IPS裝置管理員5.1 — 調整簽名

目錄

簡介

入侵防禦系統(IPS)5.1包含1000多個內建預設簽名。您不能重新命名或刪除內建簽名清單中的簽名，但可以停用簽名以將其從檢測引擎中刪除。您可以稍後啟用已停用的簽名。但是，此過程需要檢測引擎重建其配置，這將花費時間並可能延遲流量的處理。調整多個簽名引數時，可以調整內建簽名。已修改的內建簽名稱為調*節簽名*。

本文檔說明了使用IPS裝置管理器(IDM)調整特徵碼要使用的步驟。IDM是一個基於Web的Java應用程式，可用於配置和管理感測器。IDM的Web伺服器駐留在感測器上。您可以通過Internet Explorer、Netscape或Mozilla Web瀏覽器訪問它。

注意：您可以建立稱為自定義簽名*的簽名*。自定義簽名ID從60000開始。可以針對多種情況配置它們，例如UDP連線上的字串匹配、網路泛洪跟蹤以及掃描。每個特徵碼都是使用專為受監控流量型別設計的特徵碼引擎建立的。

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思科入侵防禦系統裝置管理員5.x。

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。

背景資訊

要將感測器配置為監視特定特徵碼的網路通訊量，必須啟用特徵碼。預設情況下，安裝特徵碼更新時會啟用最重要的特徵碼。當檢測到與已啟用的特徵碼匹配的攻擊時，感測器會生成警報，該警報儲存在感測器的事件儲存區中。基於Web的客戶端可以從事件儲存中檢索警報以及其他事件。預設情況下，感測器會記錄所有資訊警報或更高版本。

某些簽名具有子簽名。也就是說，簽名被劃分為子類別。配置子簽名時，對一個子簽名的引數所做的更改僅應用於該子簽名。例如，如果編輯簽名3050子簽名1並更改嚴重性，則嚴重性更改將僅適用於子簽名1，而不適用於3050 2、3050 3和3050 4。

調整簽名

+圖示表示此引數有更多可用選項。按一下+圖示展開該部分並檢視其餘引數。

綠色圖示表示引數當前使用預設值。按一下綠色圖示將其更改為紅色，這將啟用引數欄位，以便您可以編輯該值。

逐步程序

完成以下步驟以調整簽名：

1. 使用具有管理員或操作員許可權的帳戶登入到IDM。
2. 選擇**Configuration > Signature Definition > Signature Configuration**。系統將顯示Signature Configuration窗格。
3. 要查詢簽名，請從**Select By**（選擇依據）清單中**選擇排序**選項。例如，如果您搜尋UDP泛洪簽名，請選擇**L2/L3/L4 Protocol**，然後選擇**UDP Funderground**。「簽名配置」(Signature Configuration)窗格將刷新並僅顯示與您的分類標準匹配的簽名。
4. 要調整現有簽名，請選擇簽名並完成以下步驟：按一下**編輯**以開啟「編輯簽名」對話方塊。檢視引數值，並更改要最佳化的任何引數的值。**註：**要選擇多個事件操作，請按住**Ctrl**鍵。在Status下，選擇**Yes**以啟用簽名。**注意：**必須啟用特徵碼，感測器才能主動檢測特徵碼指定的攻擊。在「狀態」下，指定此簽名是否失效。按一下**No**啟用簽名。這會將簽名置於引擎中。**注意：**必須啟用特徵碼，感測器才能主動檢測特徵碼指定的攻擊。**注意：**按一下**取消**可撤消更改並關閉「編輯簽名」對話方塊。按一下「**OK**」（確定）。編輯後的簽名現在會顯示在清單中，並且型別設定為「已最佳化」。**注意：如**果要撤消更改，請按一下「重置」(**Reset**)。
5. 按一下**Apply**以應用更改並儲存修訂後的配置。

相關資訊

- 思科入侵防禦系統
- 技術支援與文件 - Cisco Systems