排除安全訪問解密和入侵防禦系統(IPS)工作流程故障

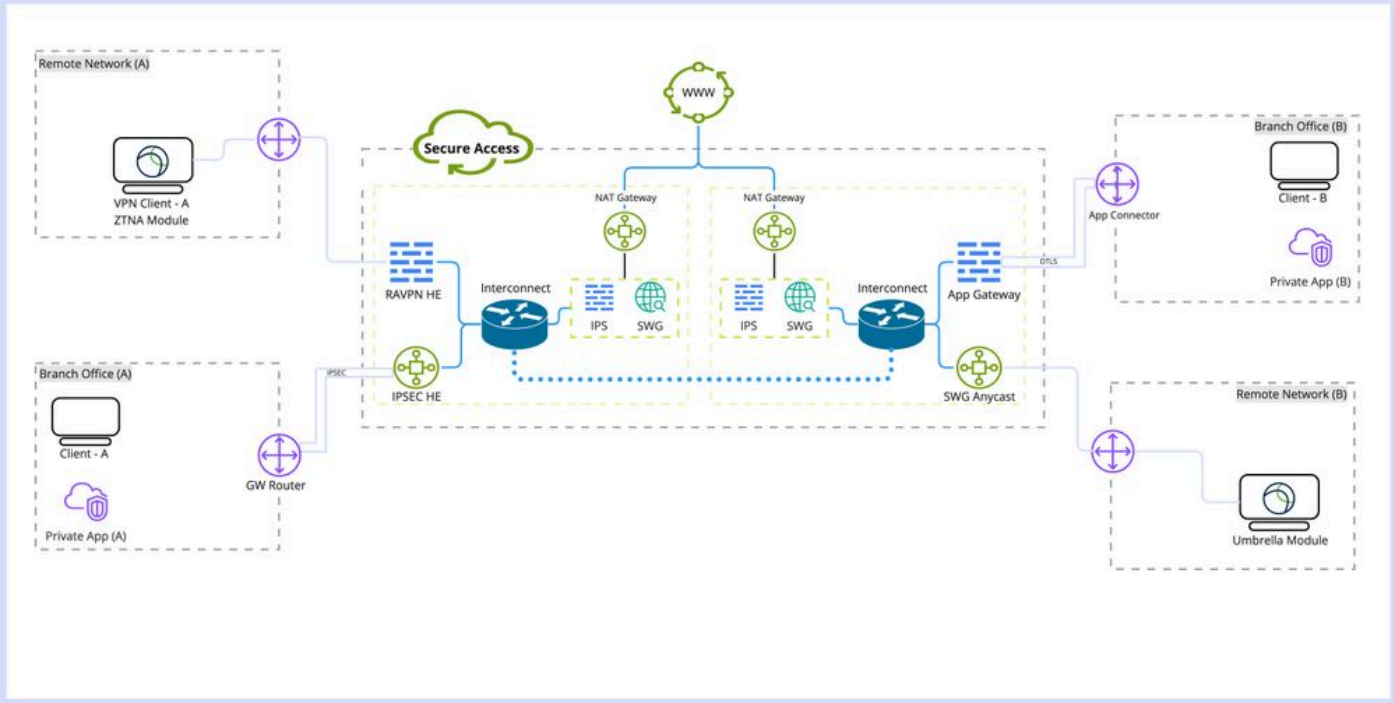
目錄

簡介

本文檔介紹安全訪問解密和IPS工作流程，並突出顯示重要設定屬性。

安全訪問架構

此安全訪問架構突出顯示安全訪問提供的不同服務和可以建立用於保護網路的不同連線方法。



安全訪問架構

架構詳細資料：

熟悉的術語：

RAVPN HE：遠端訪問虛擬專用網路頭端

IPSEC HE：遠端隧道網際網路協定安全(IPSEC)前端

ZTNA模組：零信任網路訪問模組

SWG：安全Web網關

IPS：入侵防禦系統

NAT網關：網路地址轉換網關

SWG AnyCast：安全Web網關任播入口點

部署型別：

1. 遠端訪問VPN

2. 遠端訪問隧道

3. Umbrella漫遊模組

4. 應用聯結器/應用網關

5. 零信任模組(ZTNA)

功能概述

「安全存取」提供Web Decryption and Intrusion Prevention System (IPS)功能，可增強應用程式偵測與分類，並提供更多流量相關詳細資訊，包括URL路徑、檔案名稱及其應用程式類別。並可協助預防零日攻擊和惡意程式。

