IPS 5.x und höher: Verschiedene Methoden zur Überwachung von Ereignissen

Inhalt

Einführung

Dieses Dokument enthält verschiedene Methoden zur Überwachung der IPS-Ereignisse.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf IPS 5.x und höher.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

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

Methoden zur Überwachung der IPS-Ereignisse

Derzeit gibt es vier Optionen für die Überwachung der Sensoren:

1. IPS Manager Express (IME) ist im Software-Download auf Cisco.com verfügbar. Diese Anwendung kann den IPS-Sensor mit SDEE sicher abonnieren und die Ereignisse/Protokolle abrufen, die als Folge von Problemen oder Signaturen generiert wurden, die aufgrund einer Übereinstimmung ausgelöst wurden.Der IPS Device Manager (IDM) wird aufgerufen, wenn Sie über HTTPS direkt auf den Sensor zugreifen.Zeigen Sie den Ereignisspeicher direkt auf dem Sensor mit den IDM Monitoring- oder IME Event Monitoring-Tools an. IDM und IME sind keine gültigen Lösungen, wenn Sie die Ereignisse langfristig speichern müssen, da der lokale Ereignisspeicher des Sensors ein 30-MB-Rundumpuffer ist und beginnt, sich zu überschreiben, sobald die 30-MB-Grenze erreicht ist. Dieses Limit ist nicht konfigurierbar.
2. Verwenden Sie ein CS-MARS-Gerät, um routinemäßig Ereignisse vom Sensor abzurufen und zu korrelieren. Der CS-MARS verwendet das SDEE-Protokoll, um eine sichere Verbindung zum Sensor herzustellen, um die Ereignisse abzurufen und alle paar Sekunden neue Ereignisse abzurufen.Wenden Sie sich an Ihr Account Team/Reseller/SE, um weitere Informationen zu erhalten, wenn Sie das CS-MARS-Gerät vorführen möchten.Für Cisco IPS 5.x- und 6.x-Geräte ruft MARS die Protokolle mit SDEE über SSL ab. MARS muss daher über HTTPS-Zugriff auf den Sensor verfügen. Um den Sensor vorzubereiten, müssen Sie HTTPS-Datenverkehr von der IDM/IME-Managementstation zulassen und sicherstellen, dass die IP-Adresse von MARS als zulässiger Host auf dem Sensor definiert ist.
```
sensor#conf t
 sensor(config)#service host
 sensor(config-hos)#network-settings
 sensor(config-hos-net)#access-list x.x.x.x/subnet_mask
 sensor(config-hos-net)#exit
 sensor(config-hos)#exit
 Apply Changes?[yes]:
 sensor(config)#
```
3. Überwachen Sie die Ereignisse mit dem IEV. IDS Event Viewer ist eine Java-basierte Anwendung, mit der Sie Alarme für bis zu fünf Sensoren anzeigen und verwalten können. Mit IDS Event Viewer können Sie in Echtzeit oder in importierten Protokolldateien eine Verbindung herstellen und Alarme anzeigen. Sie können Filter und Ansichten konfigurieren, um die Alarme zu verwalten. Sie können Ereignisdaten auch für weitere Analysen importieren und exportieren. Wie MARS stellt IEV eine sichere Verbindung zum Sensor her und ruft alle paar Sekunden Ereignisse ab. Das IEV speichert diese Ereignisse in einer Datenbank auf dem Server, auf dem IEV installiert ist. Die DB ist im Lieferumfang von IEV enthalten und wird zusammen mit der Anwendung installiert. Klicken Sie auf IEV, um den Download durchzuführen.**Hinweis:** Die Dokumentation für IEV finden Sie nach der Installation im Hilfemenü. Die Readme-Datei enthält Installationsinformationen.
4. Konfigurieren Sie die Signaturen auf Ihrem Sensor, sodass **request-snmp-trap** aktiviert wird, und konfigurieren Sie den Sensor für das Senden der Traps an einen SNMP-Server. Anschließend können Sie mit diesem Server die Nachrichten als Syslogs an einen anderen Computer weiterleiten.SNMP ist ein Protokoll auf Anwendungsebene, das den Austausch von Verwaltungsinformationen zwischen Netzwerkgeräten erleichtert. Mit dem SNMP können Netzwerkadministratoren die Netzwerkleistung verwalten, nach Netzwerkproblemen suchen und diese beheben und für ein mögliches Wachstum des Netzwerks vorausplanen.SNMP ist ein einfaches Anforderungs-/Antwortprotokoll. Das Netzwerkmanagementsystem gibt eine Anforderung aus, und verwaltete Geräte geben Antworten zurück. Dieses Verhalten wird mithilfe eines von vier Protokollvorgängen implementiert:GetGetNextFestlegenTrapSie können den Sensor für die Überwachung über SNMP konfigurieren. SNMP definiert eine Standardmethode für Netzwerkmanagementstationen zur Überwachung von Zustand und Status vieler Arten von Geräten, darunter Switches, Router und Sensoren.

Zugehörige Informationen

- Cisco Sensoren der Serie IPS 4200
- Cisco Intrusion Prevention System
- Problemhinweise zu Sicherheitsprodukten (einschließlich CiscoSecure Intrusion Detection)
- Technischer Support und Dokumentation für Cisco Systeme