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

内容

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特有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いています。

- 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

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。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。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

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。デバッグのレベルはありませんが、非常に詳細で、詳細レベルを変更できます。タイムスタンプ、メッセージコード、または重大度レベルがない場合もあります。これは、特定のデバッグに依存します。

次の例は、同じping要求に関するデバッグとsyslogメッセージの違いを示しています。

次に、**debug icmp trace**コマンドを入力した後のデバッグ出力**の例を示**します。

```
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
```

次に、同じICMP要求に関する**syslog**メッセージの例を示します。

```
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、この非アクティブ時間の後にセッションが切断されます。コンソール接続のデフォルトのタイムアウトは0です。これは、ユーザが手動でログアウトするまで、ユーザがログインしていることを意味します。

残念ながら、ロギング機能は特定の管理方式で設定されたタイムアウト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。

デバッグを長時間にわたって収集し続けるには、コンソール接続を使用し、**logging debug-traceコマンドを使用してsyslogサーバにリダイレクトする必要があ**ります。これらは、重大度7で発行されたsyslogメッセージ711001としてリダイレクトされます。このメッセージのログへ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から、ASAではタイムアウト後やSSH/telnet/コンソール接続でログアウト後も、デバッグをsyslogメッセージとして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、あるセッションで有効になったデバッグを別のセッションから選択的にクリアでき、バックグラウンドでアクティブなままになります。この機能を無効にするには、コマンドの前に「no」を挿入します。

```
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7です。不要なメッセージからフィルタリングするには、このメッセージの重大度を3に上げることができ、デバッグの横にエラーメッセージだけを収集できます。このリダイレクトを無効にするには、「no」を挿入します。

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

サンプル コンフィギュレーション

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

次のコマンドを使用すると、エラーメッセージおよびエラーとしてマークされたインターネット制御メッセージプロトコル(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 の設定例
- テクニカル サポートとドキュメント – Cisco Systems