Intrusion Prevention System Device Manager 5.1 - Tuning-Signatur

Inhalt

Einführung

Intrusion Prevention System (IPS) 5.1 enthält mehr als 1.000 integrierte Standardsignaturen. Sie können Signaturen nicht in der Liste der integrierten Signaturen umbenennen oder löschen, sondern Signaturen entfernen, um sie aus dem Sensormodul zu entfernen. Später können Sie pensionierte Signaturen aktivieren. Dieser Prozess erfordert jedoch, dass die Sensing Engines ihre Konfiguration neu aufbauen, was Zeit kostet und die Verarbeitung des Datenverkehrs verzögern könnte. Sie können integrierte Signaturen anpassen, wenn Sie mehrere Signaturparameter anpassen. Integrierte Signaturen, die geändert wurden, werden als *angepasste Signaturen* bezeichnet.

In diesem Dokument werden die Schritte zum Einstellen der Signatur mithilfe des IPS Device Manager (IDM) beschrieben. IDM ist eine webbasierte Java-Anwendung, mit der Sie Ihren Sensor konfigurieren und verwalten können. Der Webserver für IDM befindet sich auf dem Sensor. Der Zugriff erfolgt über die Webbrowser Internet Explorer, Netscape oder Mozilla.

Hinweis: Sie können Signaturen erstellen, die als *benutzerdefinierte Signaturen* bezeichnet werden. Benutzerdefinierte Signatur-IDs beginnen bei 60.000. Sie können sie für verschiedene Dinge konfigurieren, z. B. für die Zuordnung von Zeichenfolgen auf UDP-Verbindungen, die Verfolgung von Netzwerk-Überflutungen und für Scans. Jede Signatur wird mithilfe einer Signaturengine erstellt, die speziell für die Art des überwachten Datenverkehrs entwickelt wurde.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf dem Cisco Intrusion Prevention System Device Manager 5.x.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Um einen Sensor zur Überwachung des Netzwerkverkehrs für eine bestimmte Signatur zu konfigurieren, müssen Sie die Signatur aktivieren. Standardmäßig werden die wichtigsten Signaturen aktiviert, wenn Sie das Signatur-Update installieren. Wenn ein Angriff erkannt wird, der mit einer aktivierten Signatur übereinstimmt, generiert der Sensor eine Warnung, die im Ereignisspeicher des Sensors gespeichert wird. Die Warnungen sowie andere Ereignisse können von webbasierten Clients aus dem Ereignisspeicher abgerufen werden. Standardmäßig protokolliert der Sensor alle Informationswarnungen oder höher.

Einige Signaturen enthalten Untersignaturen. Das heißt, die Signatur ist in Unterkategorien unterteilt. Wenn Sie eine Untersignatur konfigurieren, gelten Änderungen an den Parametern einer Untersignatur nur für diese Untersignatur. Wenn Sie z. B. Signatur 3050 Untersignatur 1 bearbeiten und den Schweregrad ändern, gilt der Schweregrad nur für Untersignatur 1 und nicht für 3050 2, 3050 3 und 3050 4.

Tuning-Signaturen

Ein +-Symbol zeigt an, dass weitere Optionen für diesen Parameter verfügbar sind. Klicken Sie auf das **+** Symbol, um den Abschnitt zu erweitern und die übrigen Parameter anzuzeigen.

Ein grünes Symbol zeigt an, dass der Parameter derzeit den Standardwert verwendet. Klicken Sie auf das grüne Symbol, um es in rot zu ändern. Dadurch wird das Parameterfeld aktiviert, sodass Sie den Wert bearbeiten können.

Schrittweise Vorgehensweise

Gehen Sie wie folgt vor, um Signaturen abzustimmen:

1. Melden Sie sich bei IDM mit einem Konto mit Administrator- oder Operatorberechtigungen an.
2. Wählen Sie **Konfiguration > Signaturdefinition > Signaturkonfiguration aus**.Der Bereich Signature Configuration (Signaturkonfiguration) wird angezeigt.
3. Um nach einer Signatur zu suchen, wählen Sie eine Sortieroption aus der Liste **Select By**

(Auswählen) aus.Wenn Sie beispielsweise nach einer UDP Flood-Signatur suchen, wählen Sie **L2/L3/L4 Protocol** und dann **UDP Floods aus**.Der Bereich Signaturkonfiguration wird aktualisiert und nur die Signaturen angezeigt, die Ihren Sortierkriterien entsprechen.

4. Um eine vorhandene Signatur anzupassen, wählen Sie die Signatur aus, und führen Sie die folgenden Schritte aus:Klicken Sie auf **Bearbeiten**, um das Dialogfeld Signatur bearbeiten zu öffnen.Überprüfen Sie die Parameterwerte, und ändern Sie den Wert jedes Parameters, den Sie anpassen möchten.**Hinweis:** Um mehrere Ereignisaktionen auszuwählen, halten Sie die **Strg**-Taste gedrückt.Wählen Sie unter Status die Option **Ja**, um die Signatur zu aktivieren.**Hinweis:** Die Signatur muss aktiviert sein, damit der Sensor den von der Signatur angegebenen Angriff aktiv erkennen kann.Geben Sie unter Status an, ob diese Signatur eingestellt wird. Klicken Sie auf **Nein**, um die Signatur zu aktivieren. Dadurch wird die Signatur in den Motor eingesteckt.**Hinweis:** Für den Sensor muss eine Signatur aktiviert werden, um den von der Signatur angegebenen Angriff aktiv erkennen zu können.**Hinweis:** Klicken Sie auf **Abbrechen**, um die Änderungen rückgängig zu machen und das Dialogfeld Signatur bearbeiten zu schließen.Klicken Sie auf **OK**.Die bearbeitete Signatur wird nun in der Liste angezeigt, wobei der Typ auf Tuned gesetzt ist.**Hinweis:** Wenn Sie die Änderungen rückgängig machen möchten, klicken Sie auf **Zurücksetzen**.
5. Klicken Sie auf **Apply**, um die Änderungen zu übernehmen und die überarbeitete Konfiguration zu speichern.

Zugehörige Informationen

- Cisco Intrusion Prevention System
- Technischer Support und Dokumentation - Cisco Systems