CS-MARS — 新增並配置IPS感測器作為報告裝置

目錄

簡介

本文檔介紹如何準備思科安全入侵防禦系統(IPS)裝置和任何已配置的虛擬感測器，以充當思科安全監控、分析和響應系統(CS-MARS)的報告裝置。

必要條件

需求

對於Cisco IPS 5.x、6.x和7.x裝置，MARS使用SSL上的SDEE獲取日誌。因此，MARS必須能夠通過HTTPS訪問感測器。為了準備感測器，必須在感測器上啟用HTTP伺服器，啟用TLS以允許HTTPS訪問，並確保MARS的IP地址被定義為允許的主機，該主機可以訪問感測器並獲取事件。如果已將感測器配置為允許從網路上的有限主機或子網訪問，可以使用**access-list ip_address/netmask**命令啟用此訪問。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 運行軟體版本4.2.x及更高版本的Cisco Secure MARS裝置
- 運行軟體版本6.0及更高版本的Cisco 4200系列IPS裝置

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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

相關產品

此配置也可用於以下感測器：

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

設定

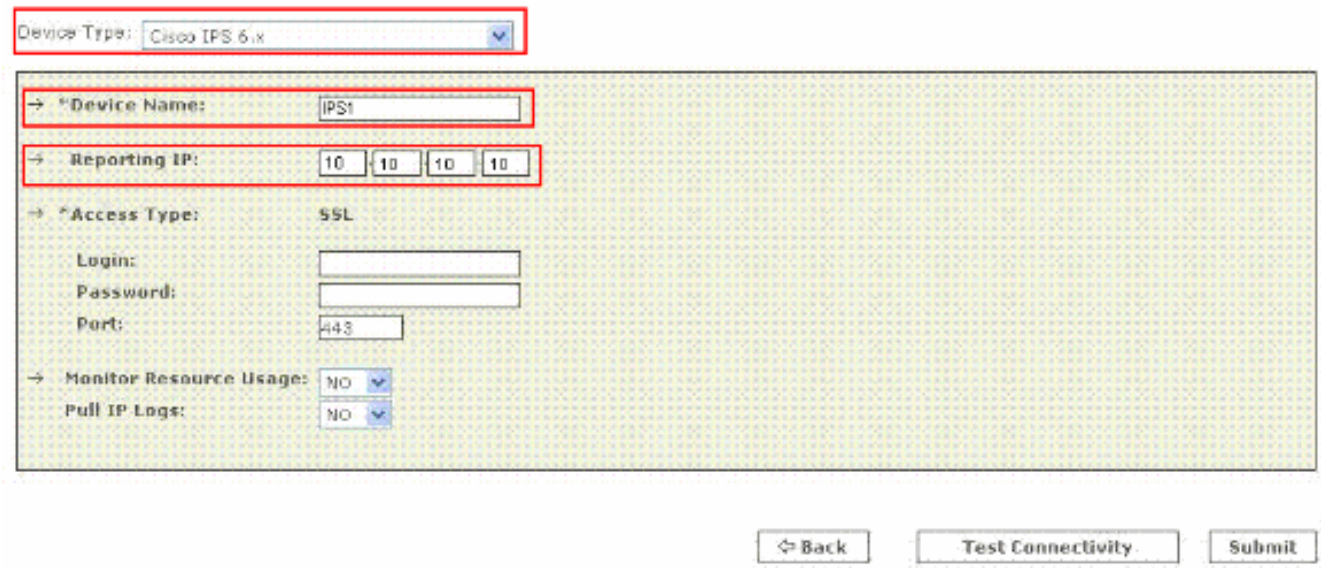
本節提供有關如何向思科安全監控、分析和響應系統(CS-MARS)裝置新增和配置Cisco Secure Intrusion Prevention System(IPS)感測器的資訊。

在MARS中新增和配置Cisco IPS 6.x或7.x裝置

在MARS中定義Cisco IPS 6.x或7.x裝置時，可以發現裝置上配置的任何虛擬感測器。當您發現這些虛擬感測器時，這允許MARS按虛擬感測器分離報告的事件。它還允許您調整每個虛擬感測器的受監控網路清單，從而提高所需報告的準確性。

