適応型セキュリティ アプライアンスのログとデバッグの違い

目次

概要

このドキュメントでは、バージョン 8.4 以降が稼働する適応型セキュリティ アプライアンス（ASA）のデバッグ機能に関する簡単な説明を示します。 ただし、一部の機能はバージョン 9.5(2) 以降でのみ利用可能です。

前提条件

要件

このドキュメントに関しては個別の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- ASA ソフトウェア バージョン 9.5(2) が稼働する ASA 5506-X
- Cisco Adaptive Security Device Manager（ASDM）バージョン 7.5.2

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

基本ロギング機能

ASA は、デバッグ メッセージを Cisco IOS® デバイスとは異なる方法で処理します。 デフォルトでは（後で説明する「logging debug-trace」を使用しないかぎり）、デバッグ メッセージは、コンソール ポート経由または telnet/Secure Shell（SSH）経由で接続されたときに画面に表示されますが、完全に独立しています。 コンソールを使用すると、debug コマンドを入力した直後に表

示されます。 SSH セッションでも同様のアクションが発生します。

独立しているとは、コンソール ポートでデバッグを有効にし、SSH 経由で接続すると、デバッグは SSH に表示されないことを意味します。 手動で再度有効にする必要があります。 またデバッグが 1 つの SSH セッションで有効になると、他のセッションではまったく表示されません。これは、**session debugging** のように参照できます。

また SSH または Telnet セッションで有効化されたデバッグはこのコマンドにかかわらず表示されるため、デバッグを表示するために ASA で **terminal monitor** コマンドを入力する必要はありません。 このコマンドの目的は Cisco IOS デバイスとは大きく異なり、この機能については ASA Syslog 設定例 で詳細に説明します。

Syslog とデバッグ メッセージの違い

デバッグは、ASA の特定のプロトコルまたは機能に対して指定されたメッセージです。 デバッグレベルはない代わりに非常に詳細で、詳細レベルを変更できます。 さらに、タイムスタンプ、メッセージ コード、または重大度が含まれていない場合もあります。 これは個々のデバッグによって異なります。

この例では、同じ ping 要求に対するデバッグと syslog メッセージの違いを示します。

これは、**debug icmp trace** コマンドを入力した後のデバッグ出力の例です。

```
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
```

これは、同じ ICMP 要求に対する **syslog** メッセージの例です。

```
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
```

デバッグの収集

SSH または Telnet のデフォルトのタイムアウトは 5 分で、この時間非アクティブの状態が続くと、セッションは切断されます。 コンソール接続のデフォルトのタイムアウトは 0 のため、ユーザが手動でログアウトするまでログインしていることになります。

残念ながら、ロギング機能は特定の管理手法のタイムアウト設定によって制限されるため、SSH セッションが終了すると、デバッグも停止します。

延長してデバッグを収集し続けるには、コンソール接続を使用する必要があります。すると、**logging debug-trace** コマンドでそれらを syslog サーバにリダイレクトできます。 これらは重大度 7 で発行される syslog メッセージ 711001 としてリダイレクトされます。ログへのこのメッセージの送信を停止するには、コマンドの前に「no」を挿入します。

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

バージョン 9.5.2 以降では、ASA は SSH/telnet/コンソール接続のタイムアウトまたはログアウト後に、syslog メッセージとしてデバッグを送信し続けることができます。 **debug-trace persistent** コマンドを入力すると、1 つのセッションで有効になったデバッグを選択的に他のセッションから区別し、バックグラウンドでアクティブなままにできます。 この機能を無効にするには、コマンドの前に「no」を挿入してください。

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

デフォルトでは、すべてのデバッグ メッセージの重大度はレベル 7 です。不要なメッセージからそれらのメッセージをフィルタするため、重大度を 3 に上げることができます。これにより、デバッグ側のエラー メッセージのみ収集します。 このリダイレクションを無効にするには、「いいえ」を挿入します。

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

設定例

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

これらのコマンドにより、エラー メッセージ、およびエラーとしてもマークされた Internet Control Message Protocol（ICMP）デバッグを syslog サーバに送信できます。

```
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
```

関連情報

- ASA Syslog 設定例
- テクニカル サポートとドキュメント – Cisco Systems