal	L3-External	Bad IPs List	any	any	Web-Server-Tier-DC	Web Servers	any	Acme	application-default	Allow		

若要建立此規則：

- 防止已知不良來源試圖存取資料中心。使用安全性規則原則 **Source Address**（來源位址）中的 **Negate**（否定）選項封鎖不良 IP 位址的連線。此範例使用外部動態清單（**Bad IPs List**（不良 **IP** 清單））識別不良 IP 位址並將其封鎖。（來源位址中加刪除線的文字表示其被否定而非允許。）
- 將應用程式限制為僅用於商業目的的應用程式，並允許其僅在預設連接埠（**application-default**（應用程式預設））上執行，防止躲避型惡意軟體試圖在非標準連接埠上執行。在此範例中，廠商使用了一個叫做 **Acme** 的專有應用程式。我們建立了自訂應用程式以識別 **Acme** 專有應用程式，以便防火牆對流量進行分類並套用適當的安全性原則。
- 將 **Acme** 應用程式流量的目的地限制為 **Web-Server-Tier-DC** 區域的 **Web-Servers** 動態位址群組。如果目的地位址未在 Web 伺服器層中，防火牆將丟棄流量。

透過檢視預先定義的應用程式報告確認僅您在安全性政策規則中明確允許的應用程式正在執行（**Monitor**（監控）> **Reports**（報告）> **Application Reports**（應用程式報告）> **Applications**（應用程

式））。如果您在報告中看到意外的應用程式，請檢閱應用程式允許規則並對其進行細化，使其不允許出現意外的應用程式。

建立網際網路至資料中心解密原則規則

建立解密原則規則以提供對從網際網路進入資料中心的流量之可視性，以便您套用安全性原則至該流量。當您建立允許存取一組資料中心伺服器的安全性原則規則時，請建立解密原則規則以解密該流量。在建立網際網路至資料中心應用程式允許規則中，我們已建立安全性政策規則，允許僅使用允許的應用程式存取從網際網路進入資料中心 Web 伺服器層的流量。我們在此建立解密政策規則（**Policies**（政策）> **Decryption**（解密））以解密此規則允許的流量。

為解密流量以便安全性原則規則根據原則檢查並允許或封鎖該流量，解密原則規則必須使用與類似安全性原則規則相同的來源區域和使用者，及相同的目的地區域和位址（通常由動態位址群組定義，以便您在新增或移除伺服器時，無需提交操作即可更新防火牆）。在安全性原則和解密原則中定義相同來源和目的地會將兩種原則套用至相同流量中。

解密規則會使用建立資料中心最佳做法解密設定檔中顯示的最佳做法資料中心解密設定檔。

對於每個規則，設定解密記錄和日誌轉送。請在防火牆資源允許時記錄最多的解密流量。

STEP 1 | 解密從網際網路進入資料中心 Web 伺服器的允許流量。

此規則展示了如何解密從外部建立的連線進入資料中心的流量。例如，我們建立的應用程式允許規則允許外部流量僅使用某些應用程式存取資料中心 Web 伺服器。為保護資料中心 Web 伺服器，請解密流量以便防火牆可檢查流量並套用威脅防禦設定檔。

		Source		Destination		Decrypt Options					
NAME	TAGS	ZONE	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Internet to DC	Internet to DC BP	L3-External	any	Web-Server-Tier-DC	Web Servers	decrypt	ssl-inbound-inspection	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在本例中，來源為 **L3-External** 區域，目的地為 **Web-Server-Tier-DC** 區域的 **Web-Servers** 動態位址群組中指定的伺服器。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Inbound Inspection**（**SSL** 輸入檢查）。為 Web 伺服器指定伺服器憑證，並套用資料中心最佳做法解密設定檔以對流量套用 SSL 輸入檢查和 SSL 通訊協定設定。

STEP 2 | 若允許進行此類存取，或針對您允許的其他應用程式，為從網際網路進入任何其他伺服器群組的流量建立類似解密原則規則。

建立網際網路至資料中心 DoS 保護原則規則

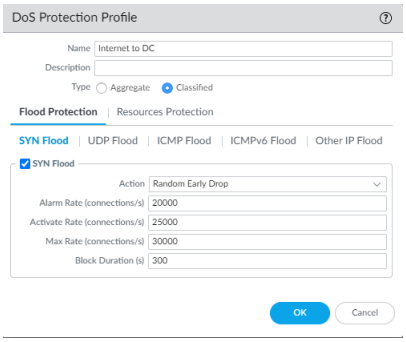
攻擊者用於破壞網路的一種方法是阻斷服務 (DoS) 攻擊，其目的是摧毀連線至網際網路的目標系統，使其癱瘓，並使所有合法使用者和服務無法使用這些系統。資料中心 Web 伺服器是一個極具吸引力的目標，因為破壞了它可阻止大部分對資料中心的合法存取。

透過將分類 DoS 保護原則套用到流向這些伺服器的網際網路流量，來保護資料中心 Web 伺服器層。分類 DoS 保護原則會將控制傳入連線數量的分類 DoS 保護設定檔套用到在此原則中定義的流量。

此外，為每個區域設定封包緩衝區保護，以保護防火牆免受單一工作階段 DOS 攻擊，此類攻擊可摧毀防火牆的封包緩衝區並導致合法流量丟失，特別是在保護重要服務的防火牆上。

STEP 1 | 建立分類 DoS 保護設定檔，透過限制每秒連線數來防止 SYN 洪水攻擊，從而保護資料中心 Web 伺服器免受 DoS 攻擊。

此 DoS 保護設定檔可限制您附加設定檔的 DoS 保護原則規則中所定義流量的每秒連線數 (CPS)，以防止 DoS 攻擊破壞您的 Web 伺服器。設定檔設定了漸進式 CPS 閾值，以提醒您，啟動隨時早期丟棄 (RED) 封包丟棄，並封鎖新連線，同時作為封鎖新連線的持續時間。您為保護資料中心 Web 伺服器而設定的 CPS 閾值取決於 Web 伺服器的容量。



若要建立此設定檔：

- 在 **Objects**（物件）> **Security Profiles**（安全性設定檔）> **DoS Protection**（**DoS** 保護）中，**Add**（新增）分類的 DoS 保護設定檔。
- 為設定檔 **Name**（命名）、選取 **Classified**（分類）作為設定檔 **Type**（類型）、將 CPS 值設定為警報（**Alarm Rate**（警報率））、啟動 RED（**Activate Rate**（啟動率））、開始封鎖新工作階段（**Max Rate**（最大速率））（然後設定當 CPS 速率達到（**Max Rate**（最大速率））閾值時封鎖新工作階段（**Block Duration**（封鎖期間）的時間（秒）。

如果您未使用 *UDP* 或其他 *IP* 通訊協定，可將您想要封鎖之通訊協定的流量保護 *CPS* 設定為零封包，使用安全性政策規則組合以允許應用程式，並使用區域保護設定檔封鎖未使用的通訊協定，從而進行限制。

STEP 2 | 建立分類 DoS 保護原則規則，以定義您想要保護的伺服器，使其免受 DoS 攻擊，並對其附加 DoS 保護設定檔。

此規則可防止 SYN 洪水攻擊破壞您的資料中心 Web 伺服器層。此範例將分類 DoS 保護設定檔套用到允許連線至 Web 伺服器層的外部流量。

NAME	TAGS	Source			Destination		SERVICE	ACTION	Protection		LOG FORWARDING
		ZONE/INTERFACE	ADDRESS	USER	ZONE/INTERFACE	ADDRESS			AGGREGATE	CLASSIFIED	
DC Web Server Protection	Internet to DC BP	L3-External	~~Bad IPs List~~	any	Web-Server-Tier-DC	Web Servers	service-http service-https	protect	none	profile: Internet to DC destination-ip-only	DoS-LF

若要建立此規則：

- 若要將 DoS 保護套用到流入 Web 伺服器層的流量，DoS 保護原則必須套用至與允許流量之安全性原則規則相同的流量。在本範例中，此 DoS 規則可保護我們在建立網際網路至資料中心應用程式允許規則中允許的流量。
- 在 [Option/Protection（選項/保護）] 頁籤上，指定網頁服務（**service-http** 和 **service-https**），將動作設定為 **protect**（保護）以將 DoS 保護設定檔的 SYN 洪水閾值套用至流量、設定日誌轉送方法（假設您已設定日誌轉送），並選取我們在先前步驟（**Internet to DC**（網際網路至 **DC**））為流量設定的分類 DoS 保護設定檔。

若要防止外部來源的 SYN 洪水攻擊，請建立單獨的 DoS 保護原則規則，將您的內部區域指定為來源區域，而不是 **L3-External**。為外部和內部攻擊來源建立單獨的規則可提供單獨報告，從而讓調查攻擊嘗試變得更容易。

定義初始資料中心至網際網路流量安全性原則

根據資料中心架構，資料中心中的伺服器可能會存取網際網路，以擷取軟體更新或檢查伺服器憑證撤銷狀態。安全性計劃通常著重於使用者通訊，而忽略了與網際網路進行通訊的伺服器，因此資料中心為攻擊者絕佳的隱身之地。當資料中心伺服器啟動與網際網路進行直接通訊時，您需要防禦以下幾種安全性風險：