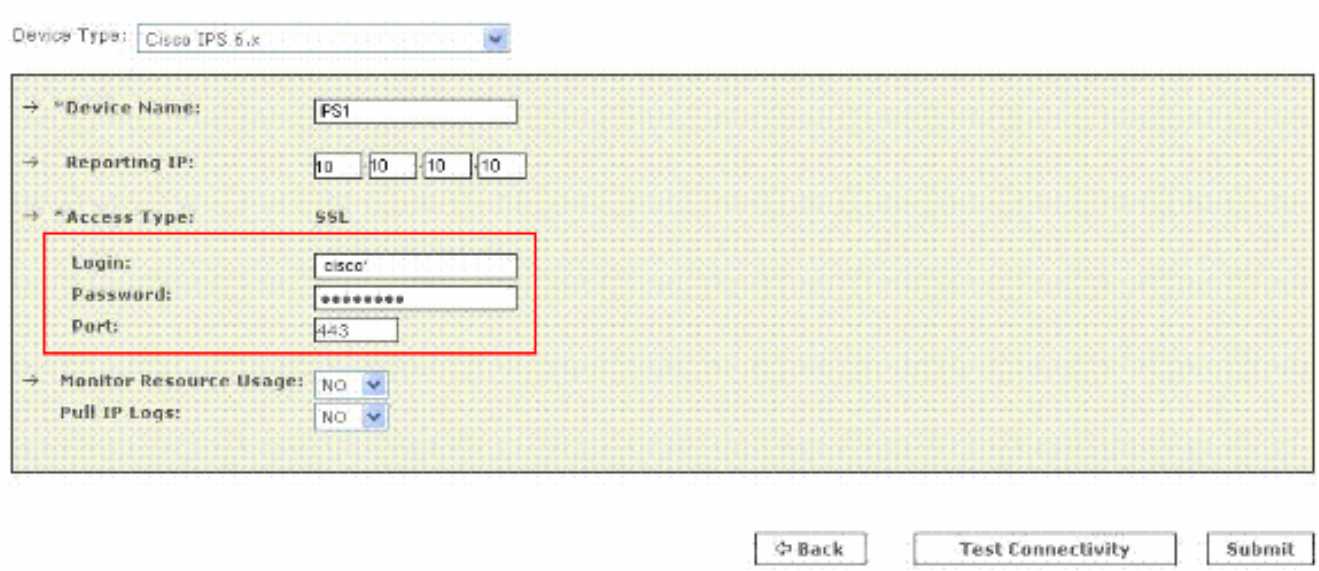
完成以下步驟，以便在MARS中新增和配置Cisco IPS 6.x或7.x裝置：

1. 選擇**Admin > System Setup > Security and Monitor Devices**。然後，按一下**Add**。
2. 從Device Type清單中選擇**Cisco IPS 6.x或Cisco IPS 7.x**。現在在**Device Name**欄位中輸入感測器的主機名，如下所示。IPS1是本示例中使用的裝置名稱。「Device Name（裝置名稱）」值必須與配置的感測器名稱相同。



