CS-MARS： CS-MARS へのレポート デバイスとして Cisco IPS センサーを追加する設定例

目次

はじめに

この資料に Cisco Secure 侵入防御システム（IPS）デバイスおよび設定されたバーチャル センサーを Ciscoセキュリティ モニタリング、分析および応答システム（CS-MARS）にとしてレポート中のデバイスを機能するために準備する方法を説明されています。

前提条件

要件

Cisco IPS に関しては 5.x、6.x および 7.x デバイスは SSL 上の SDEE を使用して、MARS ログを引っ張ります。 そのため、MARS からセンサーに対して HTTPS アクセスできる必要があります。 センサーを準備するために、センサーの HTTP サーバをイネーブルに設定して下さい HTTPS アクセスを許可することを TLS を可能にし、センサーにアクセスし、イベントを引っ張ることができる 1 つを MARS の IP アドレスが許可されたホストと定義されること確かめます。限られたホストからアクセスかネットワークのサブネットを可能にするためにセンサーが設定される場合 **access-list ip_address/**このアクセスをイネーブルにするために**ネットマスク** コマンドを使用できます。

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。

- ソフトウェア バージョン 4.2.x および以降を実行する Cisco Secure MARS デバイス
- ソフトウェア バージョン 6.0 およびそれ以降が実行されている Cisco 4200 シリーズ IPS デ

バイス

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。

関連製品

この設定は、次のセンサーにも使用できます。

- IPS-4240
- IPS-4255
- IPS-4260
- IPS-4270-20

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

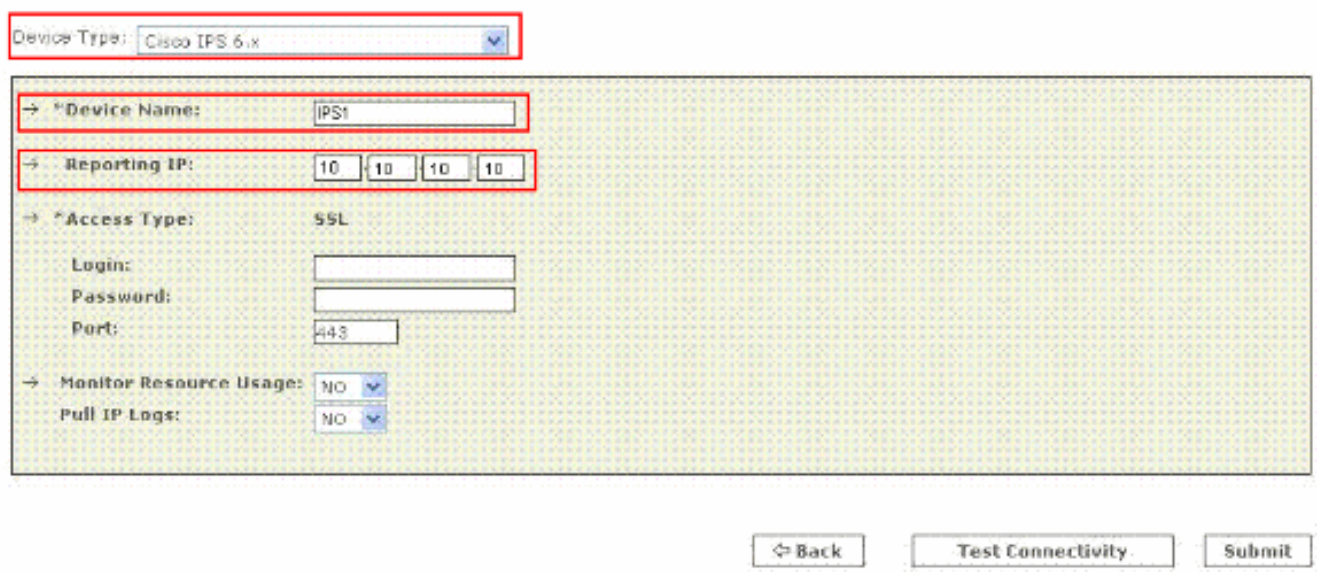
このセクションでは Ciscoセキュリティ モニタリング、分析および応答システム（CS-MARS）デバイスに Cisco Secure 侵入防御システム（IPS）センサーを追加し設定する、方法の情報が表示されます。