- 資料外洩—攻擊者使用合法應用程式（如 FTP 或 HTTP）或其他方法（如 DNS 通道作業）來竊取資料。建立應用程式安全性政策規則允許清單，僅允許伺服器更新所需的應用程式，從而封鎖所有其他應用程式，即使它們在其他情況下是合法應用程式亦是如此。寬鬆的應用程式規則讓攻擊者有機可乘。
- 使用合法應用程式的命令與控制 **(C2)**—若允許資料中心伺服器使用不用於軟體更新之合法應用程式與網際網路進行通訊，則攻擊者可以使用這些合法應用程式進行 C2 活動。例如，允許非標準連接埠上的 Web 瀏覽為攻擊者創造機會。僅允許伺服器在其預設連接埠上僅使用軟體更新所需的特定應用程式來與網際網路進行通訊，而不是使用其他應用程式，即使這些應用程式合法且被批准用於其他用途亦是如此。
- 下載其他惡意軟體—若攻擊者入侵資料中心伺服器，伺服器上的惡意軟體可能會透過回撥或其他機制從網際網路中下載更多惡意軟體。嚴格的允許規則允許僅使用必要的更新應用程式僅與相應的更新伺服器進行通訊，可防止攻擊者接觸包含惡意軟體的網站以及洩漏資料。此外，在資料中心伺服器（和所有端點）上安裝 Cortex XDR 代理程式，防止執行已存留在伺服器上的惡意軟體。

資料中心至網際網路流量安全性方法

採用傳統舊方法保護流向網際網路的資料中心流量，會使有價值的資產面臨風險，而最佳做法方法則會保護有價值的資產。

傳統方法	風險	最佳做法方法
建立基於連接埠的規則及/或基於 IP 的規則，可在受信任網路中提供足夠的安全性。	基於連接埠的規則及基於 IP 的規則無法控制可允許連接至網際網路的應用程式。若連接埠已開啟，則所有應用程式均可使用該連接埠。	建立嚴格的基於應用程式的允許規則，僅允許擷取更新的資料中心伺服器僅使用合法應用程式，從而僅與合法的更新伺服器進行通訊。記錄和監控允許規則違規。 當您從基於連接埠的規則轉換到基於應用程式的規則時，請在規則庫中將基於應用程式的規則置於其將取代之基於連接埠的規則之上。為這兩種規則重設原則規則命中計數器。若流量符合基於連接埠的規則，則其原則規則命中數會增加。調整基於應用程式的規則，直至在一段時間內沒有任何流量符合基於連接埠的規則，然後移除基於連接埠的規則。
資料中心伺服器僅存取受信任伺服器（如更新伺服器），因此無需解密該流量。	已存在於資料中心的惡意軟體或命令和控制軟體，可能會嘗試與外部伺服器進行通訊，以下載更多的惡意軟體或洩漏資料。	解密從資料中心到網際網路的所有流量。建立自訂 URL 類別，可定義允許資料中心伺服器在安全性原則內接觸並使用的 URL，以限制對外部伺

傳統方法	風險	最佳做法方法
		服器的網際網路存取。使用解密原則內相同自訂 URL 來解密流向這些外部伺服器的流量。
混用封鎖及警示來自多個供應商的威脅防禦設定檔。	個別工具的結合為攻擊者留下了安全性漏洞，可能無法很好地協同工作。	Palo Alto Networks 協同安全性工具套件協同工作，可以堵住安全性漏洞並防止攻擊。

建立資料中心至網際網路應用程式允許規則

資料中心伺服器啟動到網際網路上外部伺服器之連線的主要使用案例是更新軟體或取得憑證狀態。最大的風險是連線至錯誤的伺服器，特別是對於 Linux 更新，因為您可能無意中連線至很多第三方 URL。確保您的資料中心伺服器僅使用其預設連接埠上的必要應用程式，從合法的更新伺服器接收更新。

為此，請建立嚴格的應用程式允許規則，限制資料中心伺服器將連線至的外部伺服器和資料中心伺服器在連線至外部伺服器時使用的應用程式。標記所有認可的應用程式，方法是採用預先定義的認可的標籤。（Panorama 和防火牆將不帶「認可」標籤的應用程式視為未經認可的應用程式。）嚴格的應用程式允許規則集透過下列方式破壞潛在的攻擊：

- 防止已在資料中心伺服器上的惡意軟體連線至遭受入侵的外部伺服器（背景連線通訊）及下載額外資料，因為允許規則不允許連線至這類伺服器。
- 防止攻擊者使用合法應用程式（如 FTP、HTTP 或 DNS 閘道）竊取資料，或使用合法應用程式（如非標準連接埠上的網頁瀏覽）進行命令與控制 (C2) 操作，因為允許規則不允許資料中心伺服器使用這類應用程式與網際網路通訊。另一種防止資料洩露的方法是使用檔案封鎖設定檔的 **Direction**（方向）控制來封鎖輸出更新檔案，這樣您僅可下載軟體更新檔案。

為需要不同外部伺服器組軟體更新的應用程式建立嚴格的允許規則。在許多情況下，僅使用 App-ID 不足以保護資料中心伺服器。例如，對於 Linux 伺服器更新，僅將流量限制到 *yum* 或 *apt-get* 等更新應用程式是不夠的，因為這並不能防止連線至非法伺服器。最佳做法是找到資料中心伺服器需要連線的 URL，建立指定要使用的網站的自訂 URL 類別（**Objects**（物件）> **Custom Objects**（自訂物件）> **URL Category**（**URL** 類別）），並將其與安全性原則規則中的 App-ID 相結合。透過防止使用非法應用程式與防止連線至不在自訂 URL 類別中的更新伺服器，App-ID 與自訂 URL 類別的結合將鎖定資料中心伺服器可與之連線的外部伺服器。例如，在允許資料中心伺服器連線至 CentOS 更新伺服器的安全性原則規則中，您可建立叫做 *CentOS-Update-Servers* 的自訂 URL 類別並新增伺服器使用的 CentOS 更新站點至此自訂類別。

若要找到合法 *Linux* 更新伺服器及其他更新伺服器的 *URL*，請與軟體工程、開發運營及更新軟體的其他群組合作，瞭解其取得更新的位置。您還可記錄網頁瀏覽工作階段，收集開發人員連線的 *URL*，然後將 *URL* 帶入工程中以篩選適合安全性原則的 *URL*。

不要在與網際網路通訊的資料中心伺服器的安全性原則規則中使用 *URL* 篩選設定檔（*PAN-DB URL* 篩選），因為您不會希望允許所有更新伺服器。限制通訊，使資料中心伺服器僅可連線至其擷取更新的特定伺服器。

此外，所有允許的通訊應在每個應用程式的標準連接埠上進行。任何應用程式都不得在非標準連接埠上執行。與所有資料中心流量一樣，需要監控允許規則違規行為，因為違規行為表示您需要更新安全性政策以允許合法流量或攻擊者已進入或正在嘗試進入網路。

對資料中心安全性原則規則庫進行排序向您展示如何利用我們為其他三個資料中心流量建立的所有其他規則和封鎖規則對這些規則進行排序，如此便不會有規則影響其他規則。

若要在多個資料中心之間套用一致的安全性原則，您可重複使用範本和範本堆疊，以便相同的原則適用於每個資料中心。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

下列所有允許規則：

- 附加最佳做法安全性設定檔群組，其包含最佳做法安全性設定檔。使用安全性設定檔群組可讓您一次將所有最佳做法設定檔都套用至規則，而不是個別指定每個設定檔。安全性設定檔群組會更快速且更輕鬆地設定防止惡意軟體、漏洞、C2 流量以及已知和未知威脅的攻擊。
- 記錄流量（在工作階段端），讓您可以追蹤和分析規則違規，以及包含日誌轉送。將日誌轉送至日誌伺服器，並在適用時，將日誌電子郵件轉送給適當的管理員。

STEP 1 | 允許資料中心伺服器存取軟體更新伺服器。

此規則展示了如何限制對網際網路上軟體更新伺服器的存取，以便資料中心伺服器僅與合法、已知的伺服器通訊，而不與其他外部更新伺服器通訊。此範例允許工程資料中心伺服器存取 CentOS 更新伺服器並限制通訊，以僅使用必要的應用程式建立僅到合適更新伺服器組的連線。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
CentOS Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		

若要建立此規則：

- 將 CentOS 更新請求的來源限制為需要擷取更新的資料中心伺服器，在此範例中即為 **Engineering-DC-Infra** 區域的 **Dev-Servers** 動態位址群組。
- 將資料中心伺服器可用於與外部更新伺服器進行通訊的應用程式限制為必要應用程式，在此範例中即為用於 CentOS 更新的 **yum**。僅允許應用程式在預設連接埠上執行，防止躲避型惡意軟體試圖使用非標準連接埠。
- 建立自訂 URL 類別以定義資料中心伺服器可連線的更新伺服器之 URL。在此範例中，**CentOS-Update-Servers** 自訂 URL 類別定義了資料中心伺服器可連線的更新伺服器 URL。

透過結合這些限制，還可以防止已入侵資料中心伺服器的攻擊者攻擊其他目的地及使用其他應用程式竊取資料或下載其他惡意軟體。

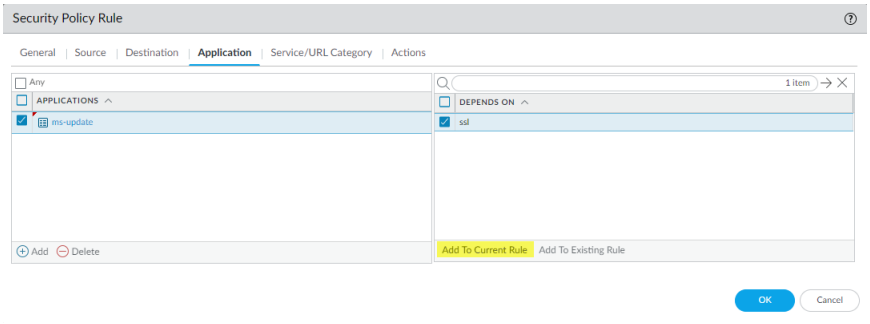
同樣地，允許相同伺服器與 Microsoft Windows 更新伺服器通訊的規則將使用相同結構。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
Windows Update	DC to Internet BP	universal	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		

