實施VPN故障排除的平台設定

目錄

簡介

本文檔介紹如何使用Secure Firewall Management Center和Secure Firewall Threat Defense輕鬆組織和識別VPN調試日誌。

必要條件

需求

思科建議您瞭解以下主題：

- 安全防火牆威脅防禦(FTD)
- 安全防火牆管理中心(FMC)

- 對FMC GUI和FTD CLI導航的基本瞭解
- 平台設定的現有策略分配

採用元件

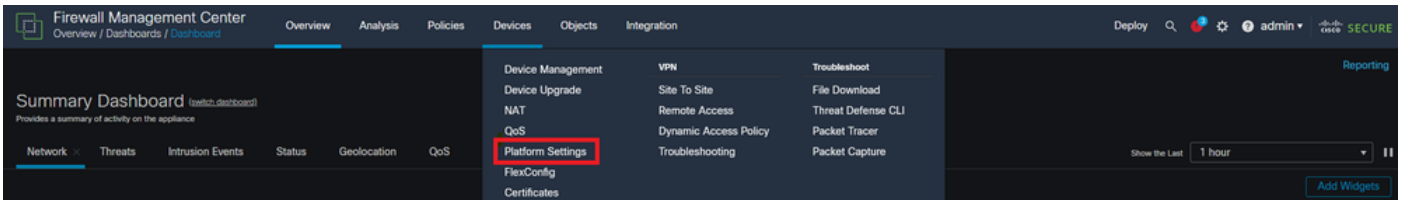
本檔案中的資訊是根據以下軟體版本和硬體版本：

- 防火牆管理中心版本7.3
- 防火牆威脅防禦版本7.3

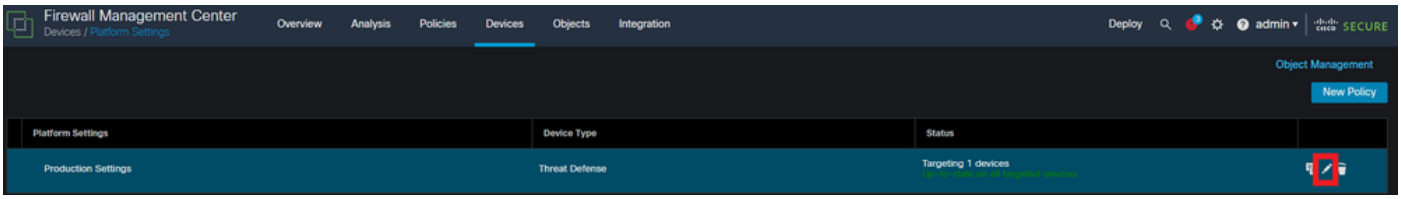
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

