Cisco安全IPS — 不包括誤報警報

目錄

簡介

本檔案介紹思科安全入侵防禦系統(IPS)的誤報排除。

必要條件

需求

本文件沒有特定需求。

採用元件

本檔案中的資訊是根據Cisco Secure Intrusion Prevention System(IPS)版本7.0和Cisco IPS manager Express 7.0。

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。

慣例

如需文件慣例的詳細資訊，請參閱思科技術提示慣例。

誤報和誤報警報

當給定資料包或資料包序列與Cisco安全IPS簽名中定義的已知攻擊配置檔案的特性匹配時，Cisco安全IPS會觸發警報。一個關鍵的IPS特徵碼設計准則是儘可能減少誤報和漏報的發生。

當IPS報告某些良性活動為惡意活動時，就會發生誤報（良性觸發器）。這需要人類干預來診斷事件。大量誤報會大量消耗資源，而分析這些誤報所需的專業技能成本高昂且難以找到。

當IPS未檢測到並報告實際的惡意活動時，就會出現假陰性。其後果可能是災難性的，在發現新的漏洞攻擊和駭客技術時，必須不斷更新簽名。最小化假負值被賦予非常高的優先順序，有時會犧牲較高的誤報率。

由於IPS用來檢測惡意活動的特徵碼的性質，如果不嚴重降低IPS的有效性或嚴重破壞組織的計算基礎架構（如主機和網路），幾乎不可能完全消除誤報和漏報。 部署IPS時的自定義調整將誤報降至最低。當計算環境發生變化時（例如，部署新系統和應用程式時），需要進行定期重新調整。Cisco Secure IPS提供靈活的調整功能，可在穩態操作期間將誤報降至最低。