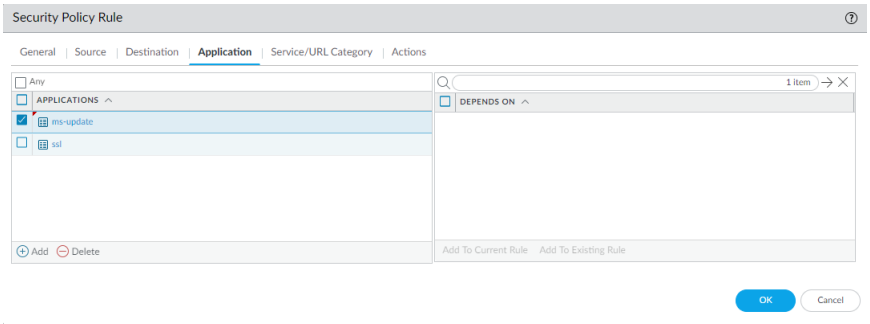
來源區域和位址與先前的 CentOS 更新規則相同。區別在於：

- 自訂 URL 類別 (**Win-Update-Servers**) 包含 Windows 更新的 URL，因此與其他 URL 的聯絡將被拒絕。
- 應用程式與 Microsoft 更新有關。除 **ms-update** 應用程式外，Microsoft 更新還需要 **ssl** 應用程式，因為 ms-update 須基於 SSL 執行。與 CentOS 更新規則一樣，僅標準連接埠有效。

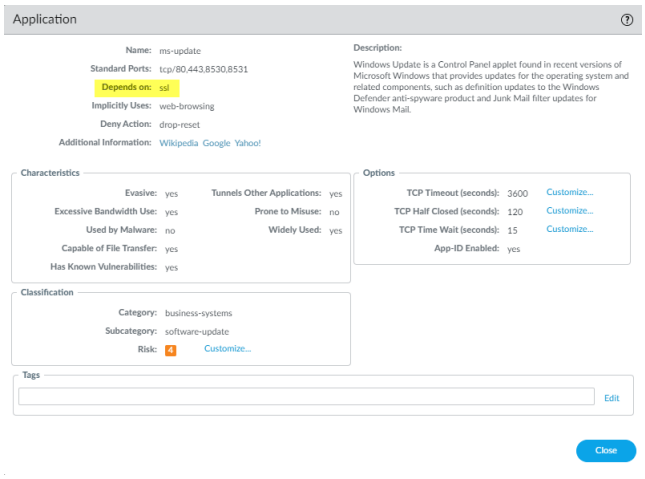
  部分應用程式取決於其他應用程式。對於指定應用程式，您必須允許所有依賴的應用程式，否則此應用程式將無法運作。當您建立安全性政策規則時，使用者介面會顯示應用程式相依項。例如，當您在規則中指定 ms-update 應用程式時，此介面會顯示 ms-update 取決於也允許 SSL：



按一下 **Add to Current Rule**（新增至目前規則），以將選取的應用程式新增至規則。



您也可以使用搜尋功能（*Objects*（物件）> *Applications*（應用程式））以找到應用程式相依性。例如，若要找到 *ms-update* 應用程式的相依性，請搜尋 *ms-update*，並按一下所產生應用程式清單中的 *ms-update* 應用程式，然後檢查 *Depends on:*（取決於：）欄位。



STEP 2 | 允許資料中心伺服器存取 DNS 和 NTP 更新伺服器。

此規則展示了如何限制對網際網路上 DNS 和 NTP 更新伺服器的存取，以便資料中心伺服器僅與合法、已知的伺服器通訊。此範例允許 IT 資料中心伺服器存取 DNS 和 NTP 更新伺服器並限制通訊，以僅使用必要的應用程式建立僅到合適更新伺服器組的連線。

NAME	TAGS	TYPE	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
NTP DNS Update	DC to Internet BP	universal	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		

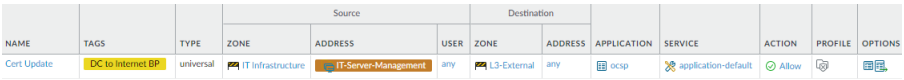
若要建立此規則：

- 將 DNS 和 NTP 更新請求的來源限制為需要擷取更新的資料中心伺服器，在此範例中即為 **Engineering-DC-Infra** 區域的 **DNS-NTP-Servers** 動態位址群組。
- 將資料中心伺服器可用於與這些外部更新伺服器進行通訊的應用程式限制為必要應用程式，在此範例中即為 **dns** 和 **ntp**。允許應用程式僅在預設連接埠上執行，防止躲避型惡意軟體試圖使用非標準連接埠。
- 建立自訂 URL 類別以定義資料中心伺服器可連線的更新伺服器之 URL。在此範例中，**NTP-DNS-Update-Servers** 自訂 URL 類別定義了資料中心伺服器可連線的更新伺服器 URL。

STEP 3 | 允許資料中心伺服器存取憑證授權伺服器，以取得數位憑證的撤銷狀態並確保其有效。

此規則將使資料中心伺服器連線至網際網路上的線上憑證狀態協定 (OCSP) 回應程式（伺服器）以檢查驗證憑證的撤銷狀態。與瀏覽器憑證撤銷清單 (CRL) 更新相比，OCSP 回應程式提供了最新的憑證狀態，而

前者依賴於 CRL 瀏覽器更新的頻率來瞭解憑證撤銷狀態，因此 CRL 比 OCSP 回應程式更容易過時。當您在防火牆上設定憑證設定檔時，可以將 CRL 狀態驗證設定為 OCSP 的遞補方法，以防 OCSP 回應程式執行不到。



若要建立此規則：

- 將憑證撤銷檢查請求的來源限制為需要檢查憑證驗證的資料中心伺服器，在此範例中即為 **IT-Infrastructure** 區域的 **IT-Server-Management** 動態位址群組。
- 將資料中心伺服器可用於與外部憑證撤銷伺服器進行通訊的應用程式限制為必要應用程式。此範例確保了資料中心伺服器與 OCSP 回應程式之間的連線，因此唯一需要指定的應用程式是 **ocsp**。允許應用程式僅在預設連接埠上執行，防止躲避型惡意軟體試圖使用非標準連接埠。

透過檢視預先定義的應用程式報告確認僅您在安全性政策規則中明確允許的應用程式正在執行（**Monitor**（監控）> **Reports**（報告）> **Application Reports**（應用程式報告）> **Applications**（應用程式））。如果您在報告中看到意外的應用程式，請檢閱應用程式允許規則並對其進行細化，使其不允許出現意外的應用程式。

建立資料中心至網際網路解密原則規則

建立解密原則規則以提供從資料中心伺服器傳送至網際網路的流量之可視性。解密從資料中心伺服器傳送至網際網路的所有流量。從資料中心內部建立到網際網路之連線的唯一帳戶是服務帳戶，且這些流量中的大部分都與軟體更新有關，因此無需考慮隱私問題。解密和檢查流量非常重要，因為如果更新伺服器受到攻擊，資料中心伺服器可下載惡意軟體並透過軟體更新程序進行傳播。檢查流量並套用最佳做法威脅防禦設定檔可保護您的資料中心不受惡意軟體攻擊，否則可以使用合法應用程式從合法更新伺服器下載惡意軟體。

在建立資料中心至網際網路應用程式允許規則中，我們已建立允許資料中心伺服器與網際網路更新伺服器建立連線的安全性政策規則，以更新作業系統軟體、DNS、NTP，以及檢查憑證。我們在此建立了類似的解密原則規則以解密更新安全性原則規則允許的流量。

不要解密轉送至憑證撤銷伺服器（線上回應程式）的流量。線上憑證狀態協定 *(OCSP)* 流量通常使用 *HTTP*，因此流量為未加密的明碼。此外，*SSL* 轉送 *Proxy* 解密可能會使更新程序中斷，因為防火牆充當中間人 *Proxy*，並會用 *Proxy* 憑證取代用戶端憑證，而 *OCSP* 回應程式可能不接受。

解密原則規則共享一些與這些流量相關的通用元素：

- 當您建立解密原則規則時，目的是解密流量，以便安全性原則規則檢查流量並根據原則允許或封鎖流量。為此，解密原則規則必須使用與類似安全性原則規則相同的來源區域和使用者，及相同的目的地區域和位址（通常由動態位址群組定義，以便您在新增或移除伺服器時，無需提交操作即可更新防火牆）。在安全性原則和解密原則中定義相同來源和目的地會將兩種原則套用至相同流量中。
- 所有這些規則的動作動作均會解密。
- 對於每個規則，設定解密記錄和日誌轉送。請在防火牆資源允許時記錄最多的解密流量。
- 所有這些解密規則都會使用建立資料中心最佳做法解密設定檔中顯示的最佳做法資料中心解密設定檔。

在許多情況下，解密原則規則範例包括自訂 URL 類別（**Objects**（物件）> **Custom Objects**（自訂物件）> **URL Category**（**URL** 類別））以縮小解密流量的範圍。每個解密原則規則皆使用與類似安全性原則規則相同的自訂 URL 類別（及來源和目的地），以便將解密和安全性原則套用至完全相同的流量中。App-ID 與自訂 URL 類別的組合使防火牆只能解密規則所允許的流量，而不解密防火牆將封鎖的流量，從而可縮短處理週期。（解密必須在安全性原則規則評估之前進行。）

STEP 1 | 解密資料中心伺服器與網際網路上軟體更新伺服器之間的流量。

此規則展示了如何解密資料中心伺服器軟體更新流量，以洞察網際網路更新伺服器上可能存在的威脅，以便防火牆進行封鎖。此範例根據我們已在建立資料中心至網際網路應用程式允許規則中建立的類似應用程式允許規則，來解密資料中心伺服器與網際網路上 CentOS 更新伺服器之間允許的流量。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
CentOS Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	CentOS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在本例中，來源為 **Engineering-DC-Infra** 區域的 **Dev-Servers** 動態位址群組，目的地為網際網路（**L3-External** 區域）。
- 指定與類似安全性政策規則中相同的自訂 URL 類別 (**CentOS-Update-Servers**) 以將目的地範圍縮小到僅限規則允許的流量，這樣防火牆便不會浪費時間解密其將丟棄的流量。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Forward Proxy**（**SSL** 轉送 **Proxy**）。套用資料中心最佳做法解密設定檔以對流量套用 SSL 轉送 Proxy 和 SSL 協定設定。

