



第 5 章 VPN デバイスの設定

VPN(仮想私設網)デバイスは MARS にリモート ホスト、ログインの要求や拒否、およびアクセス時間に関する情報を提供します。MARS はこのデータを使用して、エンドツーエンドの攻撃パス分析を実行したり、起動された攻撃が経由する VPN デバイスを識別することができます。

この章では、次に示す VPN デバイスをブートストラップして、MARS に追加する方法を示します。

- ・ Cisco VPN 3000 Concentrator

Cisco VPN 3000 Concentrator

MARS は Cisco VPN 3000 Concentrator(バージョン 4.0.1 および 4.7)からイベントを受信して、処理することができます。通信をイネーブルにするには、次の 2 つのタスクを実行する必要があります。

- ・ VPN 3000 Concentrator のブートストラップ
- ・ MARS への VPN 3000 Concentrator の追加

VPN 3000 Concentrator のブートストラップ

イベントを生成して MARS アプライアンスにパブリッシュするように Cisco VPN 3000 Concentrator を設定するには、正しいイベントが正しいフォーマットで生成されていることを確認し、Syslog イベントおよび SNMP トラップを MARS アプライアンスにパブリッシュするように Cisco VPN 3000 Concentrator に指示する必要があります。

Syslog イベントおよび SNMP(簡易ネットワーク管理プロトコル)トラップを MARS に送信するように Cisco VPN 3000 Concentrator を設定する手順は、次のとおりです。

ステップ 1 ブラウザを開き、Cisco VPN 3000 Concentrator Series Manager にログインします。

ステップ 2 左側のツリーで、**Configuration > System > Events > General** の順に選択します。

Configuration | System | Events | General

This section lets you configure default event handling.

Save Log on Wrap	<input type="checkbox"/>	Check to save the event log to a file on wrap.
Save Log Format	Multiline	Select the format of the saved log files.
FTP Saved Log on Wrap	<input type="checkbox"/>	Check to automatically FTP the saved log to a remote destination.
E-mail Source Address		Enter the e-mail address that appears in the From: field.
Syslog Format	Original	Select the format of Syslog messages.
Events to Log	Severities 1-5	Select the events to enter in the log.
Events to Console	Severities 1-3	Select the events to display on the console.
Events to Syslog	Severities 1-5	Select the events to send to a Syslog Server.
Events to E-mail	None	Select the events to send to an E-mail Recipient.
Events to Trap	Severities 1-3	Select the events to send to an SNMP Trap Destination.

143210

ステップ 3 Save Log Format が Multiline であることを確認します。

ステップ 4 Syslog Format が Original であることを確認します。

ステップ 5 Events to Log フィールドで **Severities 1-5** を選択します。

ステップ 6 Events to Syslog フィールドで **Severities 1-5** を選択します。

ステップ 7 Events to Trap フィールドで **Severities 1-3** を選択します。

ステップ 8 左側のツリーで、**Configuration > System > Events > Syslog Servers** の順に選択します。

ステップ 9 **Add** をクリックして、ターゲット Syslog サーバを定義します。

Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

Syslog Server	cs-mars	Enter the IP address or hostname of the syslog server.
Port	514	Enter the port used by the syslog server.
Facility	Local 7	Select the syslog facility tag for events sent to this server.
<input type="button" value="Add"/> <input type="button" value="Cancel"/>		

143209

ステップ 10 Syslog Server フィールドに、MARS アプライアンスの IP アドレスまたはホスト名を入力します。

ステップ 11 **Add** をクリックして、Syslog サーバの設定を保存します。

ステップ 12 右上の **Save** をクリックして、すべての変更を保存します。

MARS への VPN 3000 Concentrator の追加

VPN 3000 Concentrator を MARS に追加する手順は、次のとおりです。

ステップ 1 Admin > Security and Monitor Devices > Add の順に選択します。

ステップ 2 Device Type リストで、Cisco VPN Concentrator 4.0.1 または Cisco VPN Concentrator 4.7 を選択します。

Device Type:

→ *Device Name:

→ Access IP:

→ Reporting IP:

→ *Access Type:

SNMP RO Community:

→ Monitor Resource Usage:

143208

ステップ 3 Device Name フィールドに VPN Concentrator の名前を入力します。

ステップ 4 Access IP フィールドに VPN Concentrator の管理に使用する IP アドレスを入力します。

ステップ 5 Reporting IP フィールドに、管理コンテキストから送信される Syslog メッセージの送信元となる IP アドレスを入力します。

ステップ 6 Access Type リストで、SNMP を選択します。

ステップ 7 (任意)MARS がこのコンセントレータの MIB オブジェクトを取得できるようにするには、SNMP RO Community フィールドにデバイスの読み取り専用コミュニティ スtring を入力します。

MARS は SNMP RO String を使用して、レポート デバイスの CPU 使用率およびその他のデバイス異常データに関連する MIB を読み取ります。

ステップ 8 Discover をクリックします。

ステップ 9 Submit をクリックします。