解密：本文中的解密是指透過安全Web網關(SWG)模組對超文本傳輸協定(HTTPS)流量進行解密，以及對IPS檢查的流量進行解密。

IPS：防火牆級別的入侵檢測和防禦系統，需要對流量進行解密才能執行全部功能。

解密對於多種安全訪問功能是必要的，例如防資料丟失(DLP)和遠端瀏覽器隔離(RBI)、檔案檢查、檔案分析和檔案型別阻止。

安全訪問中的解密和IPS相關設定

這是Secure Access中可用解密和IPS相關設定的快速概述。

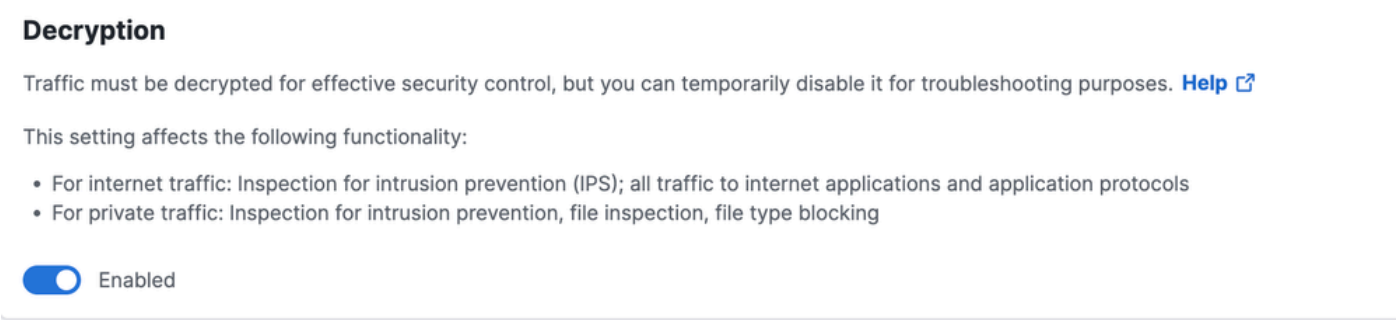
IPS解密

這是IPS的全局設定，用於停用或啟用所有策略的IPS引擎。

屬性：

- 此選項不會影響安全Web網關解密（Web解密）
- 停用和啟用每個策略的IPS功能有限，只能檢查握手的初始階段，而不檢查請求正文。

組態: 控制台->安全->訪問策略->規則預設值和全局設定->全局設定-> IPS解密



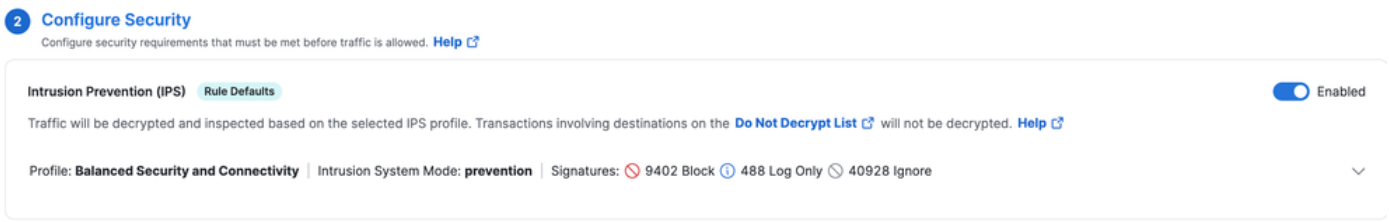
每個策略的IPS設定

此選項允許停用和啟用每個策略庫的IPS。

屬性：

- 此選項控制每個策略是否啟用或停用IPS。
- 此選項取決於Decrypt for IPS設定，如果全局的Decrypt for IPS選項被停用，則其行為僅檢查握手的初始階段，而不檢查請求正文。
- 此選項不會影響SWG（Web解密）

配置：控制台->安全->訪問策略->編輯策略->配置安全->入侵防禦(IPS)