防火牆管理中心

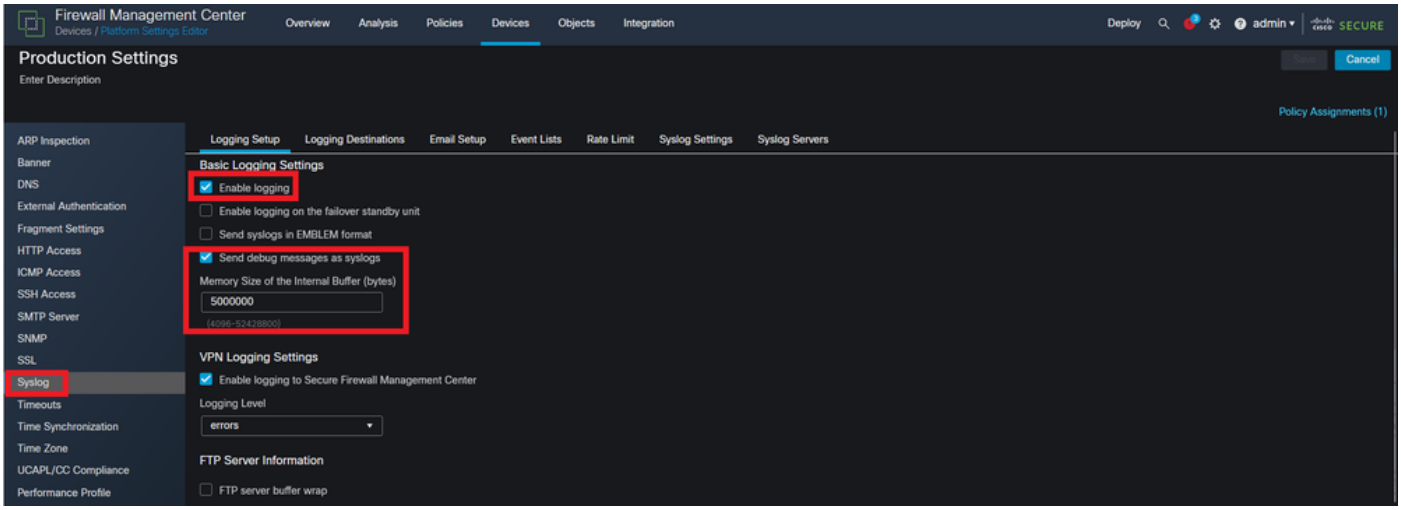
前往 。Devices > Platform Settings



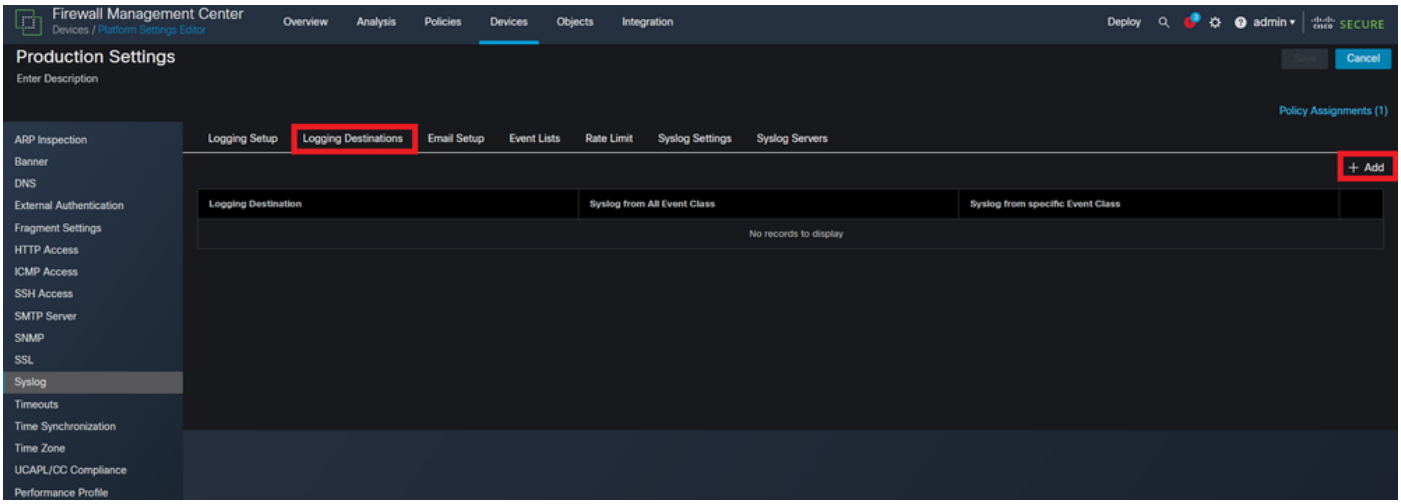
按一下**pencil**copy和delete之間的icon。



導航到Syslog選項左欄中的，並確保和**Enable Logging**啟用**Send debug messages as syslog**該功能。此外，請確保Memory Size of the Internal Buffer，設定的值已足以用於進行故障排除。