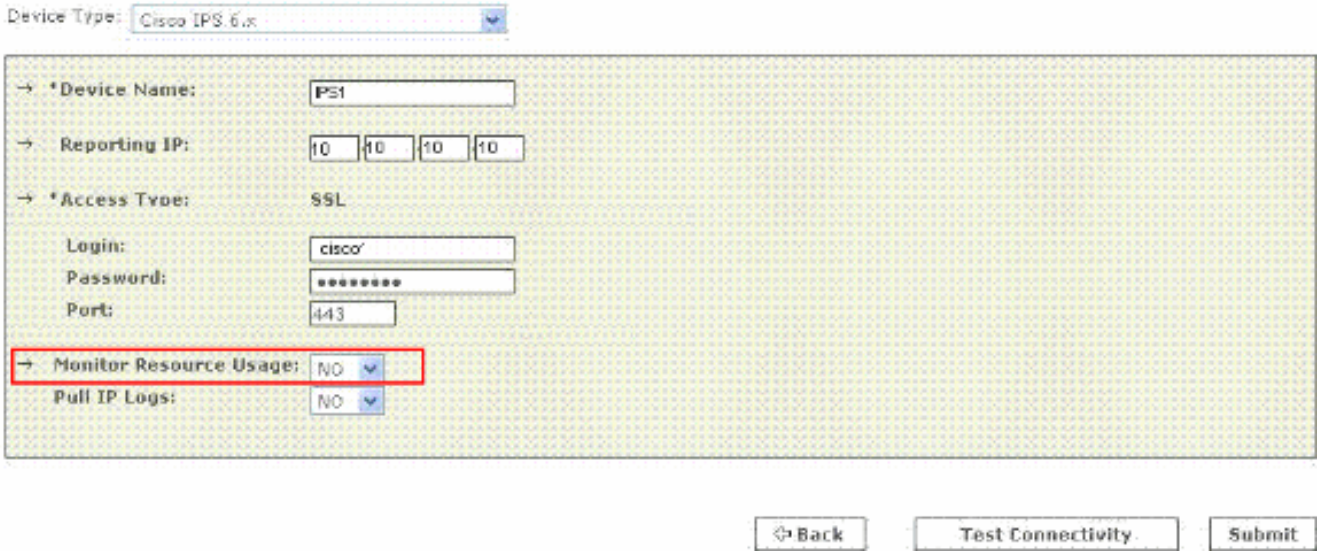
現在，在**Reporting IP**欄位中輸入管理IP地址。報告IP地址與管理IP地址相同。

3. 在**登入**欄位中，輸入與用於訪問報告裝置的管理帳戶關聯的使用者名稱。現在，在**Password**欄位中，輸入與**Login**欄位中指定的使用者名稱相關聯的**密碼**。在此範例中，**使用者名稱**為**cisco**，而使用**密碼**為**cisco123**。在**Port**欄位中輸入感測器上運行的Web伺服器監聽的TCP埠**號**。預設HTTPS埠為443。