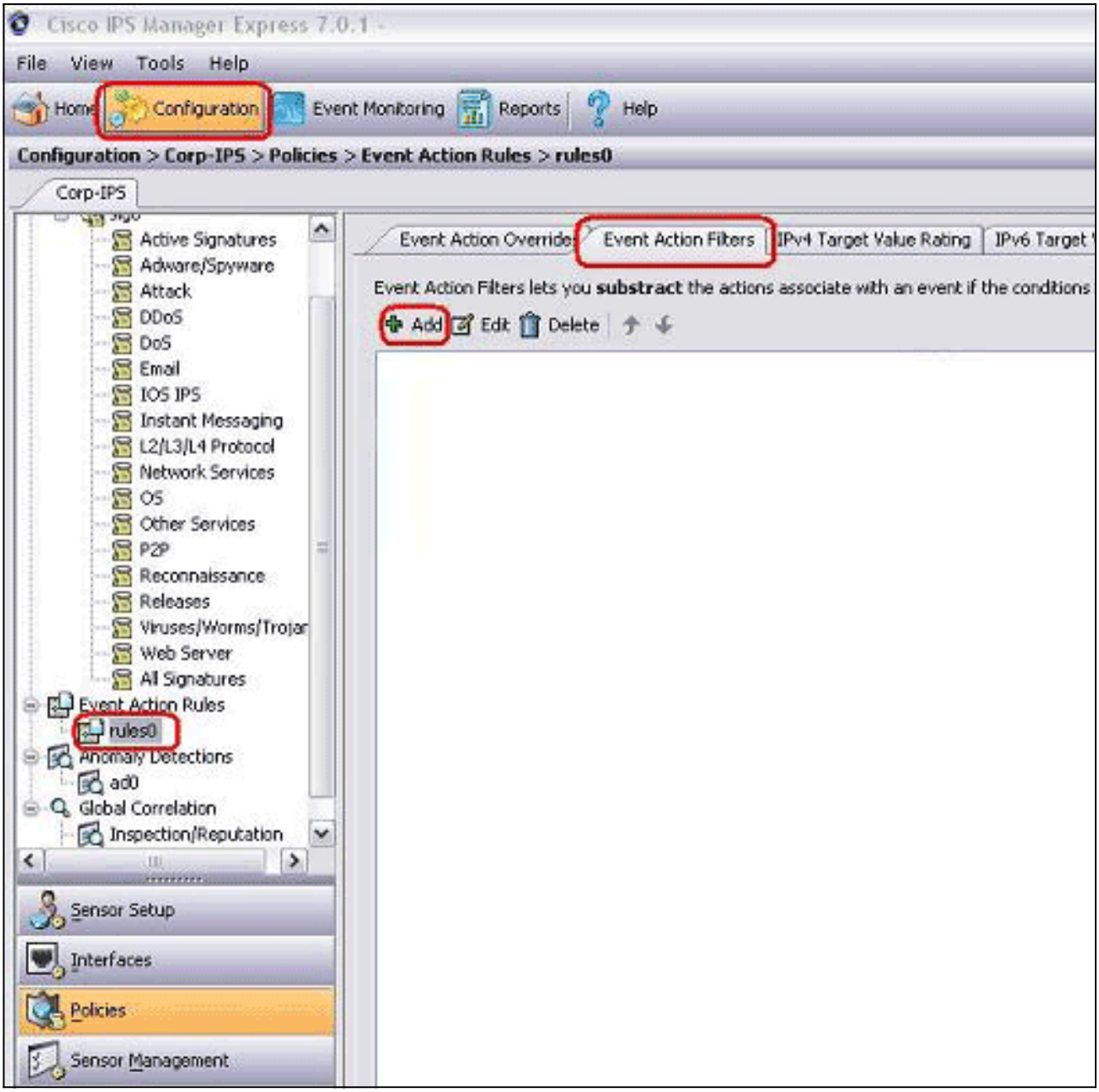
Cisco安全IPS排除機制

Cisco Secure IPS提供從特定主機或網路地址排除特定特徵碼或將特定特徵碼排除到特定主機或網路地址的功能。從通過此機制明確排除的主機或網路觸發排除的簽名時，不會生成警報圖示或日誌記錄。例如，網路管理站可能透過執行ping掃描執行網路探索，執行ping掃描會觸發具有回應簽章（簽章ID 2100）的ICMP網路掃描。 如果排除該簽名，則無需在每次運行網路發現過程時分析警報並刪除它。