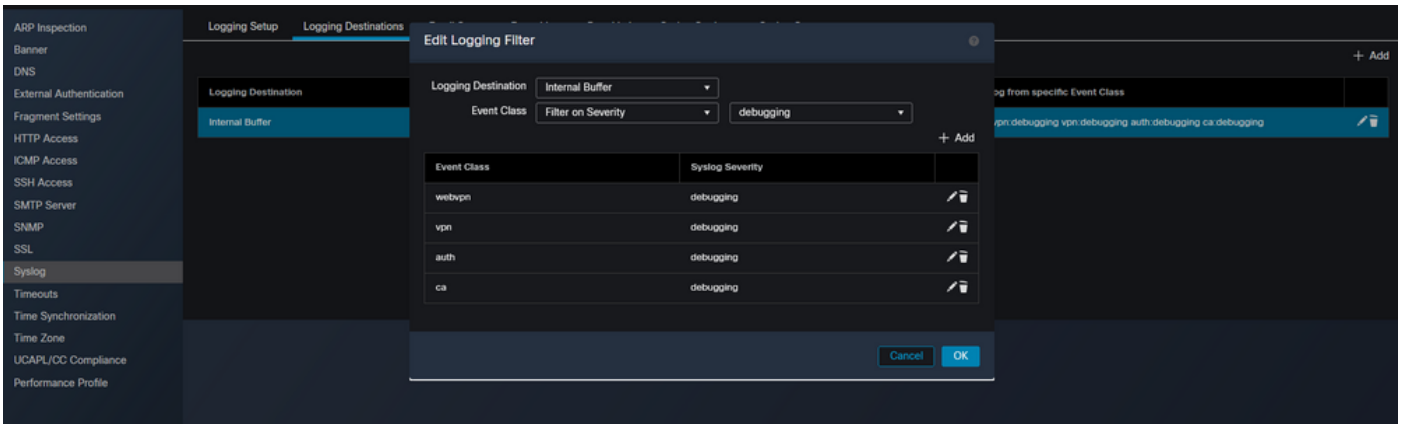


按一下 **Logging Destinations**，然後按一下 **+Add**.



在本節中，日誌記錄目標為管理員的首選項並使**Internal Buffer**用它。更改為**Event Class Filter on Severity and debugging**.，完成此操作後，按一下+Add並選擇webvpn、vpn auth、和caSyslog嚴重性為debugging。此步驟允許管理員將這些調試輸出篩選到特定系統日誌消息711001。這些調試輸出可以根據故障排除型別進行修改。但是，在本示例中選擇的選項涵蓋最常見的「站點到站點」、「遠端訪問」和AAA VPN相