Cisco IPS を MARS の 6.x か 7.x デバイス追加し、設定して下さい

Cisco IPS を MARS の 6.x か 7.x デバイス定義するとき、デバイスで設定されるバーチャル センサーを検出できます。 これらのバーチャル センサーを検出するとき、これは MARS がバーチャル センサーで報告されたイベントを分けるようにします。 それはまた望ましいレポートの正確さを改善する各々のバーチャル センサーに監視されたネットワークのリストを調整することを可能にします。

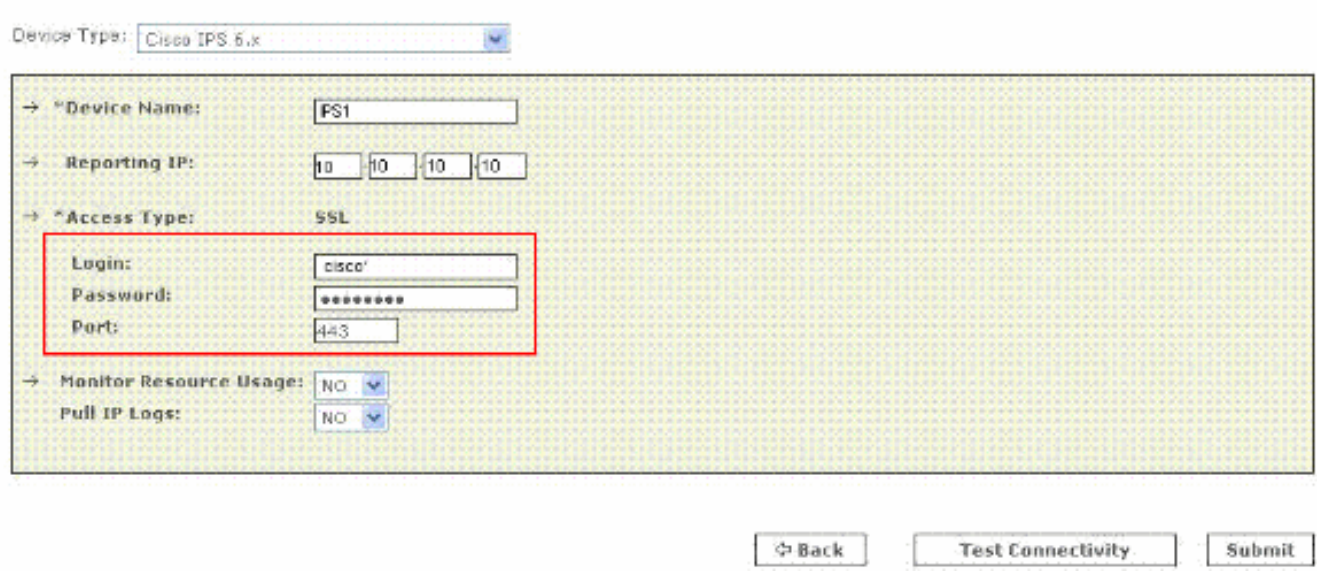
Cisco IPS を追加し、設定するためにこれらのステップを MARS の 6.x か 7.x デバイス完了して下さい:

1. **> システム設定 > Security** 『Admin』 を選択 し、**デバイスを監視して下さい。** それから、『Add』 をクリック して下さい。
2. デバイス型リストから **IPS 6.x か Cisco IPS 7.x を**『Cisco』 を選択 して下さい。 この場合ここに示されているように **Device Name フィールド**でセンサーのホスト名を入力して下さい。 IPS1 はこの例で使用されるデバイス名です。 デバイス名値は設定されたセンサー名前と同一である必要があります。