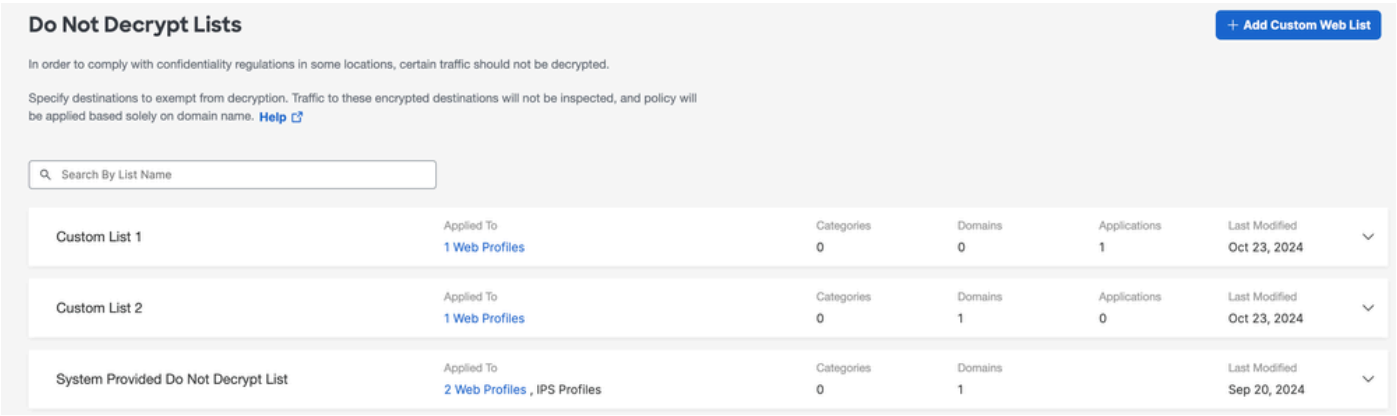
不解密清單

可連結到安全配置檔案以繞過域或IP地址解密的一組目標清單。

屬性：

- 允許繞過Web解密自定義域
- 此清單僅影響Web解密而非IPS，但系統提供的不解密清單除外
- 包含繞過IPS和Web解密的（系統提供的不解密清單）
- 此選項需要與要附加到策略的安全配置檔案結合使用
- 僅當在安全性設定檔中啟用「解密」時，才能使用此清單