基於相同的來源和目的地及相同的自訂 URL 類別，為需要連線至網際網路更新伺服器的每組資料中心伺服器允許的資料中心流量，建立與類似安全性原則規則類似的解密原則規則。例如，基於類似安全性原則規則，需要與 Microsoft Windows 更新伺服器通訊的資料中心伺服器之解密原則規則如下所示：

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Win Update Decrypt	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	L3-External	any	Win-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

STEP 2 | 解密資料中心伺服器與網際網路上 NTP 和 DNS 更新伺服器之間的流量。

此規則展示了如何解密資料中心伺服器 NTP 和 DNS 更新流量，以洞察這些網際網路伺服器上可能存在的威脅，以便防火牆進行封鎖。此範例會根據我們在建立資料中心至網際網路應用程式允許規則中建立的類似應用程式允許規則，來解密允許的流量。

		Source		Destination			Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	ZONE	ADDRESS	URL CATEGORY	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
DNS-NTP Update Decrypt	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	L3-External	any	NTP-DNS-Update-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在本例中，來源為 **IT Infrastructure**（**IT** 基礎結構）區域的 **DNS-NTP-Servers** 動態位址群組，而目的地為網際網路（**L3-External** 區域）。
- 指定與類似安全性政策規則中相同的自訂 URL 類別 (**NTP-DNS-Update-Servers**) 以將目的地範圍縮小到僅限規則允許的流量。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Forward Proxy**（**SSL** 轉送 **Proxy**）。套用資料中心最佳做法解密設定檔以對流量套用 SSL 轉送 Proxy 和 SSL 協定設定。

定義初始內部資料中心流量安全性原則

資料中心內的流量在資料中心伺服器與各個應用程式層之間流動。您可以認為資料中心周邊內的所有內容皆受信任，因此無需檢查該流量。然而，若攻擊者入侵資料中心伺服器，且各個應用程式層之間的流量不通過防火牆，則攻擊者可透過資料中心橫向移至重要的伺服器，下載更多的惡意軟體，改變伺服器用途以及使用資料中心之外的合法應用程式洩漏資料，就像過去幾年發生的幾起重大外洩事件一樣。

防止惡意軟體在資料中心內獲得立足點的最佳措施是，使用嚴格的特定應用程式允許規則來保護流量，並使用放置在各個應用程式層之間的新世代防火牆來檢查流量。

此外，不允許資料中心內存在不明應用程式。不明應用程式可能指示攻擊者已獲得資料中心的存取權限。為專有內部應用程式建立自訂應用程式，使您可以用 App-ID 加以識別，並將安全性套用至該流量。若未為專有應用程式建立自訂應用程式，則防火牆會將其視為不明的 TCP 流量或不明的 UDP 流量。問題在於，防火牆會以與處理其他不明應用程式相同的方式處理專有應用程式，您應該封鎖不明應用程式，因為它們可能是攻擊者的工具。如果您允許資料中心內存在不明應用程式，則您可能會將資產王國的金鑰交給攻擊者。

對於不明的商業應用程式，您可以向 *Palo Alto Networks* 提交要求來建立 *App-ID*。

如果您有單獨用於定義一組連接埠的自訂工作階段逾時而建立的現有「應用程式定覆寫」政策，請透過設定基於服務的工作階段逾時，將現有的「應用程式覆寫」政策轉換為基於應用程式的政策，以維持每個應用程訂的自訂逾時，然後將規則移轉為基於應用程式的規則。「應用程式覆寫」政策以連接埠為基礎。當您使用「應用程式覆寫」政策維持一組連接埠的自訂工作階段逾時時，您會失去對那些流動的應用程式可見度，因此您不知道也無法控制由哪些應用程式使用連接埠。基於服務的工作階段逾時達到自訂逾時，同時又能維持應用程式的可見度。

- 內部資料中心流量安全性方法
- 建立內部資料中心應用程式允許規則
- 建立內部資料中心解密原則規則

內部資料中心流量安全性方法

使用傳統舊方法保護資料中心伺服器之間的東西向流量，會使有價值的資產面臨風險，而最佳做法方法則會保護有價值的資產。

傳統方法	風險	最佳做法方法
您無需分割未跨資料中心周邊的流量，因此應用程式層之間的流量也無需通過安全性基礎結構。	入侵任何資料中心伺服器的攻擊者，可以橫向移動至重要的資料中心伺服器並將其用途轉變。資料中心內的攻擊者可隨意移動，而無需擔心被發現。	使用嚴格的允許規則分割應用程式層之間的流量，可避免不必要的通訊、減少攻擊面，並有助於防止攻擊者在資料中心內橫向移動。記錄和監控允許清單違規。
資料中心在信任網路內是安全的，因此並不急於快速修補資料中心伺服器。	漏洞的開放時間更長，並向攻擊者提供攻擊載體。	及時在資料中心伺服器上安裝修補程式以關閉漏洞。建立允許清單安全性政策規則可協助您瞭解資料中心內的執行內容，以及未修補服務的執行位置。
混用封鎖及警示來自多個供應商的威脅防禦設定檔。	個別工具的結合為攻擊者留下了安全性漏洞，可能無法很好地協同工作。	Palo Alto Networks 協同安全性工具套件協同工作，可以堵住安全性漏洞並防止攻擊，以及識別試圖在

傳統方法	風險	最佳做法方法
		資料中心伺服器之間傳播的不明惡意軟體。

此外：

- 為每種功能建立唯一的服務帳戶。例如，只允許特定的服務帳戶複製交換郵箱，只允許 Web 伺服器上的特定服務帳戶查詢 MySQL 資料庫。請勿將一個服務帳戶用於兩種功能。
- 監控服務帳戶。
- 請勿允許資料中心內的一般使用者帳戶。

當您從基於連接埠的規則轉換到基於應用程式的規則時，請在規則庫中將基於應用程式的規則置於其將取代之基於連接埠的規則之上。為這兩種規則重設原則規則命中計數器。若流量符合基於連接埠的規則，則其原則規則命中數會增加。調整基於應用程式的規則，直至在一段時間內沒有任何流量符合基於連接埠的規則，然後移除基於連接埠的規則。

建立內部資料中心應用程式允許規則

資料中心流量通常由多層應用程式流量組成，其在不同伺服器層之間流動，為 SharePoint、WordPress、內部專有應用程式等應用程式提供服務。最常見的多層應用程式架構包含 Web 伺服器（表現層）、應用程式伺服器（應用程式層）和資料庫伺服器（資料層）。建立資料中心分割策略提供了如何在應用程式層之間部署防火牆及如何分割資料中心的指南。

資料中心伺服器之間流量的處理方式取決於流量。對於大部分應用程式流量，將威脅防護設定檔新增至安全性政策允許規則以檢查流量。例如，始終套用最佳做法安全性設定檔來保護財務應用程式、工程開發應用程式等的 Web、應用程式及伺服器層之間的流量。套用威脅防禦設定檔的例外情況是高容量、低價值應用程式的流量，如信箱複製和備份流量。您仍然允許存取這些應用程式，但因為防火牆在複製之前已經檢查流量，所以套用威脅防禦設定檔會消耗防火牆 CPU 週期，而不會提供額外價值。

WildFire 安全性設定檔可以識別試圖在資料中心伺服器之間傳播的未知惡意軟體，透過在惡意軟體未造成任何損害之前發現它來防止資料洩露。如果您無法使用 WildFire 全域雲端，可部署 WildFire 私人雲端或 WildFire 混合雲端。

本節中的範例安全性政策規則顯示如何允許需要使用 Web 伺服器、應用程式伺服器和資料庫伺服器層的多層資料中心財務應用程式的流量，以便為這些應用程式提供服務。範例包括兩個我們為其建立了自訂應用程式的專有內部應用程式：**Billing-App** 和 **Payment-App**。為這些應用程式建立自訂 App-ID 可讓防火牆能夠識別它們，控制它們，並對其套用安全性原則。不要在資料中心允許未知應用程式，因為您無法識別這些應用程式及對其套用安全性原則，且其可能表示您的資料中心有攻擊者入侵。每個資料中心應用程式都應具有 App-ID。

僅允許應用程式在其標準（*application-default*（應用程式預設值））連接埠上執行。在某些情況下，業務需求可能要求您進行例外處理，允許應用程式在特定用戶端與伺服器之間使用非標準連接埠。在這些情況下，請注意在非標準連接埠上執行的應用程式流量，並確保您知道在非標準連接埠上執行的應用程式的每個實例。在非標準連接埠上執行的應用程式，如果您未將其列為明確（已知）的例外情況，則表明可能存在躲避型惡意軟體。

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

對資料中心安全性原則規則庫進行排序向您展示如何利用我們為其他三個資料中心流量建立的所有其他規則和封鎖規則對這些規則進行排序，如此便不會有規則影響其他規則。

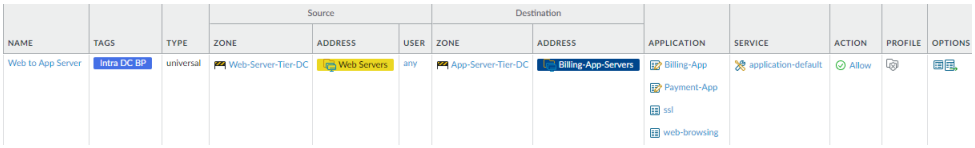
若要在多個資料中心之間套用一致的安全性原則，您可重複使用範本和範本堆疊，以便相同的原則適用於每個資料中心。範本使用變數以套用特定裝置的值，例如 *IP* 位址、*FQDN* 等，同時維持一個全域安全性政策並減少您需要管理的範本和範本堆疊的數目。

