Unterschiede zwischen Protokollen und Debuggen auf Adaptive Security Appliances

Inhalt

Einführung

Dieses Dokument enthält eine einfache Beschreibung der Debugfunktionen in Adaptive Security Appliances (ASAs), die Version 8.4 und höher ausführen. Einige Funktionen sind jedoch nur in Version 9.5(2) und höher verfügbar.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- ASA 5506-X mit ASA Software Version 9.5(2)
- Cisco Adaptive Security Device Manager (ASDM) Version 7.5.2

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.

Grundlegende Protokollierungsfunktionen

ASAs behandeln Fehlermeldungen anders als Cisco IOS® Geräte. Standardmäßig (sofern nicht "logging debug-trace", wie weiter unten beschrieben, verwendet wird), werden diese entweder beim Anschließen über den Konsolenport oder über Telnet/Secure Shell (SSH) auf dem

Bildschirm angezeigt, aber sie sind völlig unabhängig. Wenn Sie die Konsole verwenden, werden sie sofort nach Eingabe des Befehls debug angezeigt. Die gleiche Aktion tritt auch bei einer SSH-Sitzung auf.

Unabhängigkeit bedeutet, dass die Debug-Meldungen nicht auf SSH angezeigt werden, wenn Sie Debug auf dem Konsolenport aktivieren und über SSH verbunden sind. Sie müssen diese manuell erneut aktivieren. Wenn Debugger für eine SSH-Sitzung aktiviert sind, werden sie in der anderen Sitzung ebenfalls nicht angezeigt. Sie können darauf als **Sitzungsdebuggen** verweisen.

Es ist auch nicht erforderlich, den Befehl **terminal monitor** auf einer ASA einzugeben, um Debugging anzuzeigen, da das auf SSH oder einer Telnet-Sitzung aktivierte Debugging unabhängig von diesem Befehl angezeigt wird. Der Zweck dieses Befehls unterscheidet sich stark von Cisco IOS-Geräten, und diese Funktion wird im ASA Syslog-Konfigurationsbeispiel detailliert beschrieben.

Unterschied zwischen Syslog- und Debug-Meldungen

Bei den Debuggen handelt es sich um angegebene Meldungen für ein bestimmtes Protokoll oder eine bestimmte Funktion von ASAs. Es gibt keine Ebene von Debug, sondern sie sind sehr detailliert und die Detailstufe kann geändert werden. Sie verfügen möglicherweise auch nicht über einen Zeitstempel, einen Nachrichtencode oder einen Schweregrad. Dies hängt vom jeweiligen Debuggen ab.

In diesem Beispiel wird der Unterschied zwischen Debug- und Syslog-Meldungen in Bezug auf dieselbe Ping-Anforderung veranschaulicht.

Dies ist ein Beispiel für die Debugausgabe, nachdem Sie den Befehl **debug icmp trace** eingegeben haben:

```
ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1 seq=29 len=32

ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1 seq=29 len=32
```

Dies ist ein Beispiel für eine **Syslog-**Meldung bezüglich derselben ICMP-Anforderung:

```
Jan 01 2016 13:29:22: %ASA-6-302020: Built inbound ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0

Jan 01 2016 13:29:22: %ASA-6-302021: Teardown ICMP connection for faddr 10.229.24.48/1
 gaddr 10.48.67.75/0 laddr 10.48.67.75/0
```

Debugger sammeln

Das Standard-Timeout für SSH oder Telnet beträgt fünf Minuten, und die Sitzung wird nach dieser Inaktivität getrennt. Das Standard-Timeout für die Konsolenverbindung ist 0. Das bedeutet, dass der Benutzer angemeldet ist, bis sich der Benutzer manuell abmeldet.

Leider ist die Protokollierungsfunktion durch das Timeout für eine bestimmte Managementmethode begrenzt, sodass die SSH-Sitzung nach Beendigung des Debuggens ebenfalls beendet wird.

Um die Debug-Dateien für einen längeren Zeitraum zu erfassen, müssen Sie die

Konsolenverbindung verwenden und sie dann mit dem Befehl **debug-trace** auf den Syslog-Server umleiten. Sie werden als Syslog-Meldung 711001 mit dem Schweregrad 7 umgeleitet. Um das Senden dieser Nachrichten an Protokolle zu beenden, können Sie vor dem Befehl "no" (Nein) einfügen.

```
logging debug-trace
no logging debug-trace
```

Ab Version 9.5.2 können Sie mit der ASA nach einer Zeitüberschreitung weiterhin Debug-Meldungen als Syslog-Meldungen senden oder sich bei einer SSH-/Telnet-/Konsolenverbindung abmelden. Wenn Sie den Befehl **debug-trace persistent** eingeben, können Sie in einer Sitzung aktiviertes Debuggen selektiv aus einer anderen Sitzung löschen, und sie bleiben im Hintergrund aktiv. Um diese Funktion zu deaktivieren, fügen Sie vor dem Befehl "no" (Nein) ein.

```
logging debug-trace persistent
no logging debug-trace persistent
```

Standardmäßig haben alle Debugmeldungen den Schweregrad 7. Um sie aus unerwünschten Nachrichten zu filtern, können Sie den Schweregrad dieser Nachricht auf 3 erhöhen, sodass Sie nur Fehlermeldungen neben den Debuggen sammeln. Geben Sie "no" ein, um diese Umleitung zu deaktivieren.

```
logging message 711001 level 3
no logging message 711001 level 3
```

Beispielkonfiguration

```
logging enable
logging host 10.0.0.1
logging trap errors
logging debug-trace persistent
logging message 711001 level errors
debug icmp trace
```

Mit diesen Befehlen können Sie Fehlermeldungen und auch als Fehler markierte Internet Control Message Protocol (ICMP)-Debugger an den Syslog-Server senden:

```
Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo request from 10.229.24.48 to 10.48.67.75 ID=1
 seq=29 len=32

Jan 01 2016 13:30:22: %ASA-3-711001: ICMP echo reply from 10.48.67.75 to 10.229.24.48 ID=1
 seq=29 len=32
```

Zugehörige Informationen

- ASA Syslog-Konfigurationsbeispiel
- Technischer Support und Dokumentation - Cisco Systems