配置：控制台->安全->不解密清單



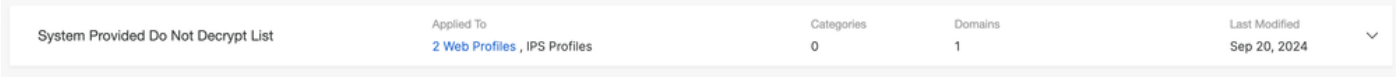
系統提供的不解密清單

「不解密」清單的一部分，具有在安全訪問中同時應用於解密和IPS的附加功能。

屬性：

- 這是唯一同時影響IPS和Web解密的自定義不解密清單
- 沒有選項可按策略自定義此清單。

配置：控制台->安全->不解密清單->系統提供的不解密清單



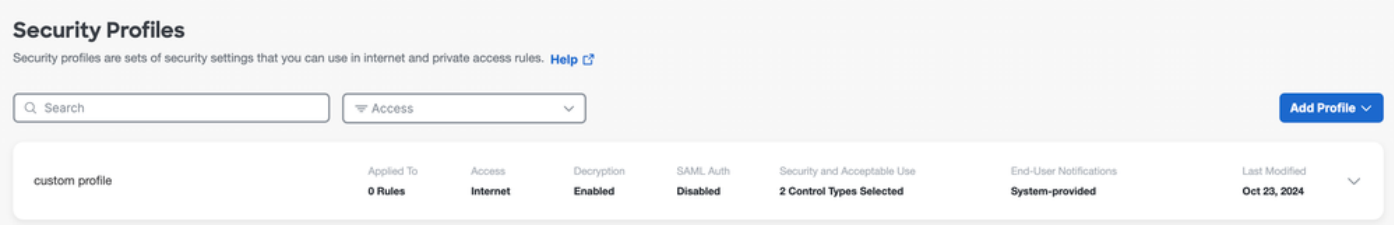
安全性設定檔設定