下列所有允許規則：

- 附加最佳做法安全性設定檔群組，其包含最佳做法安全性設定檔。使用安全性設定檔群組可讓您一次將所有最佳做法設定檔都套用至規則，而不是個別指定每個設定檔。安全性設定檔群組會更快速且更輕鬆地設定防止惡意軟體、漏洞、C2 流量以及已知和未知威脅的攻擊。
- 記錄流量（在工作階段端），讓您可以追蹤和分析規則違規，以及包含日誌轉送。將日誌轉送至日誌伺服器，並在適用時，將日誌電子郵件轉送給適當的管理員。

STEP 1 | 允許 Web 伺服器層和應用程式伺服器層之間的財務應用程式流量。

此規則限制了可以在財務部帳單伺服器的 Web 伺服器層和應用程式伺服器層之間流動的流量，以便只有使用合法應用程式的流量才能存取帳單伺服器。（當我們建立使用者至資料中心應用程式允許規則時，還建立了規則來限制財務使用者對資料中心的存取，以便只有適當的財務使用者才能存取資料中心。）該規則使用動態位址群組來指定每個應用程式層中的伺服器—**Web-Servers** 指定 Web 伺服器層中的伺服器位址，**Billing-App-Servers** 指定財務帳單應用程式伺服器層中的伺服器位址。



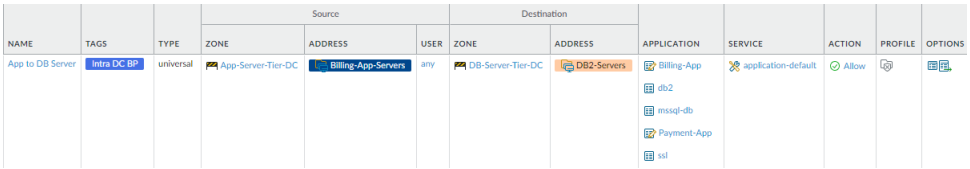
若要建立此規則：

- 將財務應用程式流量的來源限制在 **Web-Server-Tier-DC** 區域的 Web 伺服器 (**Web-Servers**)。
- 將財務應用程式流量的目的地限制在 **App-Server-Tier-DC** 區域的帳單伺服器 (**Billing-App-Servers**)。
- 限制 Web 伺服器可用於存取帳單應用程式伺服器的應用程式，並僅允許應用程式在其預設連接埠上執行。在此範例中，應用程式包括兩個自訂應用程式：**Billing-App** 和 **Payment-App**，您可在建立應用程式時為其指定預設連接埠。財務部將這些專有應用應用程式用於帳單和支付服務。

建立類似規則以控制 Web 伺服器層與其他應用程式伺服器層之間的應用程式與流量。

STEP 2 | 允許應用程式伺服器層和資料庫伺服器層之間的財務應用程式流量。

此規則限制了可以在財務部帳單伺服器的應用程式伺服器層和資料庫伺服器層之間流動的流量，以便只有使用合法應用程式的流量才能在帳單應用程式伺服器與帳單資料庫伺服器之間流動。該規則使用動態位址群組來指定每個應用程式層中的伺服器—**Billing-App-Servers** 指定應用程式伺服器層中的伺服器位址，**DB2-Servers** 指定財務資料庫伺服器層中的伺服器位址。



若要建立此規則：

- 將財務應用程式流量的來源限制在 **App-Server-Tier-DC** 區域的帳單應用程式伺服器 (**Billing-App-Servers**)。
- 將財務應用程式流量的目的地限制在 **DB-Server-Tier-DC** 區域的資料庫伺服器 (**DB2-Servers**)。
- 限制帳單應用程式伺服器可用於存取資料庫伺服器的應用程式並僅允許應用程式在其預設連接埠或其已知非預設連接埠上執行。

建立類似規則以控制其他應用程式的應用程式伺服器層與資料庫伺服器層之間的應用程式與流量。

透過檢視預先定義的應用程式報告確認僅您在安全性政策規則中明確允許的應用程式正在執行（**Monitor**（監控）> **Reports**（報告）> **Application Reports**（應用程式報告）> **Applications**（應用程式））。如果您在報告中看到意外的應用程式，請檢閱應用程式允許規則並對其進行細化，使其不允許出現意外的應用程式。

建立內部資料中心解密原則規則

為何要解密資料中心內的流量？畢竟，資料中心沒有使用者，是安全網路內一個非常安全的環境。但事實並非如此。資料中心恰恰是攻擊者藏身的理想場所，因為許多人認為資料中心很安全，而不會去查看。但網路其他部分的基本原理也同樣適用於資料中心：您不能防止自己免受您看不見的威脅的攻擊。解密經加密的資料中心流量，使防火牆能夠檢查流量、控制存取、使威脅可見，並保護您的寶貴資產。

部分資料中心流量未加密（明碼）。不要在明碼流量上啟用解密，因為沒有要解密的流量。

在建立內部資料中心應用程式允許規則中，我們已建立安全性政策規則，允許涉及不同應用程式層中財務部應用程式的伺服器相互通訊。我們在此建立了類似的解密原則規則以解密這些規則允許的流量。

對於每個規則，設定解密記錄和日誌轉送。請在防火牆資源允許時記錄最多的解密流量。

STEP 1 | 解密 Web 伺服器層和應用程式伺服器層之間的財務應用程式流量。

此規則解密財務部帳單伺服器的 Web 伺服器層和應用程式伺服器層之間流動的流量，以便防火牆看到流量，並保護每一層的伺服器免受潛在威脅攻擊。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
Web to App	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在此範例中，來源為 **Web-Server-Tier-DC** 區域的 **Web-Servers** 動態位址群組，目的地為 **App-Server-Tier-DC** 區域的 **Billing-App-Servers**。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Forward Proxy**（**SSL** 轉送 **Proxy**）。套用資料中心最佳做法解密設定檔以對流量套用 SSL 轉送 Proxy 和 SSL 協定設定。

STEP 2 | 解密應用程式伺服器層和資料庫伺服器層之間的財務應用程式流量。

此規則解密了財務部帳單伺服器的應用程式伺服器層和資料庫伺服器層之間流動的流量，以便防火牆看到流量，並保護每一層的伺服器免受潛在威脅攻擊。

		Source			Destination		Decrypt Options					
NAME	TAGS	ZONE	ADDRESS	USER	ZONE	ADDRESS	ACTION	TYPE	DECRYPTION PROFILE	LOG SETTINGS	LOG SUCCESSFUL SSL HANDSHAKE	LOG UNSUCCESSFUL SSL HANDSHAKE
App to DB	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	decrypt	ssl-forward-proxy	DC BP Decryption	Decrypt-LF	true	true

若要建立此規則：

- 指定與類似安全性原則規則相同的來源和目的地。在此範例中，來源為 **App-Server-Tier-DC** 區域的 **Billing-App-Servers** 動態位址群組，目的地為 **DB-Server-Tier-DC** 區域的 **DB2-Servers**。
- 在選項頁籤上，將動作設定為 **Decrypt**（解密）並將解密類型設定為 **SSL Forward Proxy**（**SSL** 轉送 **Proxy**）。套用資料中心最佳做法解密設定檔以對流量套用 SSL 轉送 Proxy 和 SSL 協定設定。

對資料中心安全性原則規則庫進行排序

本主題提供範例安全性政策規則庫的快照，而此範例顯示所有四個資料中心流量流程的規則順序。前幾節詳細討論了每條安全性原則規則（以及解密原則規則、必要時的驗證原則與 DoS 保護原則規則）。

安全性政策規則的順序至關重要。任何規則不應影響另一規則。例如，封鎖規則不應該封鎖想要允許的流量，因此您必須在封鎖流量的規則生效之前放置允許規則。此外，允許規則不應該允許想要封鎖的流量。透過建立極為具體的允許規則，您可以嚴格控制允許的應用程式以及使用人員和無法使用的人員。

規則 **1-7**：前兩個規則封鎖 QUIC 應用程式，以防止它封鎖流量或防止解密。接下來的五個規則允許使用者的 DNS 存取權限，並允許特定使用者群組的特定應用程式和伺服器存取權限。這些是建立使用者至資料中心應用程式允許規則中所設定的規則。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
1	Block QUIC UDP	none	any	any	any	L3-External	any	any	quic_udp_ports	Deny	none	
2	Block QUIC	none	any	any	any	L3-External	any	quic	application-default	Deny	none	
3	DNS Services	User to DC BP	any	any	any	IT Infrastructure	DNS-Servers	dns	application-default	Allow		
4	IT DC Server Management	User to DC BP	IT-Users	any	it-superusers	IT-Server-Access-DC	IT-Server-Management	ms-rdp ssh ssl	Custom-IT-Ports	Allow		
5	Engineering Resources	User to DC BP	Engineering-Users	any	api-users engg-users	Engineering-DC-Infra	Dev-Servers	oracle-bi perforce profinet qlikview	application-default	Allow		
6	Finance to DC	User to DC BP	Finance-Users	any	accounting-users finance-users	Finance-DC-Infra	Fin-Servers	netsuite oracle oracle-crm-ondemand oracle-forms	application-default	Allow		
7	SAP-Contractors	User to DC BP	Contractors	any	sap-contractors	SAP-Infra	SAP DB Servers	ms-sql-analysis-service mssql-db mssql-mon sap	application-default	Allow		

圖 1: 資料中心規則 **1-7**

只有指定的使用者才可在其預設連接埠上使用指定的應用程式，以僅存取指定資料中心目的地伺服器（位址）。安全性設定檔保護所有這些允許規則免遭威脅攻擊。這些規則優先於發現網路上的不明使用者與應用程式的封鎖規則，因為這些規則非常具體，且可防止認可的使用者與應用程式符合規則庫中更多較低層次的一般規則。