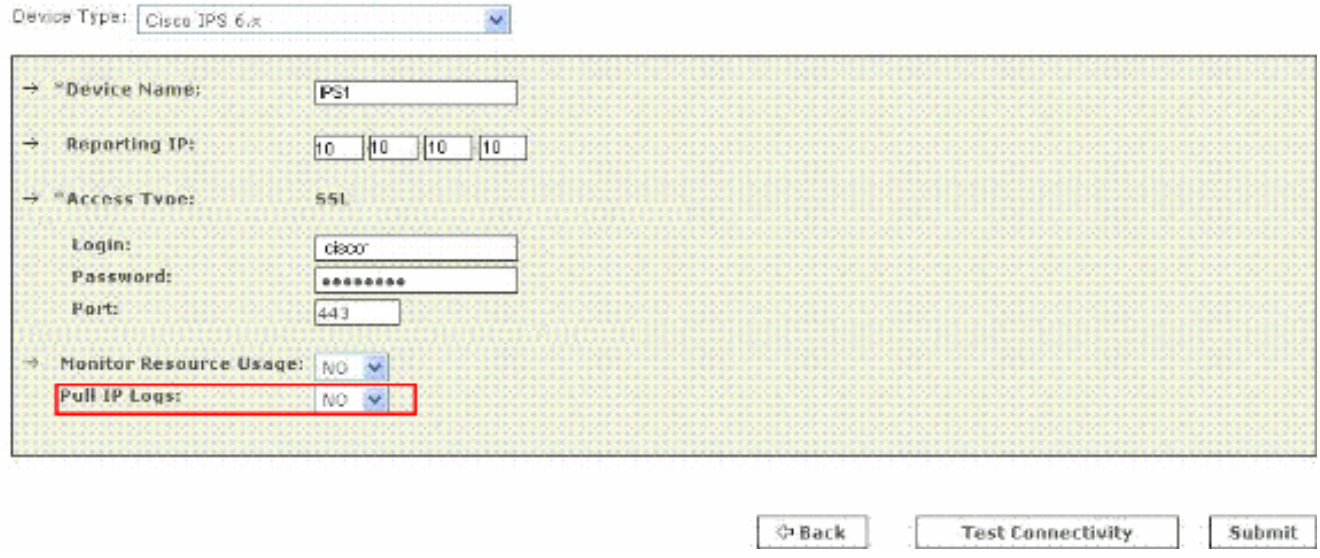


注意：雖然可以僅配置HTTP，但MARS需要HTTPS。

4. 現在驗證在**Monitor Resource Usage**清單中是否選擇了**NO**。當Monitor Resource Usage選項出現在此頁面上時，它對Cisco IPS不起作用。