在「安全性設定檔」設定中，您可以選取「啟用或停用Web解密」，稍後可與「網際網路原則」產生關聯。如果啟用了解密，您可以選擇配置的「不解密」清單之一。

屬性：

- 控制多種安全功能，包括Web解密和不解密清單
- 將提供的系統不解密清單附加到安全配置檔案會同時影響Web解密和IPS解密

配置：控制台->安全->安全配置檔案



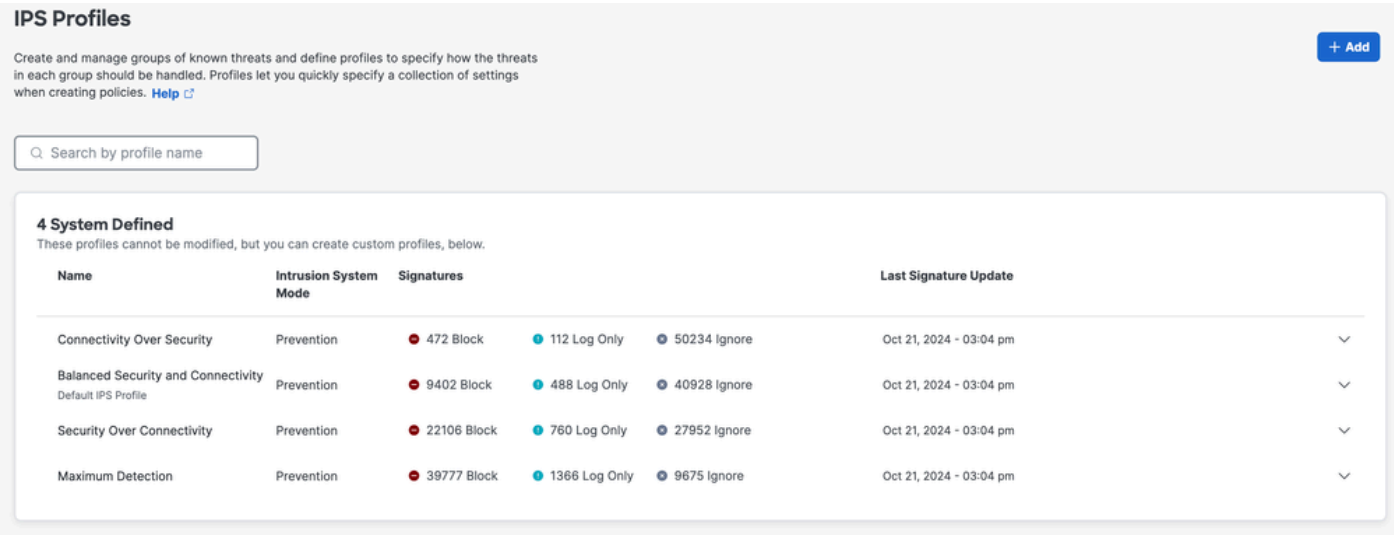
IPS配置檔案

IPS配置檔案設定包括IPS配置檔案的四個主要預定義安全設定。可依據原則設定選取。您可以選擇建立自己的自定義IPS配置檔案，以便進行更嚴格或更靈活的設定。

屬性：