規則 **8-9**：雖然之前的規則允許認可的應用程式，但接下來的兩個規則（在建立資料中心流量封鎖規則中建立）會在標準連接埠上發現和封鎖來自使用者的非預期應用程式，以及在非標準連接埠上封鎖所有應用程式。部署的使用者區域數目可能多於此範例中顯示的使用者區域數目。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
8	Unexpected-App-from-User-Zone	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
9	Unexpected-User-App-Any-Port	User to DC BP	Contractors Engineering-Users Finance-Users IT-Users	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	

圖 2: 資料中心規則 **8-9**

來自非使用者區域的流量不符合規則。將這些規則放在應用程式封鎖規則（規則 18 與 19）之上，否則那些規則將會影響這些規則。（流量符合這兩條規則，還可能符合更多的一般應用程式封鎖規則。如果應用程式封鎖規則優先，並符合還與這些規則相符的流量，則該流量將不會符合這些規則，亦不會單獨進行記錄，因此規則將無法完成預期工作：區分因員工使用者活動造成的封鎖與因非使用者區域中活動造成的封鎖）。

規則 **10-16**：接下來的七個規則允許資料中心與網際網路之間以及資料中心內的流量（在建立網際網路至資料中心應用程式允許規則、建立資料中心至網際網路應用程式允許規則和建立內部資料中心應用程式允許規則中建立）。 安全性設定檔保護所有這些允許規則免遭威脅攻擊。

	NAME	TAGS	Source ZONE	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	URL CATEGORY	ACTION	PROFILE	OPTIONS
10	Web Server Inbound	Internet to DC BP	L3-External	Bad IPs List	any	Web-Server-Tier-DC	Web Servers	Acme	application-default	any	Allow		
11	NTP DNS Update	DC to Internet BP	IT Infrastructure	DNS-NTP-Servers	any	L3-External	any	dns ntp	application-default	NTP-DNS-Update-Servers	Allow		
12	CentOS Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	yum	application-default	CentOS-Update-Servers	Allow		
13	Windows Update	DC to Internet BP	Engineering-DC-Infra	Dev-Servers	any	L3-External	any	ms-update ssl	application-default	Win-Update-Servers	Allow		
14	Cert Update	DC to Internet BP	IT Infrastructure	IT-Server-Management	any	L3-External	any	ocsp	application-default	any	Allow		
15	App to DB Server	Intra DC BP	App-Server-Tier-DC	Billing-App-Servers	any	DB-Server-Tier-DC	DB2-Servers	Billing-App db2 mssql-db Payment-App ssl	application-default	any	Allow		
16	Web to App Server	Intra DC BP	Web-Server-Tier-DC	Web Servers	any	App-Server-Tier-DC	Billing-App-Servers	Billing-App Payment-App ssl web-browsing	application-default	any	Allow		

圖 3: 資料中心規則 **10-16**

規則 **17-20**：最後四個規則是在建立資料中心流量封鎖規則中設定，會封鎖您不想在資料中心內允許之已知應用程式與非預期應用程式，並發現網路上的不明使用者。

	NAME	Source ZO...	Source ADDRESS	Source USER	Destination ZONE	Destination ADDRESS	APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
17	Block-Bad-Apps	any	any	any	App-Server-Tier-DC DB-Server-Tier-DC Engineering-DC-Infra Finance-DC-Infra IT Infrastructure SAP-Infra Web-Server-Tier-DC	any	Encrypted-Tunnels File-Sharing Remote-Access	any	Drop	none	
18	Unexpected-App-from-Any-Zone	any	any	any	Web-Server-Tier-DC	any	any	application-default	Drop	none	
19	Unexpected-App-Any-Port	any	any	any	Web-Server-Tier-DC	any	any	any	Drop	none	
20	Discover-Unknown-Users	any	any	unknown	any	any	any	any	Deny	none	

規則 17 會封鎖您從未想要在資料中心允許的應用程式。此規則位於應用程式允許規則之後，以啟用例外項的存取。例如，您可在此封鎖規則之前的應用程式允許規則中認可一個或兩個檔案共用應用程式，此規則中的應用程式篩選器隨後則會封鎖該應用程式類型的其餘部分，以防使用未認可的檔案共用應用程式。如果存在您從未想要在網路上允許的應用程式集或個別應用程式，並且沒有例外情況，例如 BitTorrent，您可以建立一個具體的封鎖規則，以僅封鎖這些應用程式並將其置於規則庫的頂端、應用程式允許規則之上。不過，如果您執行此操作，則必須確保封鎖的應用程式不具備合法的業務用途，因為使用者將無法存取它們。

規則 18 和 19 類似於規則 8 和規則 9，用於發現來自使用者的非預期應用程式（套用這些規則的流量僅來自使用者區域）。規則 18 和 19 發現來自所有其他區域的非預期應用程式。使用單獨的規則使您能夠以更大的精度記錄封鎖規則相符項。

規則 20 發現不明使用者，使您可以單獨記錄這些嘗試進行的存取，以便於調查。

與所有安全性政策規則庫一樣，最後兩個規則將會是 Palo Alto Networks 預設規則，用於內部網路區流量（允許）和網際網路區流量（拒絕）。

記錄和監控資料中心流量

防火牆的記錄與監控工具可以顯示網路上的應用程式、使用者及流量模式，包括您可能不知道的應用程式與使用者。記錄與監控可在轉換至資料中心最佳做法安全性原則，以及對其加以維護的所有階段提供實用資訊，因為它還顯示不明使用者（未透過 User-ID 識別）、不明應用程式以及非預期連接埠上的流量，所有這些皆指示安全性原則規則尚未正確或嚴格建構。記錄與監控資訊有助於您確定要允許的應用程式，以及允許哪些使用者存取哪些應用程式與裝置，還協助您調查潛在的安全性問題。

當您評估資料中心時，您可以擷取基準線測量。定期將這些基準線測量與現行測量進行比較，以評估進度，確定變更並在實作資料中心最佳做法安全性原則時找到需要改進的領域。

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

設定從防火牆到 Panorama 或諸如 SNMP 設陷伺服器或 syslog 伺服器之類的外部服務的日誌轉送，以集中顯示來自多個防火牆的日誌，使檢視與分析更為方便（防火牆僅可顯示本機日誌與報告，而不會顯示其他防火牆的日誌與報告）。若您設定日誌轉送，請一併設定傳送通知，以確認設定的日誌目的地正在接收防火牆日誌。

資料中心記錄與監控的最佳做法包含：

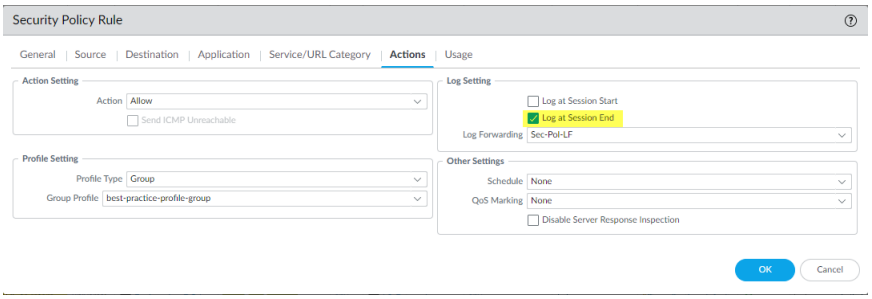
- 要記錄和監控的資料中心流量
- 監控資料中心封鎖規則並調優規則庫
- 記錄不符合區域間規則的資料中心流量
- 記錄符合區域內允許規則的資料中心內的流量

要記錄和監控的資料中心流量

依預設，Palo Alto Networks 新世代防火牆會建立某些日誌，而您需要為其他流量設定日誌記錄。最佳做法是，記錄所有資料中心流量並監控非預期應用程式、使用者、流量以及行為的日誌。

依預設，防火牆會記錄符合明確設定之安全性原則規則，並不會記錄符合規則庫底端之預先定義的區域內預設（允許相同區域內具有來源與目的地的流量），以及區域間預設（規則庫中最後一個規則，其會拒絕不符合之前規則的流量）規則。

當您建立安全性政策規則時，防火牆預設會在工作階段結束時記錄流量：



不過，防火牆預設不會轉送日誌，而且預設不會套用安全性設定檔。上一個範例所顯示的最佳做法有關將日誌轉送至適當的日誌伺服器和管理員，以及套用最佳做法安全性設定檔。

適用於大多數流量的最佳做法是，**Log at Session End**（工作階段結束時記錄），因為應用程式通常會在工作階段整個生命週期內發生變更。例如，工作階段的初始 App-ID 可能為 Web 瀏覽，但在防火牆處理一些封包之後，防火牆可能會為應用程式找到更具體的 App-ID，並變更該 App-ID。在工作階段開始時有幾種記錄流量的使用案例，包括 DNS sinkholing、存留時間較長的通道工作階段，以及從工作階段開始時需要資訊以進行疑難排解的情況。

記錄流量會記錄規則允許及拒絕或丟棄（規則違規）之流量的相關資訊，因此，無論防火牆處理流量的方式如何，均會提供有價值的資訊。規則違規強調顯示潛在的攻擊或需要調整以允許合法業務應用程式的允許規則。

當您檢查日誌中遭封鎖的流量時，請將以下兩種流量加以區分：一種為，在任何系統遭入侵之前，防火牆將其作為保護事件加以封鎖的流量，比如封鎖未允許的應用程式；另一種為，防火牆將其作為入侵後事件加以封鎖的流量，例如，已在資料中心伺服器上的惡意軟體試圖連線外部伺服器以下載更多惡意軟體或洩漏資料。