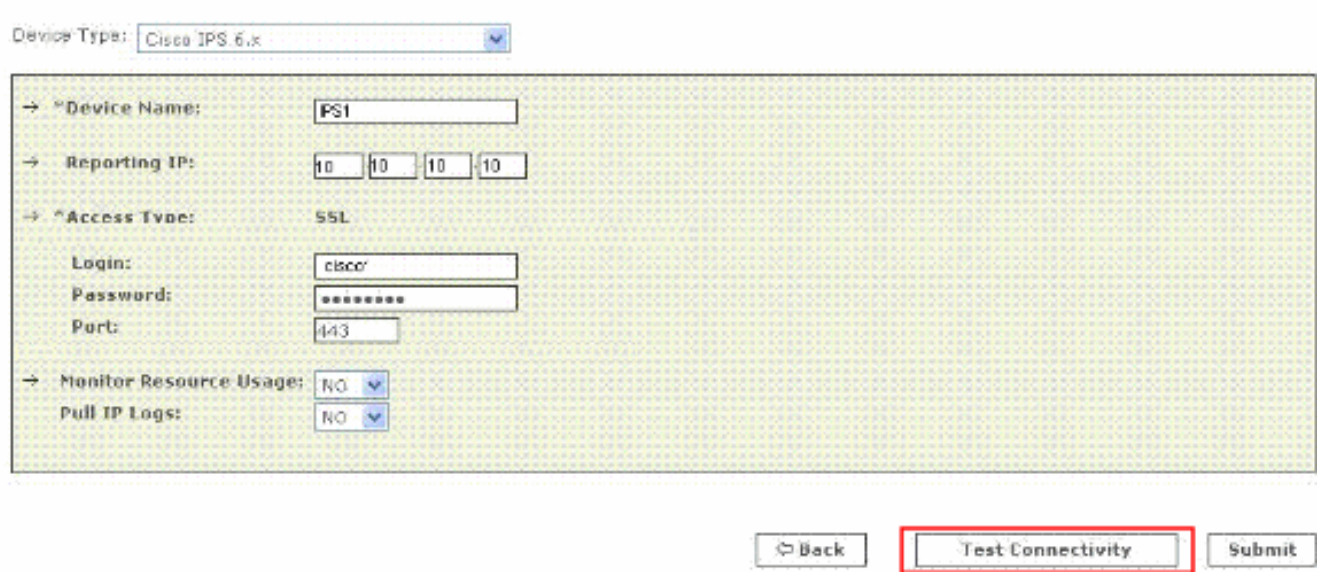


5. 要從感測器提取IP日誌，請從**提取IP日誌**清單中選擇**Yes**。這是一項可選功能，可在需要時使用。

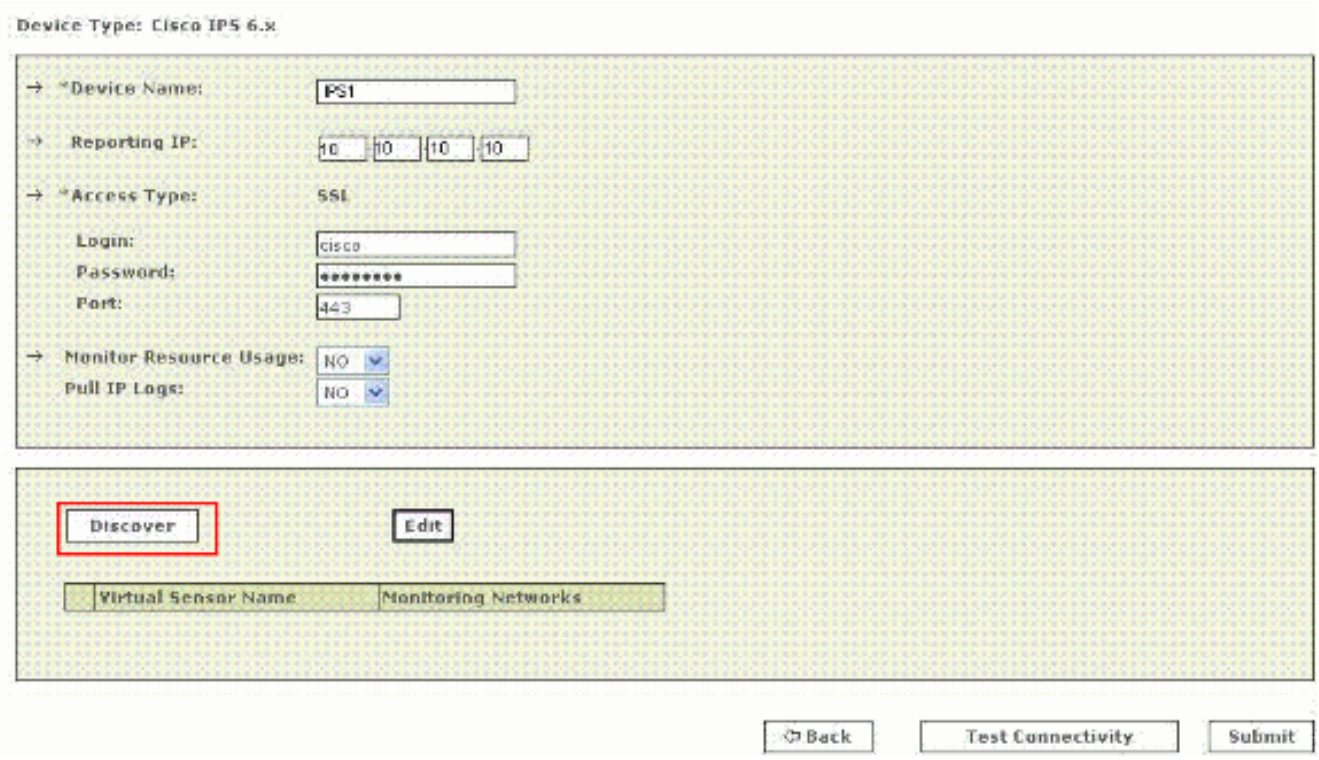


此設定適用於整個感測器，包括為虛擬感測器警報生成的日誌。