- 包含四個預先定義的IPS安全級別配置檔案
- 可以建立自定義IPS配置檔案

配置：控制台->安全-> IPS配置檔案

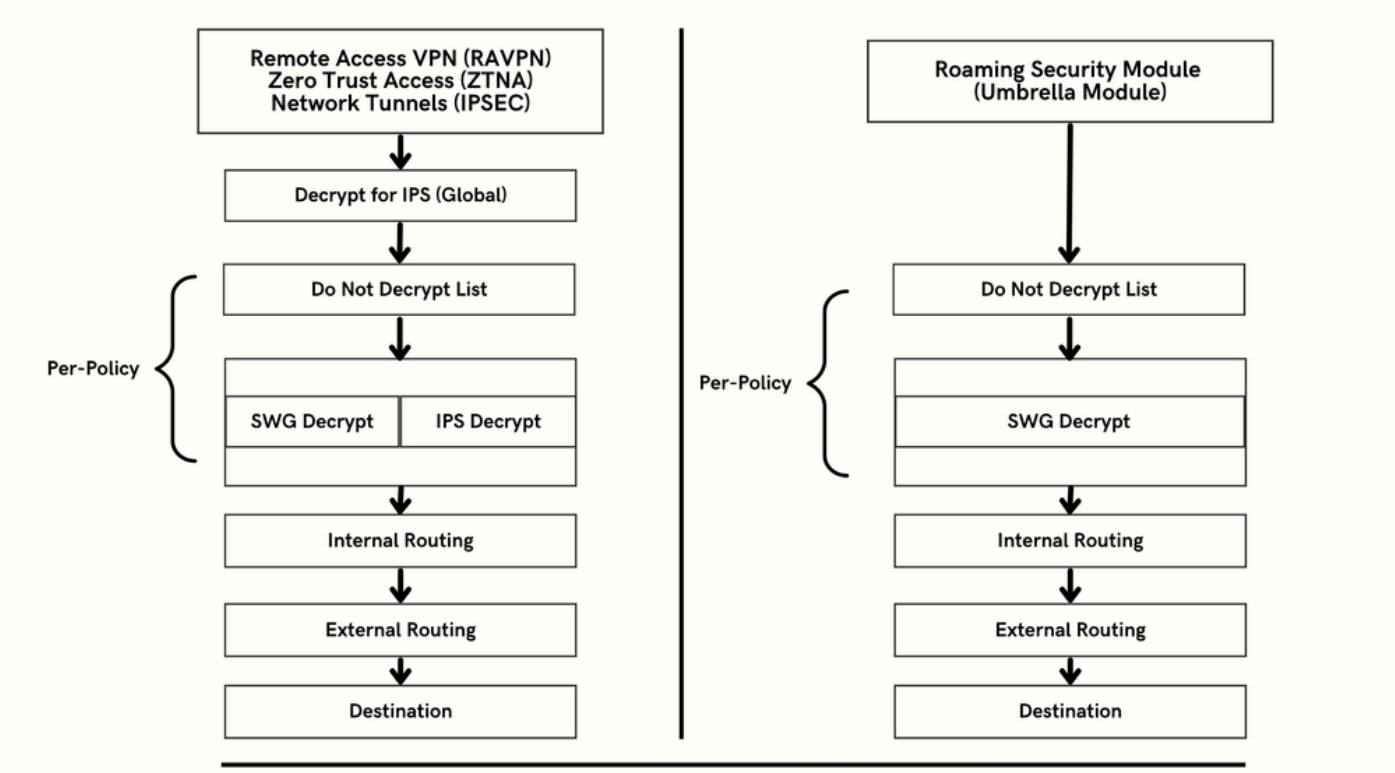


安全訪問中的HTTPS流量

根據連線方法，安全訪問具有不同的流量路徑。

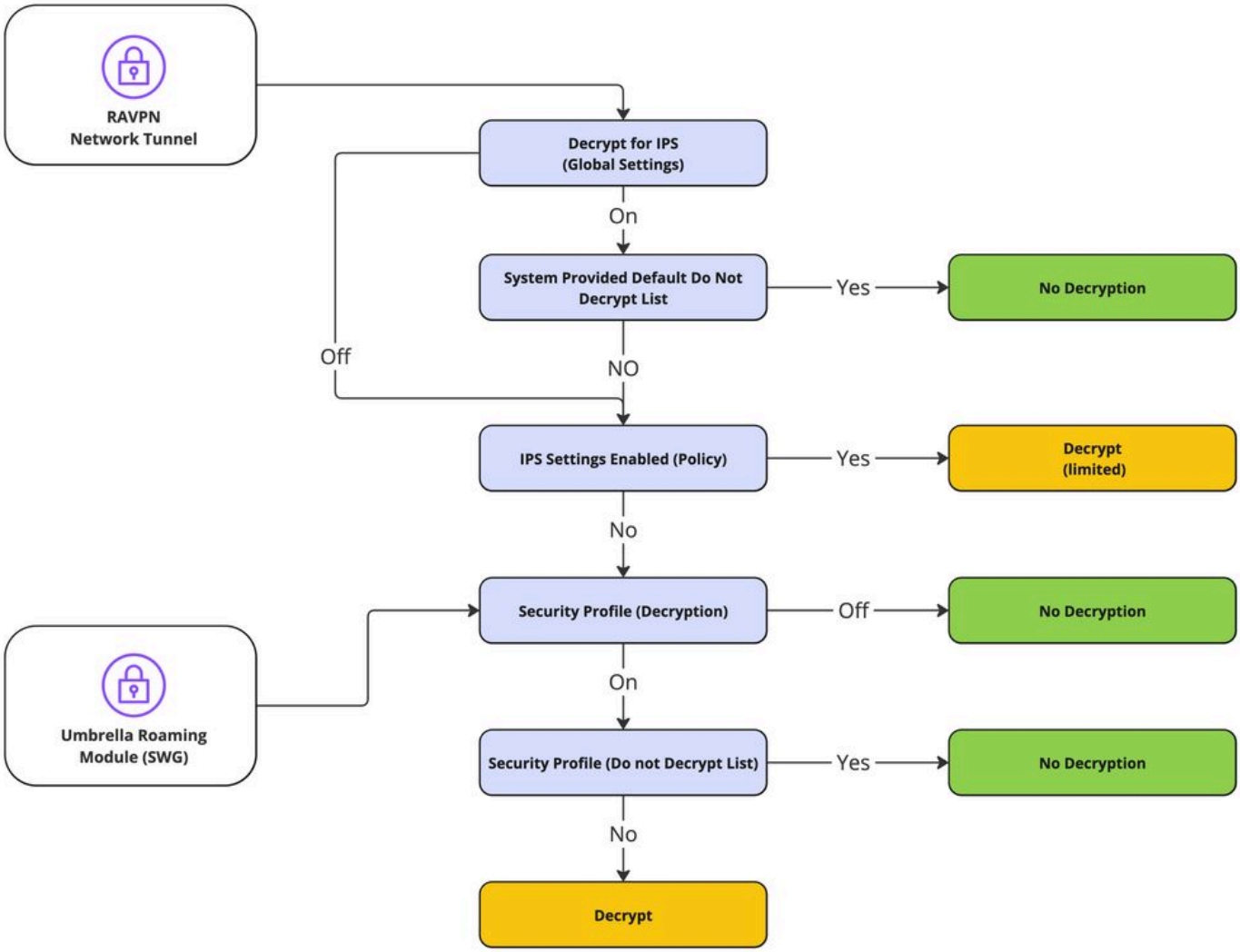
遠端訪問VPN (RAVPN)和零信任訪問(ZTNA)共用相同的元件。

漫遊安全模組（Umbrella模組）具有不同的流量路徑。



預期流量解密的時機