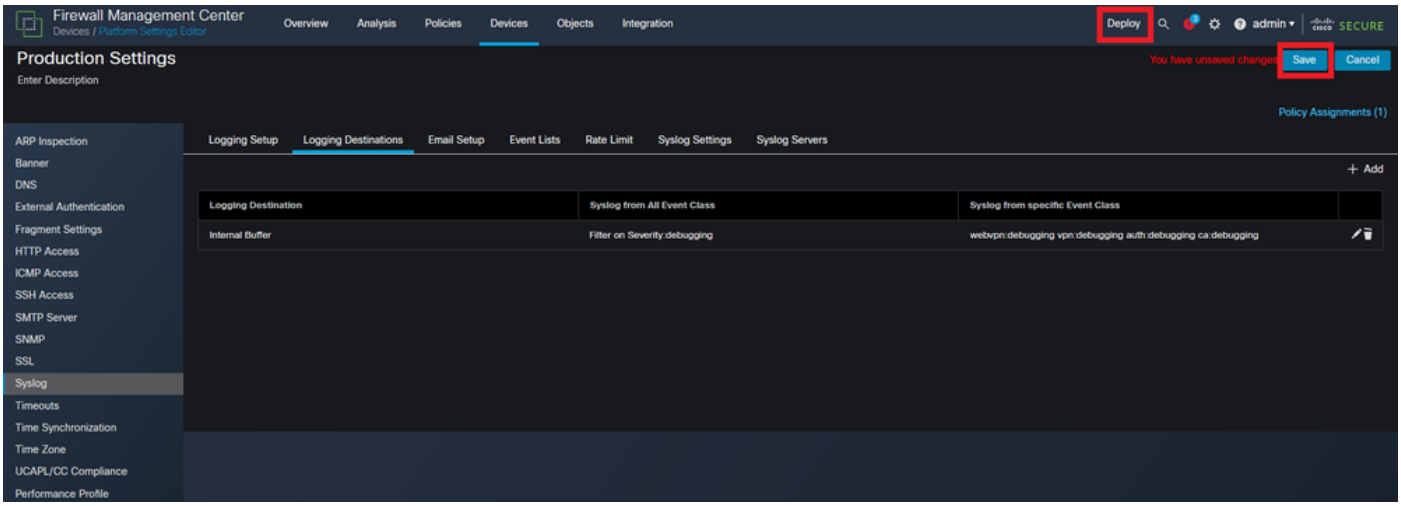
關問題。



為調試建立事件類和過濾器。

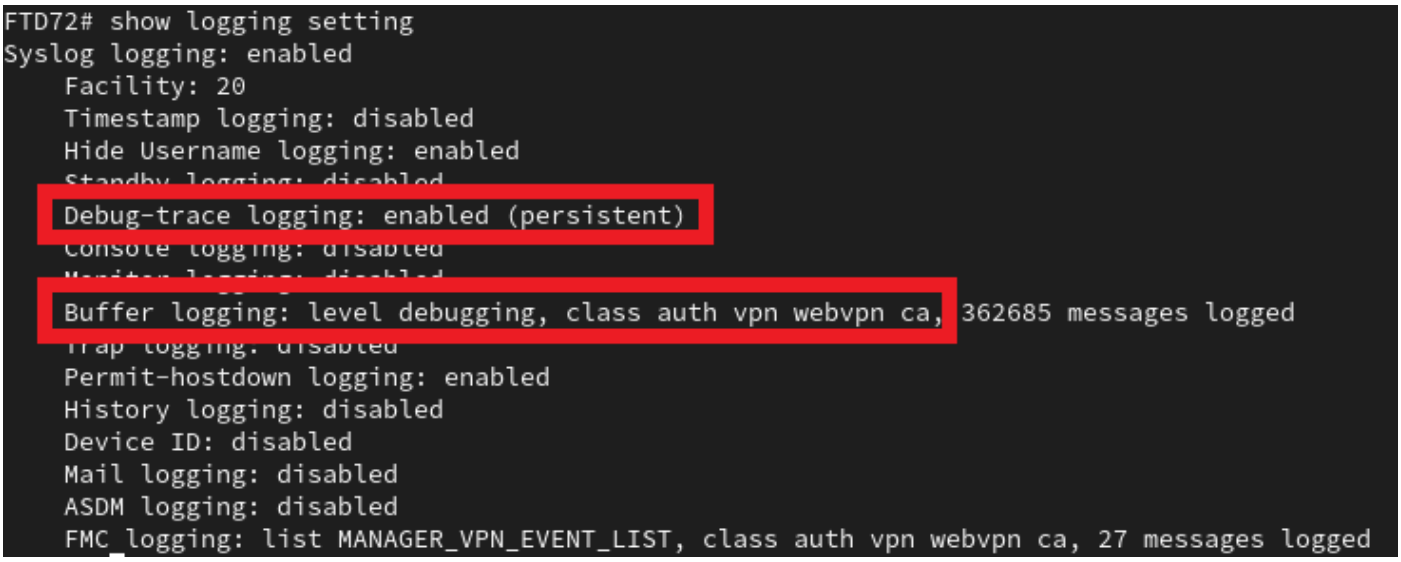
警告：這會將「緩衝區日誌記錄級別」更改為調試，並將為內部緩衝區指定的類記錄調試事件。建議將此日誌記錄方法用於故障排除，而不是長期使用。

Choose Save 在右上角，然後配Deploy置將更改。



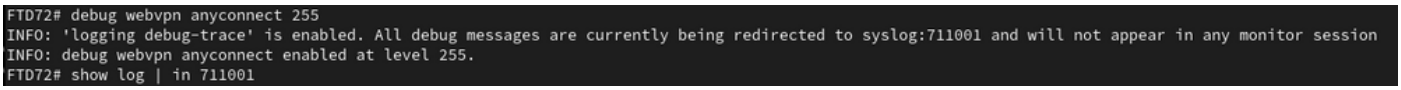
防火牆威脅防禦

導覽至FTD CLI，然後發出命令show logging setting。此處的設定反映在FMC上所做的更改。確保啟用了debug-trace logging ，並且緩衝區日誌記錄與指定的類和日誌記錄級別匹配。



在FTD CLI中顯示日誌記錄設定。

最後，應用調試以確保日誌被重定向到syslog:711001。在此例中debug webvpn anyconnect 255，將應用。這將觸發日誌記錄debug-trace通知，讓管理員知道這些調試已重定向。若要檢視這些偵錯，請發出命令show log | in 711001。現在，此系統日誌ID僅包含管理員應用的相關VPN調試。可以使用清除日誌緩衝區清除現有日誌。



顯示所有VPN調試都重定向到syslog711001。

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）。