防火牆會提供大量的監控工具、日誌以及日誌報告，藉以分析網路：

- **Monitor**（監控）> **Logs**（日誌）提供流量、威脅、User-ID 以及許多其他日誌類型，包括 **Unified**（統一）日誌，用於在一個螢幕上顯示多種日誌類型，因此您不必分別查看不同類型的日誌。當摘要內含有放大鏡圖示時，您可以按一下以深入查看日誌條目。
- **Monitor**（監控）> **PDF Reports**（**PDF** 報告）提供您可以檢視的預先定義報告，還能建立包含有預先定義報告與自訂報告的報告群組。例如，您可檢閱流量活動或進行基準線測量，以按區域或介面瞭解每個資料中心區段內的頻寬使用情形與流量。
- **Monitor**（監控）> **Manage Custom Reports**（管理自訂報告）提供建立自訂報告的能力，使您可以檢視有關封鎖規則、允許規則或任何其他感興趣主旨的資訊。
- **Monitor**（監控）> **Packet Capture**（封包擷取）讓您可以對周遊防火牆的管理介面以及網路介面的流量進行封包擷取。
- 應用程式控管中心 (**ACC**) 所提供的 Widget 會顯示應用程式、使用者、URL、威脅以及周遊網路之內容的互動式圖形摘要。例如，您可以檢閱並評估網路上的應用程式（**ACC** > **Network Activity**（網路活動）> **Application Usage**（應用程式使用情形）> **Threats**（威脅）），以瞭解應用程式中是否有任何變更或者應用程式是否存在威脅行為。若您在清單中看到非預期應用程式，則評估如何處理這些應用程式。

  使用 ACC 資訊的另一個不錯途經是，協助識別遭入侵的使用者帳戶與主機系統。透過使用 **ACC** > **Network Activity**（網路活動）> **User Activity**（使用者活動）> **Threats**（威脅）Widget 分析威脅以及與其相關聯的使用者名稱，然後使用威脅日誌隔離確切問題。
- 儀表板（**Dashboard**（儀表板））提供的 Widget 會顯示一般防火牆資訊，以及威脅、設定與系統日誌中最多 10 個最新項目。
- 使用 Panorama 來監控防火牆健康並設定新裝置的基準線、比較效能指標，以及在提交、軟體升級、內容更新、規則變更、新增應用程式這類事件之後追蹤防火牆效能。如果效能偏離裝置的基準線，您可以手動檢視並進行疑難排解，或自動開啟票證進行調查。
- 在 Panorama 或個別防火牆上，使用原則規則命中計數器來分析對規則庫進行的變更。例如，當您新增應用程式時，在您允許應用程式在網路上的流量前，將允許規則新增到規則庫中。若流量符合規則且計數器增加，則指示即使您尚未啟用該應用程式，符合該規則的流量也可能已在網路中，或者您需要調整規則。另一個範例是用基於應用程式的規則取代基於連接埠的規則，方式為：將基於應用程式的規則放在基於連接埠的規則之前，並註意是否有任何流量符合基於連接埠的規則。若流量符合基於連接埠的規則，則需要調整基於應用程式的規則以捕捉該流量。

  結合使用政策規則命中計數器，檢查 **ACC** > **Threat Activity**（威脅活動）> **Applications Using Non Standard Ports**（使用非標準連接埠的應用程式）以及 **ACC** > **Threat Activity**（威脅活動）> **Rules Allowing Apps On Non Standard Ports**（在非標準連接埠上允許應用程式的規則）Widget，以瞭解非標準連接埠上的流量是否會導致非預期規則命中。

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

監控資料中心封鎖規則並調優規則庫

制定最佳做法安全性原則是一個反覆的過程。建立資料中心流量封鎖規則後，請立即開始監控符合封鎖規則的流量，而這些規則用於識別原則漏洞、非預期行為以及潛在的攻擊。調整應用程式允許規則可導致產生符合封鎖規則但應被允許的流量，並調查可能指示攻擊的流量。

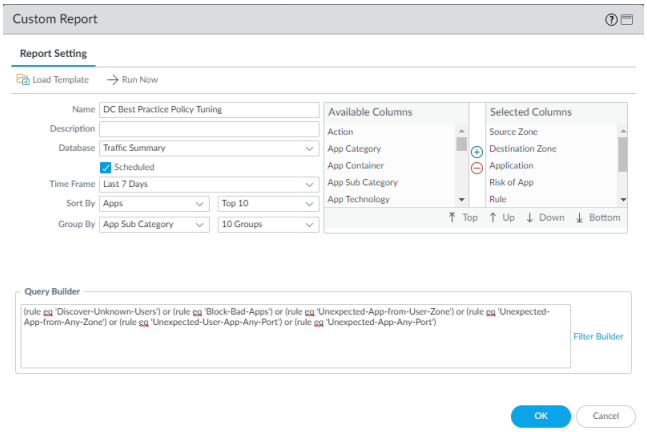
封鎖流量報告包含有價值的資訊，您可用此類資訊來調查潛在的問題。將封鎖規則存放於規則庫，即可保護有價值的資料中心資產，並在流量符合封鎖規則時提供該資訊。

遵循內容更新最佳做法，使防火牆保護最新。維護資料中心最佳做法規則庫包含資料中心防火牆的具體最佳做法。

STEP 1 | 建立自訂報告，可監控符合專用於識別原則漏洞與潛在攻擊之封鎖規則的流量。

1. 選取 **Monitor**（監控）> **Manage Custom Reports**（管理自訂報告）.
2. **Add**（新增）報告，並為其指定一個用於說明報告目的的 **Name**（名稱），在此範例中則為 **DC Best Practice Policy Tuning**（DC 最佳做法原則調整）。
3. 將 **Database**（資料庫）設為 **Traffic Summary**（流量摘要）。這也會變更 **Available Columns**（可用欄）選項。
4. 從 **Available Columns**（可用欄）中，新增 **Source Zone**（來源區域）、**Destination Zone**（目的地區域）、**Sessions**（工作階段）、**Bytes**（位元組）、**Application**（應用程式）、**Risk of App**（應用程式風險）、**Rule**（規則）以及 **Threats**（威脅）至 **Selected Columns**（選定欄）清單。如果您要監控其他類型的資訊，也請選擇這些選項。
5. 選取 **Scheduled**（已排程）方塊。
6. 設定所需的 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式）值。在此範例中，我們將 **Time Frame**（時間範圍）設定為 **Last 7 Days**（前 7 天）、將 **Sort By**（排序方式）設定為 **Apps**（應用程式），並將 **Group By**（群組方式）設定為 **App Sub Category**（應用程式子類別）。
7. 定義查詢，以比對符合專用於尋找原則漏洞及潛在攻擊的規則的流量。您可以透過使用 **or** 運算式為符合任何規則的流量建立單個報告，或建立個別報告以監控每個規則。在 **Query Builder**（查詢建立器）中，指定要包含在報告內的每個規則的名稱。此範例使用六個封鎖規則，並使用 **Or** 運算元以包含有關符合任何規則之流量的資訊：

   - `(rule eq 'Discover-Unknown-Users')`
   - `(rule eq 'Block-Bad-Apps')`
   - `(rule eq 'Unexpected-App-from-User-Zone')`
   - `(rule eq 'Unexpected-App-from-Any-Zone')`
   - `(rule eq 'Unexpected-User-App-Any-Port')`
   - `(rule eq 'Unexpected-App-Any-Port')`



STEP 2 | 定期檢閱一份或多份報告，確保您已瞭解流量符合每個封鎖規則的原因，並更新原則以包含合法應用程式與使用者，或使用該資訊來評估符合規則之流量的風險。

記錄符合區域內允許規則的資料中心內的流量

依預設，允許所有區域內流量（來源與目的地位於相同區域）。防火牆評估安全性政策後，會允許由應用程式允許清單規則控制的流量、拒絕由封鎖規則控制的流量，或者在區域內流量不符合任何規則時，依預設，防火牆會允許該流量。（依預設，防火牆封鎖區域間流量。）由於資料中心資產極為寶貴，最佳做法是監控各個資料中心伺服器之間資料中心內的所有流量，包括區域內預設允許規則允許的流量。

要瞭解此流量，請在區域內預設規則套用至資料中心內區域中的流量時對其啟用日誌記錄。記錄此流量讓您能夠檢查尚未明確允許的存取權限，以及您可能想要透過修改允許規則明確允許或明確封鎖的存取權限。

在定義初始資料中心內的流量安全性原則，我們使用了資料中心內的三個範例區域：Web-Server-Tier-DC、App-Server-Tier-DC 及 DB-Server-Tier-DC。在此範例中，我們建立自訂報告，以收集有關這三個內部資料中心區域內資料中心區域內流量的日誌資訊。

STEP 1 | 選取規則庫中的區域內預設列，然後按一下 **Override**（覆寫）以啟用編輯規則。

STEP 2 | 選取 **intrazone-default**（區域內預設）規則名稱以編輯規則。

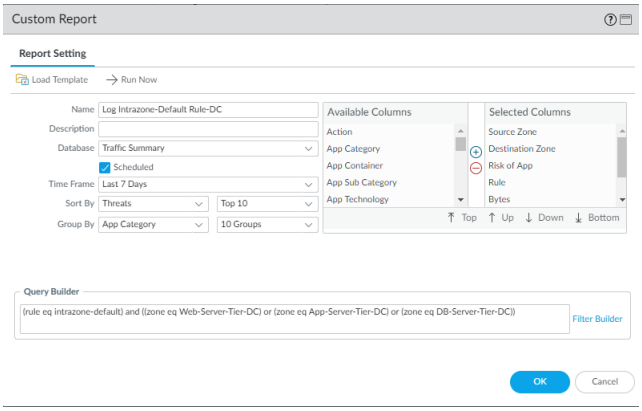
STEP 3 | 在 Actions（動作）頁籤上，選取 **Log at Session End**（工作階段結束時記錄），然後按一下 **OK**（確定）。