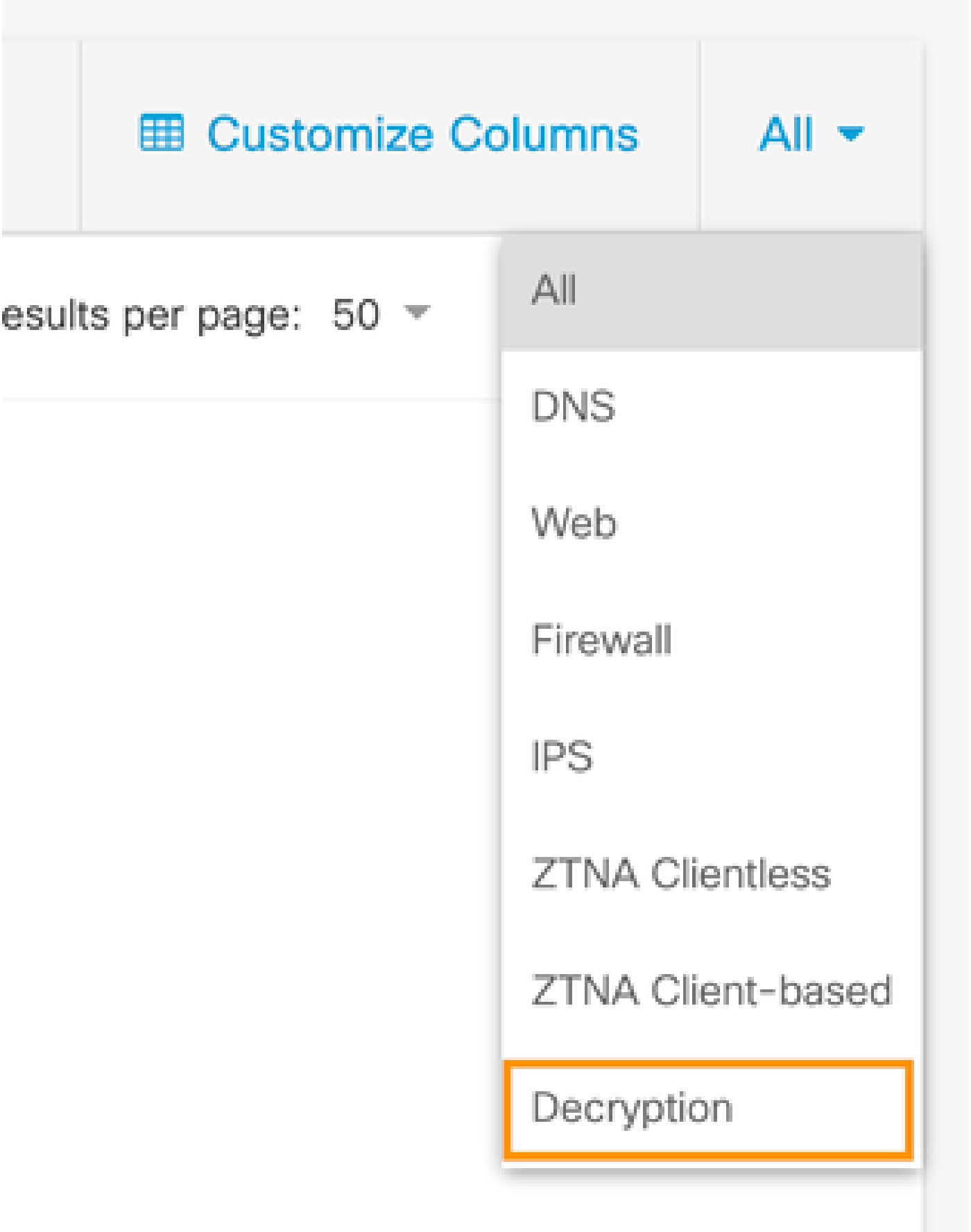
本節詳細說明了操作鏈及其解密或不解密的主要結果。

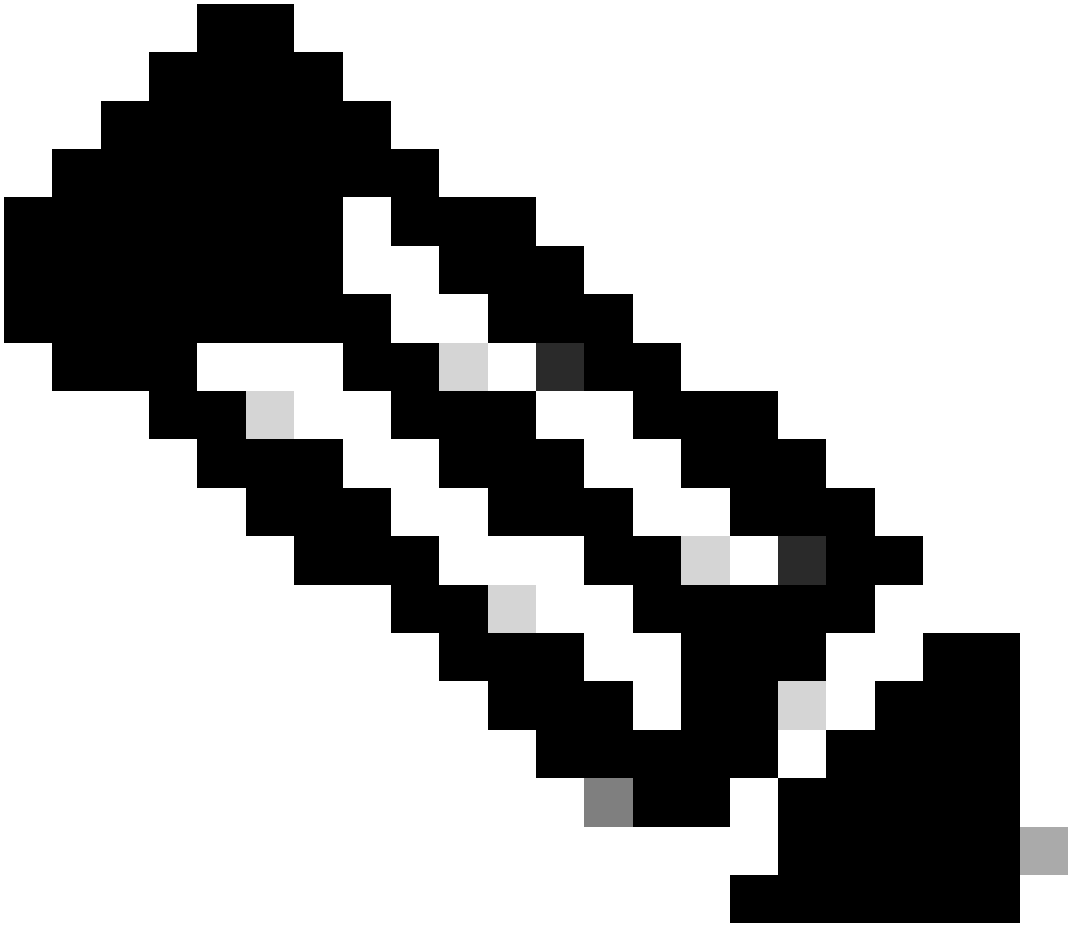


解密流程

解密與IPS相關的記錄與報告

安全訪問包括新的報告部分（解密），可透過控制台->監控->活動搜尋->切換到解密訪問。

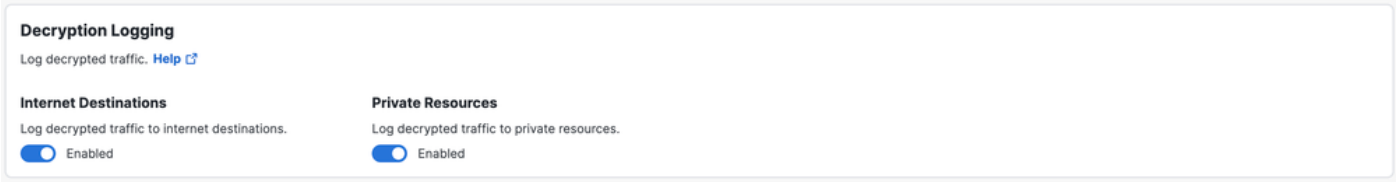

Customize Columns
All
esults per page: 50
All
DNS
Web
Firewall
IPS
ZTNA Clientless