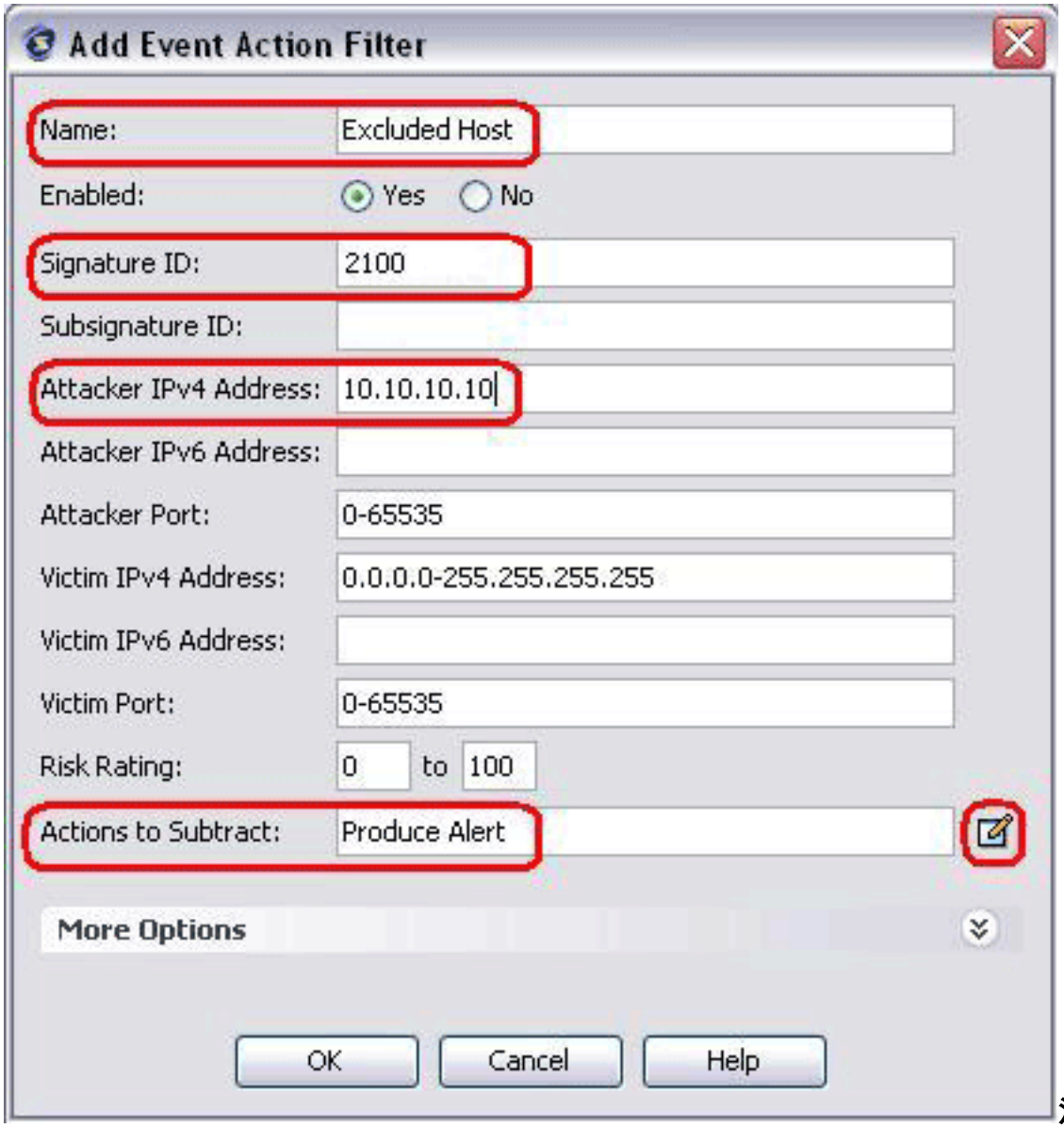
排除主機

完成以下步驟，以排除特定主機（來源IP位址）無法產生特定簽署警告：

1. 選擇**Configuration > Corp-IPS > Policies > Event Action Rules > rules0**，然後按一下**Event Action Filters**頁籤。