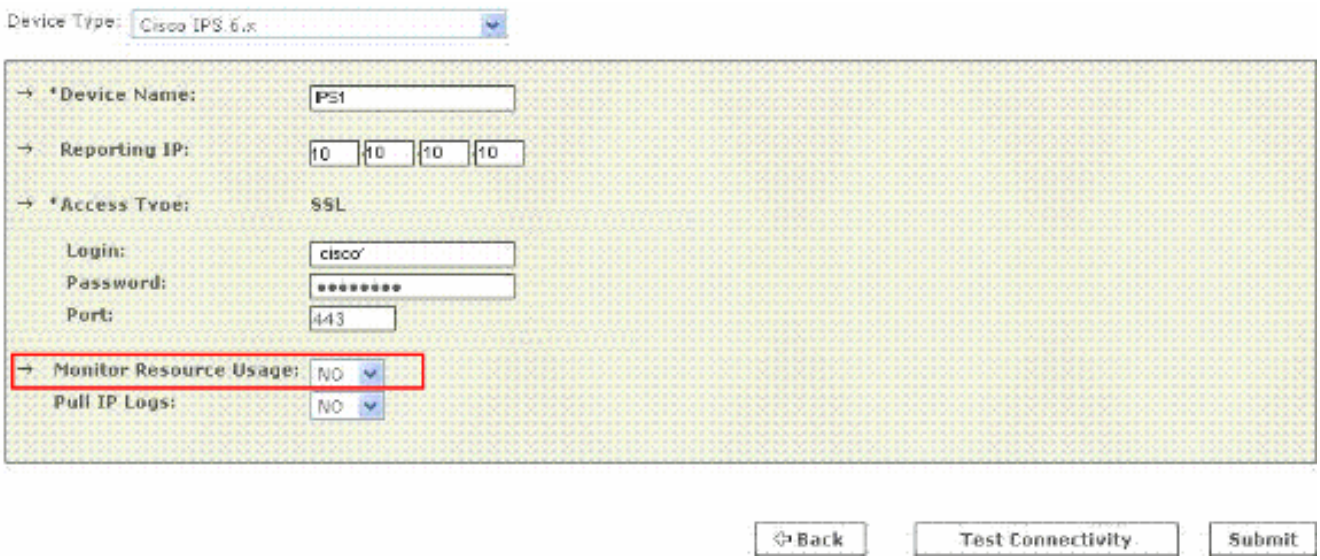
この場合**報告 IP** フィールドで管理上の IP アドレスを入力して下さい。 レポート IP アドレスは管理上の IP アドレスと同じアドレスです。

3. **Login フィールド**では、管理上のアカウントと関連付けられるレポート中のデバイスにアクセスするのに使用するユーザ名を入力して下さい。 この場合、**Password フィールド**で、規定 されるユーザ名と関連付けられる **Login フィールド**でパスワードを入力して下さい。 **ユーザー名は cisco** であり、使用される**パスワードは**この例の **cisco123** です。 またセンサーで動作する Webサーバが **Port フィールド**で受信する TCPポート番号を入力して下さい。 デフォルト HTTPS ポートは 443 です。