6. 按一下**Test Connectivity**以驗證配置並啟用虛擬感測器的發現。

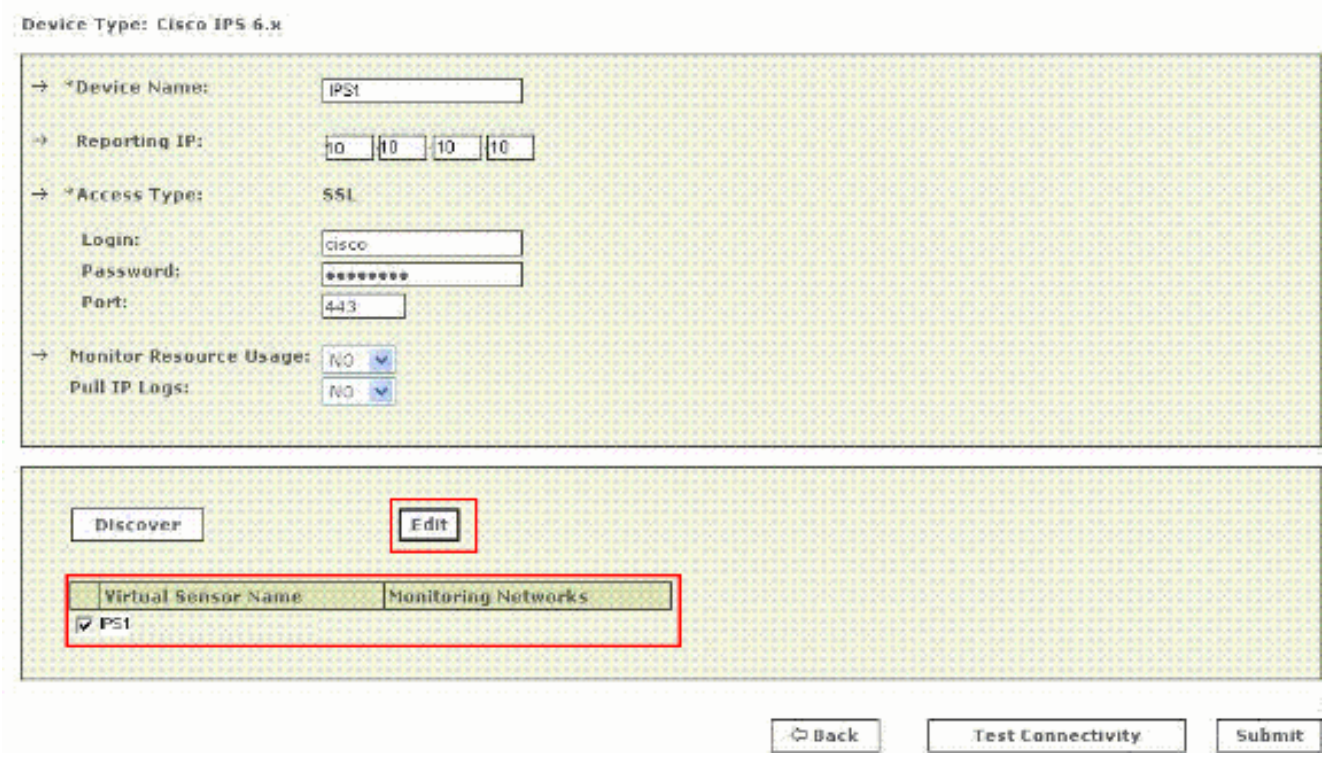


7. 按一下「**Discover**」以發現任何已定義的虛擬感測器。

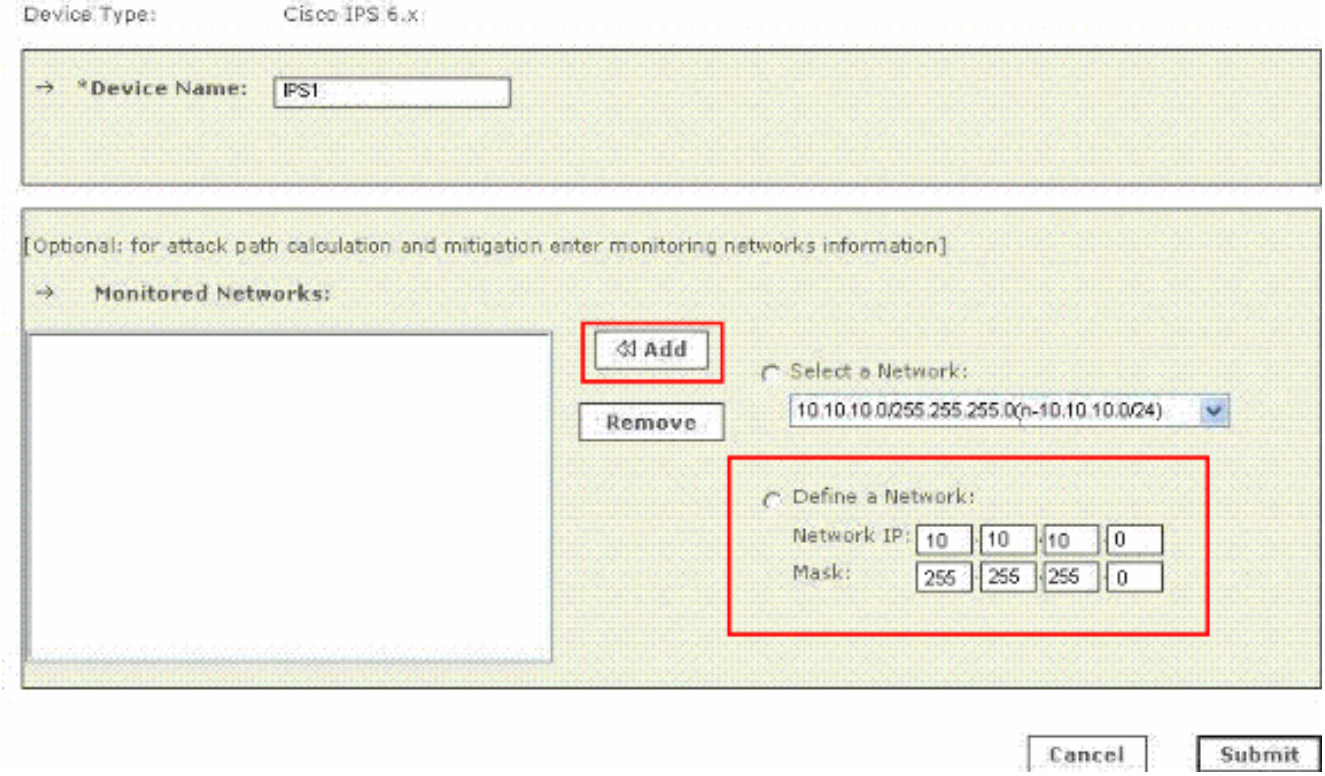


注意：MARS不知道對感測器所做的更改。無論何時更改虛擬感測器設定，您都必須在該感測器配置頁面上按一下**Discover**才能刷新MARS中的虛擬感測器詳細資訊。

8. 選擇「Virtual Sensor Name（虛擬感測器名稱）」旁邊的覈取方塊，然後按一下**Edit**，為每個虛擬感測器定義受監控的網路。此時會顯示「IPS模組」頁面，如下所示。