2. 按一下「**Add**」。
3. 在相應的欄位中鍵入過濾器名稱、簽名ID、攻擊者的IPv4地址和要減除的操作，然後按一下



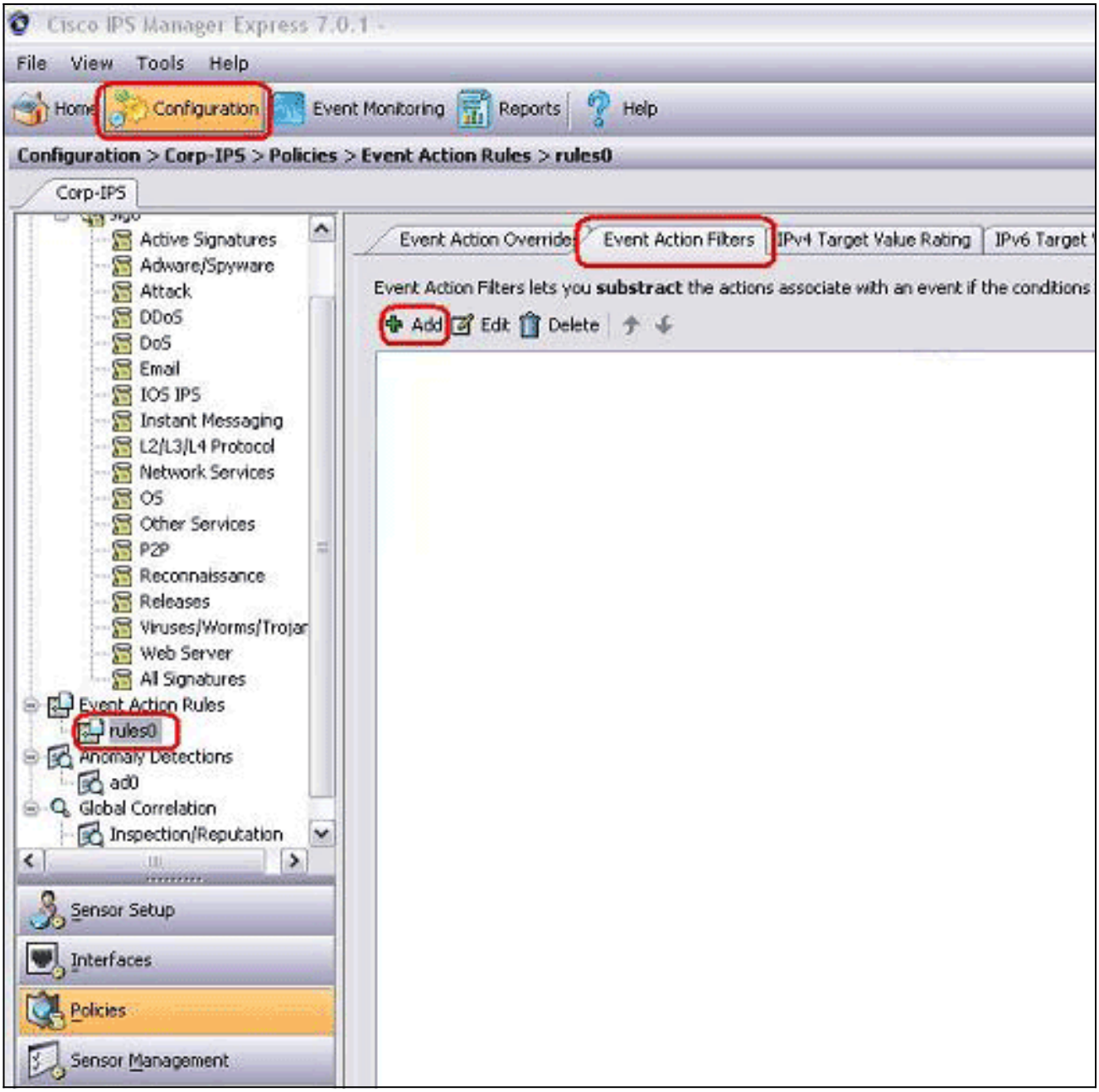
OK。**注意**：如果需要從不同的網路中排除多個IP地址，可以使用逗號作為分隔符。但是，如果使用逗號，請避免使用逗號後的尾部空格；否則您可能會收到錯誤。**註：此**外，您還可以使用「事件變數」頁籤中定義的變數。當必須在多個事件操作過濾器中重複相同的值時，這些變數很有用。必須使用美元符號($)作為變數的字首。變數可以是以下格式之一：完整IP地址；例如10.77.23.23。IP地址範圍；例如10.9.2.10-10.9.2.155。IP地址範圍集；例如，172.16.33.15-172.16.33.100、192.168.100.1-192.168.100.11。