STEP 4 | 建立自訂報告，以監控內部資料中心區域中符合此規則的流量。

1. 選取 **Monitor**（監控）> **Manage Custom Reports**（管理自訂報告）.
2. **Add**（新增）報告，並為它設定具描述性的 **Name**（名稱）。在此範例中，名稱為 **Log Intrazone-Default Rule-DC**（記錄區域內預設規則 **DC**）。
3. 將 **Database**（資料庫）設為 **Traffic Summary**（流量摘要）。
4. 從 **Available Columns**（可用欄）中，新增 **Source Zone**（來源區域）、**Destination Zone**（目的地區域）、**Sessions**（工作階段）、**Bytes**（位元組）、**Application**（應用程式）、**Risk of App**（應用程式風險）、**Rule**（規則）以及 **Threats**（威脅）至 **Selected Columns**（選定欄）清單。如果您要監控其他類型的資訊，也請選擇這些選項。
5. 選取 **Scheduled**（已排程）方塊。
6. 設定所需的 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式）值。在此範例中，選定的值分別為 **Threats**（威脅）與 **App Category**（應用程式類別）。
7. 定義查詢以比對符合資料中心區域的區域內預設規則的流量：

```
(rule eq intrazone-default) and ((zone eq Web-Server-Tier-DC) or (zone eq
 App-Server-Tier-DC) or (zone eq DB-Server-Tier-DC))
```

查詢篩選的流量符合內部網路區預設規則，還符合我們已定義的任何三個內部資料中心區域。由於預設 **Selected Columns**（選定欄）包含區域，報告會顯示每個工作階段的區域。在真實世界的資料中心中，您可能會有更多區域，並新增每個區域至查詢。產生的自訂報告設定如下所示：



8. **Commit**（提交）變更。

記錄不符合區域間規則的資料中心流量

不符合任何您設定之安全性政策規則的流量，將符合規則庫底端的預先定義的網際網路區預設封鎖規則，並將遭到拒絕。要查看與您明確設定的規則不相符的流量，請對區域間預設規則啟用日誌記錄。記錄此流量，讓您有機會檢查未明確允許之試圖進行的存取，這可能會識別您要修改允許規則之攻擊嘗試或流量。

STEP 1 | 選取規則庫中的區域間預設列，然後按一下 **Override**（覆寫）以啟用編輯規則。

STEP 2 | 選取 **interzone-default**（區域間預設）規則名稱以編輯規則。

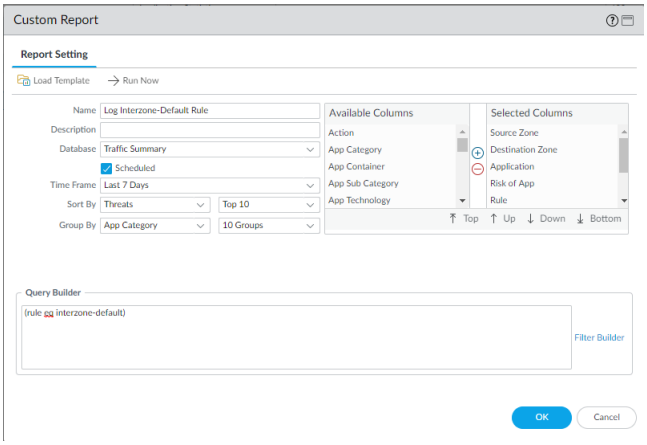
STEP 3 | 在 Actions（動作）頁籤上，選取 **Log at Session End**（工作階段結束時記錄），然後按一下 **OK**（確定）。

STEP 4 | 建立自訂報告以監控符合此規則的流量。

1. 選取 **Monitor**（監控）> **Manage Custom Reports**（管理自訂報告）.
2. **Add**（新增）報告，並為它設定具描述性的 **Name**（名稱）。在此範例中，名稱為 **Log Interzone-Default Rule**（記錄區域間預設規則）。
3. 將 **Database**（資料庫）設為 **Traffic Summary**（流量摘要）。
4. 從 **Available Columns**（可用欄）中，新增 **Source Zone**（來源區域）、**Destination Zone**（目的地區域）、**Sessions**（工作階段）、**Bytes**（位元組）、**Application**（應用程式）、**Risk of App**（應用程式風險）、**Rule**（規則）以及 **Threat**（威脅）至 **Selected Columns**（選定欄）清單。如果您要監控其他類型的資訊，也請選擇這些選項。
5. 選取 **Scheduled**（已排程）方塊。
6. 設定所需的 **Time Frame**（時間範圍）、**Sort By**（排序方式）和 **Group By**（分組方式）值。在此範例中，選取的值分別為 **Last 7 Days**（前 7 天）、**Threats**（威脅）和 **App Category**（應用程式類別）。
7. 定義查詢以比對符合區域間預設規則的流量：

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

產生的自訂報告設定如下所示：



8. **Commit**（提交）變更。

維護資料中心最佳做法規則庫

應用程式不斷演進，因此應用程式允許清單亦需隨之變化。因為最佳做法規則利用政策物件來簡化管理，所以，針對新應用程式新增支援或從允許清單移除應用程式，通常意味著需要相應地修改對應的應用程式群組或應用程式篩選器。

Palo Alto Networks 傳送您應該在防火牆上盡快自動下載和安排安裝時間的內容更新。大多數內容更新都有對威脅內容（防毒、漏洞、反間諜軟體等）的更新，而且可能含有經過修改的 App-ID。在每個月的第三個星期二的內容更新也會有新的 App-ID。您可以設定單獨的閾值以延遲安裝定期的內容更新，以及延遲安裝在下載後的，包含新 App-ID 一段指定時間的一個月一次更新。延遲安裝可讓您盡快安裝不包括新 App-ID 的內容更新以取得最新的威脅特徵，同時又提供更多時間在安裝前檢查新的 App-ID。

內容在每個月的第三個星期二更新，包含可能導致安全性政策執行變更的新 App-ID。在您安裝新的或經過修改的 App-ID 前，請檢閱政策影響、階段更新，以便測試影響和視需要修改現有的安全性政策規則。在防火牆上控制下載和安裝內容更新的最有效方式就是載入它們，然後從 Panorama 上推送（如果您有使用 Panorama）。

遵循一般內容更新最佳做法，但請謹記，資料中心可用性通常很重要，因此您可能不會選擇像在面向網際網路的防火牆上那樣快速地在資料中心內部署內容更新：

- 在將內容更新安裝到資料中心之前，請在網路安全區域中對其進行快速測試。
- 對於不包含新 App-ID 的內容更新，將安裝臨界值設定為自動下載之後不超過 8 小時，並在此期間執行測試。
- 對於包含新 App-ID 的內容更新，將安裝臨界值設定為自動下載之後不超過 8 天，並在此期間執行測試。
- 設定所有內容更新的記錄轉傳。

STEP 1 | 在安裝新的內容更新前，檢閱新的和經過修改的 App-ID，以確定是否對政策產生影響。

STEP 2 | 視需要修改現有的安全性政策規則以容納 App-ID 變化。

如果某些 App-ID 需要更多測試，您可以停用所選擇的 App-ID，然後安裝其餘的新 App ID。在下一個含有新 App-ID 的月度內容版本發佈（每個月的第三個星期二）之前，完成任何必要原則修訂的測試來避免重疊。

隨著時間的推移，資料中心中使用的應用程式清單通常會趨於穩定，因此相關的新 *App-ID* 越來越少。（大多數新 *App-ID* 都適用於面向網際網路的應用程式。）這降低了新 *App-ID* 在資料中心中產生問題的風險，並且使您能夠更快地安裝具有新 *App-ID* 的內容更新。

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

維護最佳做法規則庫的其他方法有：

- 使用 Palo Alto Networks 評估及檢閱工具識別安全性覆蓋範圍內的漏洞。
- 使用者就其無法再存取之應用程式的回饋，可在積極強制執行阻止使用規則庫或已在網路中使用之具風險的應用程式之前，識別其內存在的漏洞。
- 將評估資料中心時建立的資產詳細目錄清單與資產本身進行比較，並確保這些資產得到適當保護。
- 使用 Palo Alto Networks 記錄與監控工具（比如應用程式控管中心 (ACC)）來查找並調查非預期活動，這可能指示規則設定錯誤或遺漏規則。定期執行報告，確認已套用您想要套用的安全性層次。

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

使用 Palo Alto Networks 評估與檢閱工具

Palo Alto Networks 的客戶成功團隊已開發了具有工具與資源的 防禦架構，可助您檢閱及評估網路的安全性風險，以及如何善用防火牆功能與其他工具來保護網路安全。請聯絡 Palo Alto Networks 代表安排評估與檢閱（Palo Alto Networks 銷售工程師會進行檢閱，以提供評估網路安全性狀態的專業知識）。截至本出版物發佈時，可用的安全性風險防禦工具包括：

- 防禦狀態評估 **(PPA)**—PPA 為一組調查問卷，有助於發現網路及安全性架構所有領域的安全性風險防禦漏洞。PPA 不僅有助於識別所有安全性風險，還提供有關如何預防風險並縮小漏洞的詳細建議。該評估由經驗豐富的 Palo Alto Networks 銷售工程師指導，可協助確定您應該關注預防活動的最大風險領域。您可以在防火牆與 Panorama 上執行 PPA。
- 最佳做法評估 **(BPA)** 工具—BPA 可用於新世代防火牆與 Panorama，並評估裝置的組態，方式為測量功能的採用情況，驗證原則是否遵循最佳做法，以及提供如何修補失敗之最佳做法檢查的建議與指示。

  「安全性原則採用熱圖」元件依裝置群組、序號、區域、架構區域及其他類別篩選資訊。結果包括趨勢資料，顯示了在採用新功能、修正漏洞以及向零信任網路發展時安全性提高的速率。

  BPA 元件對防火牆或 Panorama 組態執行 200 多次安全性檢查，並對每次檢查進行通過/未通過評分。每次檢查便為 Palo Alto Networks 安全性專家確定的最佳做法。若檢查傳回未通過分數，則該工具會提供未通過分數的理由以及如何解決問題。

Palo Alto Networks 會繼續開發新工具，並改進現有工具。請聯絡 Palo Alto Networks 代表，瞭解最新工具可如何提高資料中心網路安全性。