ZTNA Client-based
Decryption



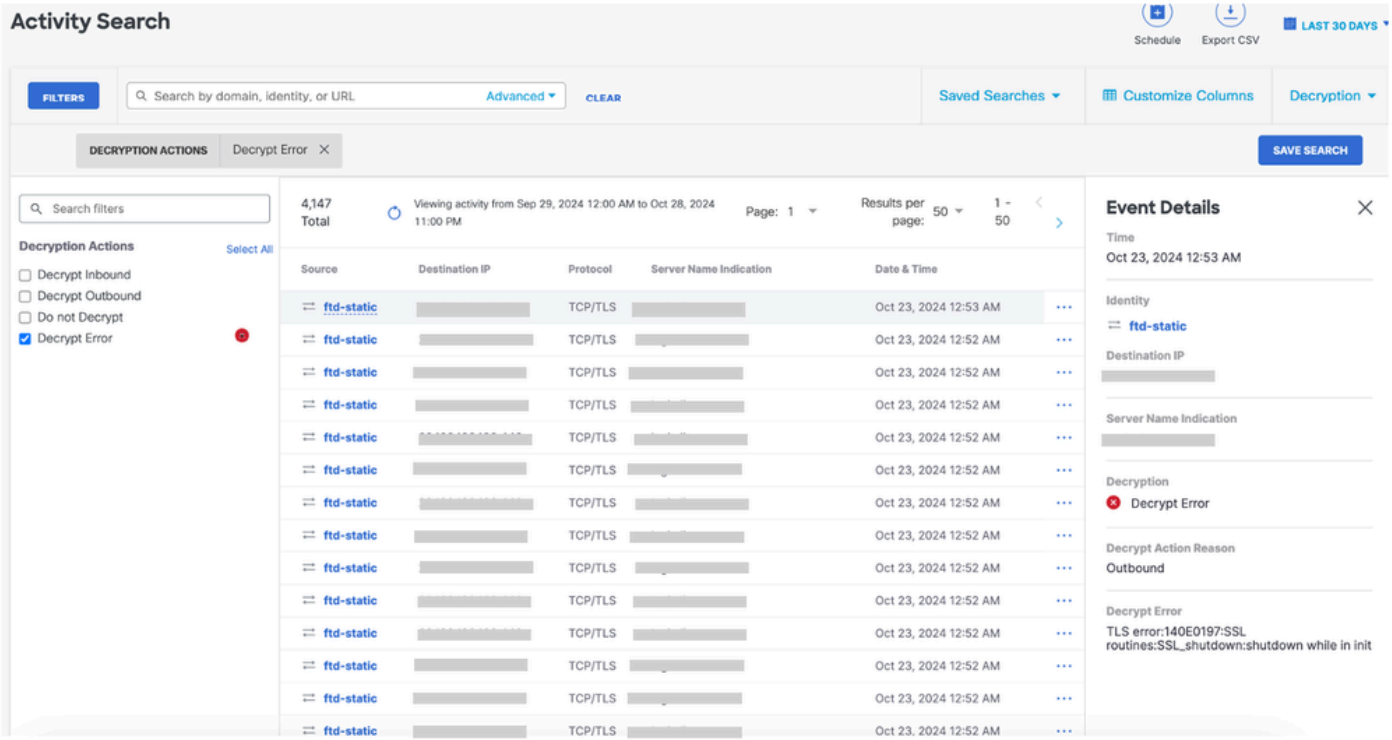
注意：要啟用解密日誌，可以在全局設定中啟用此設定：

控制台->安全->訪問策略->規則預設值和全局設定->全局設定->解密日誌記錄。

解密記錄設定：



解密錯誤的範例：



相關資訊

- Secure Access使用手冊
- 技術支援與下載- Cisco Systems

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。