排除網路

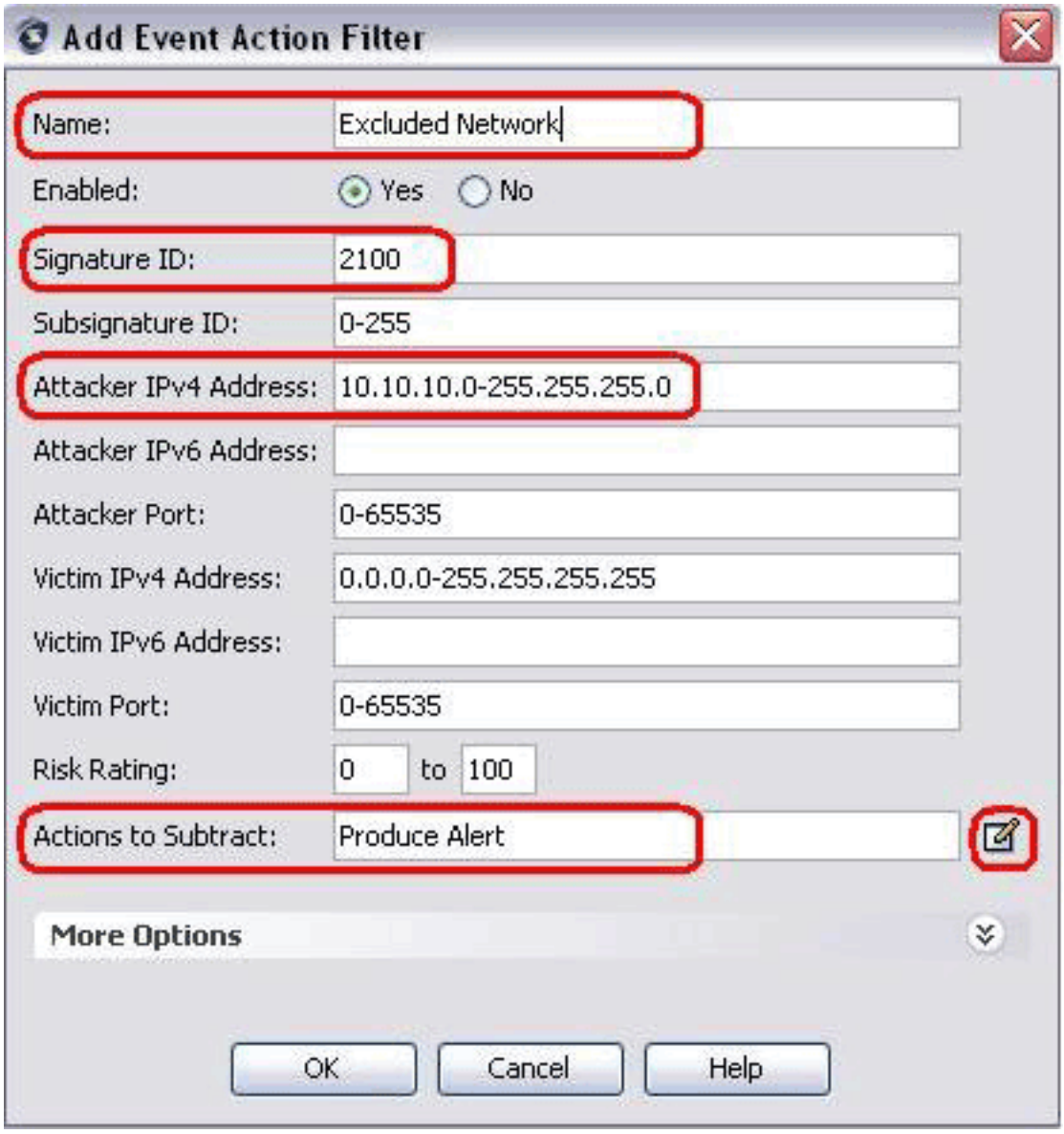
Event Action Filter（事件操作過濾器）還排除根據源或目標網路地址觸發警報的特定簽名。