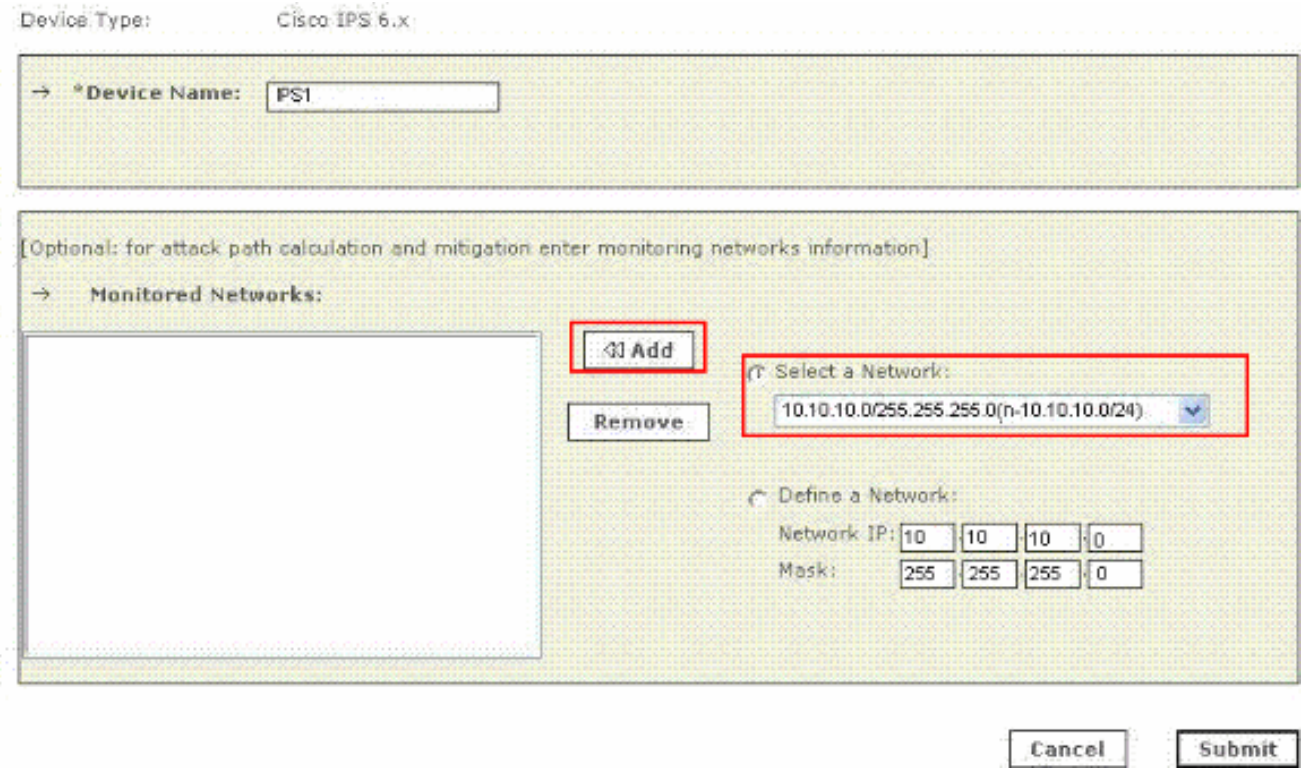


9. 要計算和緩解攻擊路徑，請指定感測器所監視的網路。選擇**定義網路**單選按鈕以手動定義網路。然後完成以下步驟以定義網路：在**Network IP**欄位中輸入網路地址。在**Mask**欄位中輸入相應的網路掩碼值。按一下「**Add**」將指定的網路移到「Monitored Networks」欄位中。如果需要定義更多網路，請重複前面的步驟。



注意：這是一個可選功能，如果需要，可以跳過此功能。

10. 按一下**Select a Network**單選按鈕以選擇連線到裝置的網路。然後完成以下步驟以選擇網路：從**Select a Network**(選擇**網路)清單中選擇**網路。按一下「**Add**」將指定的網路移到「Monitored Networks」欄位中。如果需要選擇更多網路，請重複前面的步驟。



注意：這是一個可選功能，如果需要，可以跳過此功能。

11. 對每個虛擬感測器重複**步驟8**到**步驟10**。
12. 按一下「**Submit**」以儲存變更內容。裝置名稱顯示在Security and Monitoring Information清單下。提交操作在資料庫表中記錄更改。但是，它不會將更改載入到MARS裝置的工作記憶體中。啟用操作將提交的更改載入到工作記憶體中。
13. 按一下**Activate**以啟用MARS以開始從此裝置對事件進行會話化。MARS開始設定此模組生成的事件的會話，並使用定義的檢查和丟棄規則評估這些事件。裝置在啟用之前向MARS發佈的任何事件都可以以裝置的報告IP地址作為匹配條件進行查詢。請參閱啟用報告和緩解裝置。有關啟用操作的詳細資訊。

驗證MARS是否從Cisco IPS裝置獲取事件

在網路中建立良性事件以驗證資料流是很常見的。完成以下步驟，驗證Cisco IPS裝置和MARS之間的資料流：

1. 在Cisco IPS裝置上，啟用2000和2004簽名並發出警報。特徵碼監控ICMP消息(ping)。
2. 對Cisco IPS裝置偵聽的子網上的裝置執行Ping操作。這些事件由MARS生成和拉動。
3. 驗證事件是否顯示在MARS Web介面中。您可以使用Cisco IPS裝置執行查詢。
4. 驗證資料流後，您可以在Cisco IPS裝置上禁用2000和2004簽名。**注意**：如果在MARS Web介面中配置Cisco IPS裝置期間，測試連線操作未失敗，則通訊已啟用。使用此任務可以進一步驗證警報是否正確生成和提取。

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- 思科安全監控、分析和回應系統支援頁面
- 思科入侵防禦系統支援頁面
- 思科安全監控、分析和響應系統 — 相容性資訊
- 要求建議 (RFC)
- 技術支援與文件 - Cisco Systems