完成以下步驟，排除網路生成特定簽名警報：

1. 按一下**Event Action Filters**頁籤。



2. 按一下「Add」。
3. 在相應的欄位中鍵入過濾器名稱、簽名ID、帶子網掩碼的網路地址和要減除的操作，然後按一

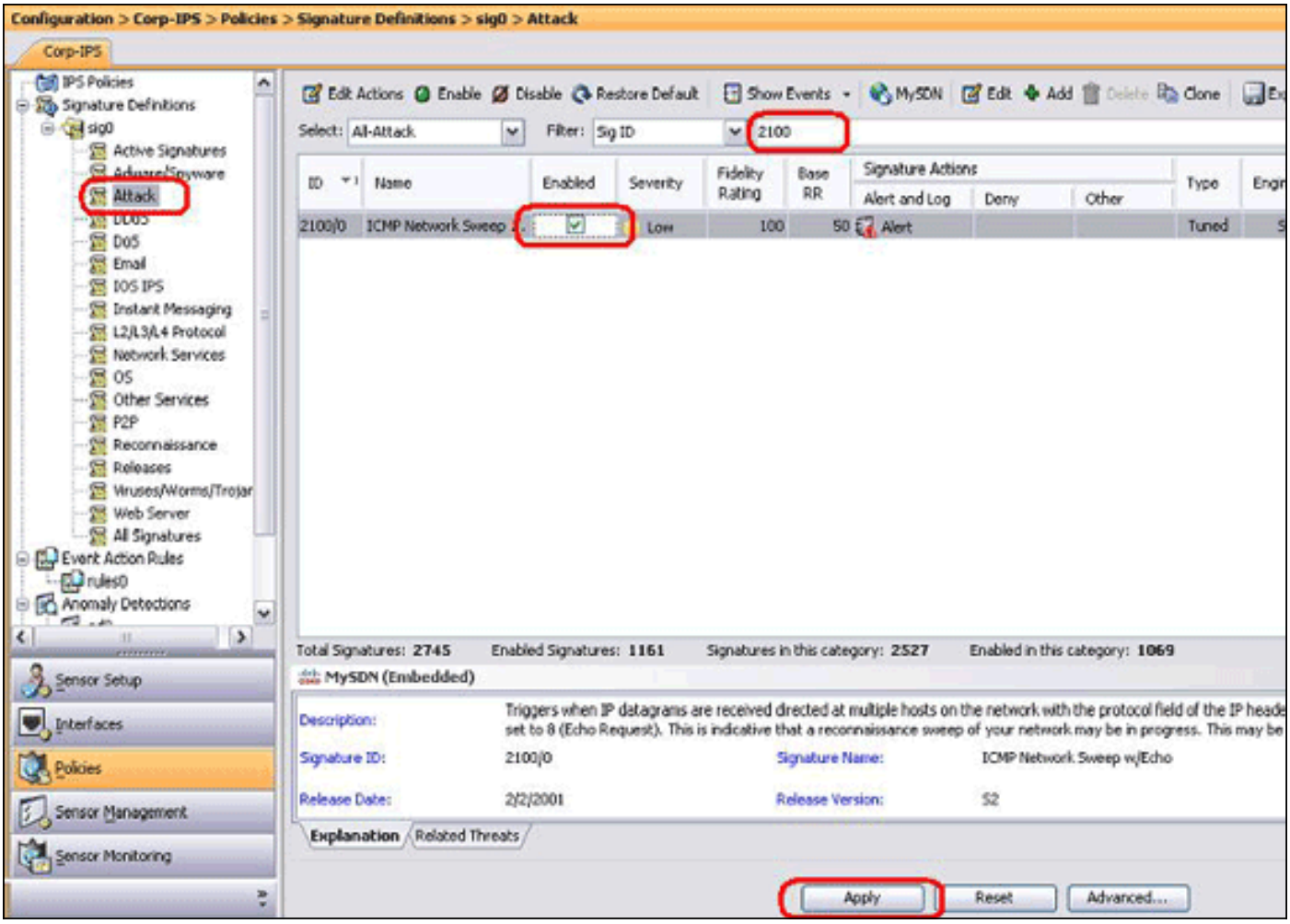


下**OK**。

全域性禁用簽名

您可能希望隨時禁用簽名以阻止警報。要啟用、禁用和停用簽名，請完成以下步驟：

1. 使用具有管理員或操作員許可權的帳戶登入到IME。
2. 選擇Configuration > sensor_name > Policies > **Signature Definitions > sig0 > All Signatures**。
3. 要查詢簽名，請從「篩選器」下拉選單中選擇一個排序選項。例如，如果要搜尋ICMP網路掃描簽名，請選擇sig0下的**All Signatures**，然後按簽名ID或名稱搜尋。sig0窗格將刷新並僅顯示與您的分類標準匹配的簽名。
4. 若要啟用或禁用現有簽名，請選擇簽名，然後完成以下步驟：檢視「已啟用」列以確定簽名的狀態。已啟用簽名選中該覈取方塊。要啟用已禁用的簽名，請選中**Enabled**覈取方塊。要禁用已啟用的簽名，請取消選中**Enabled**覈取方塊。若要停用一個或多個簽名，請選擇簽名，按一下右鍵，然後按一下**將狀態更改為>停用**。
5. 按一下「**Apply**」以應用變更並儲存修訂的組態。



相關資訊

- Cisco Secure IDS Director銷售結束
- 思科安全入侵偵測支援頁面
- 技術支援與文件 - Cisco Systems