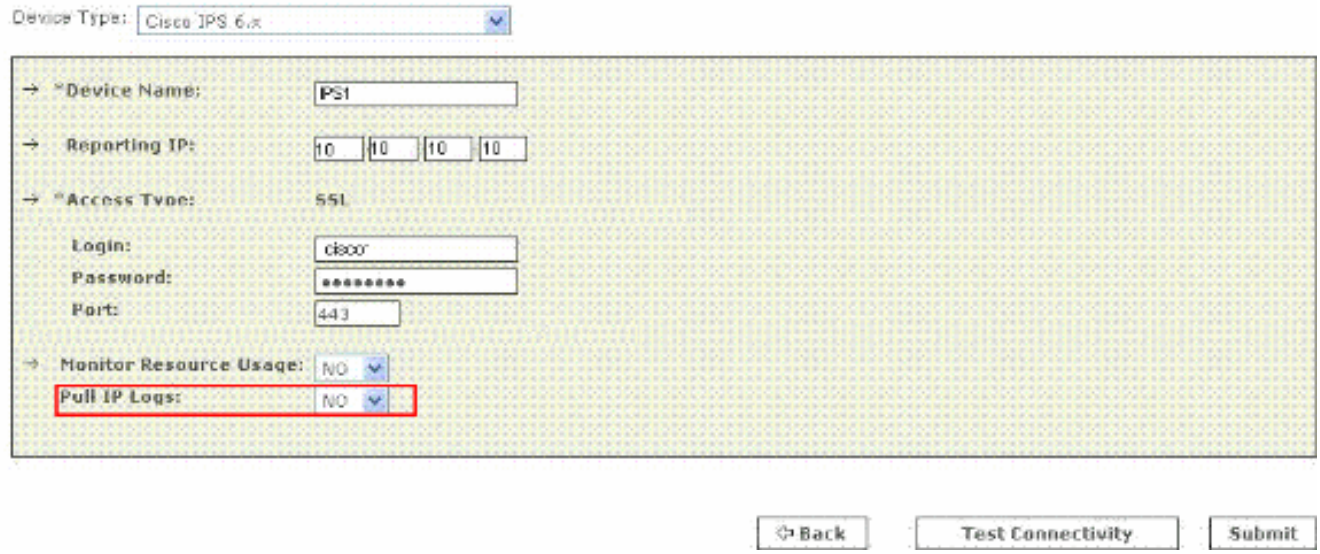


注: HTTP だけを設定することは可能性のあるの間、MARS は HTTPS を必要とします。

4. **モニタ リソース使用**リストで not chosed ことをこの場合確認して下さい。 モニタ リソース使用オプションはこのページで書かれている間、Cisco IPS のために機能しません。

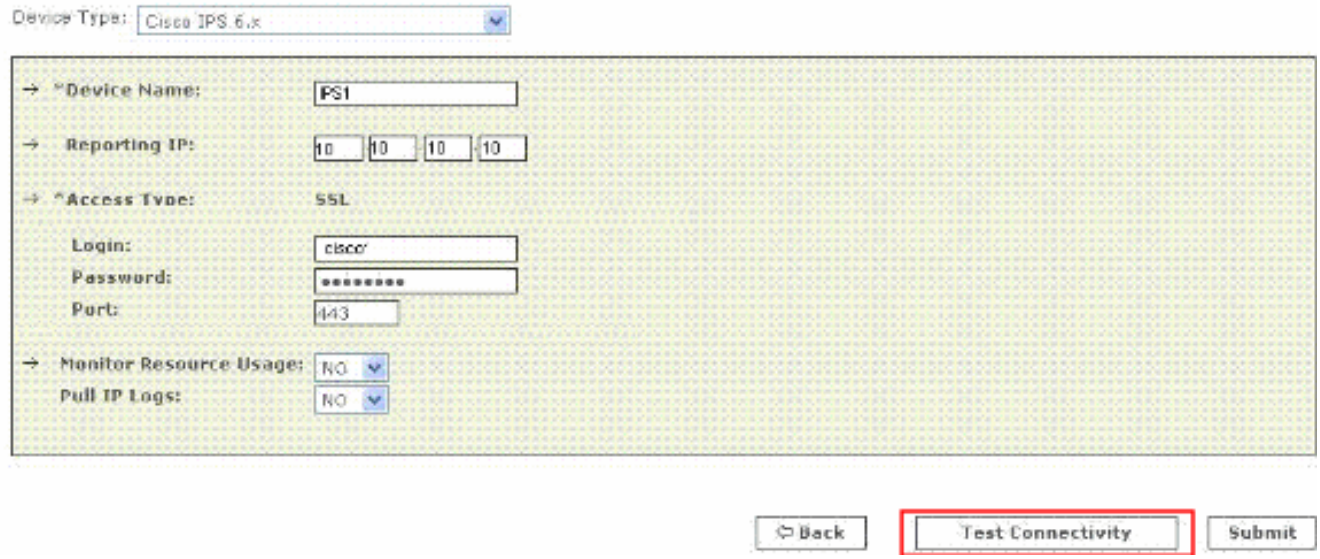


5. センサーからの IP ログを引っ張るために、**プル IP ログ**・リストから『Yes』 を選択 して下さい。 これは必要であれば使用することができるオプション機能です。

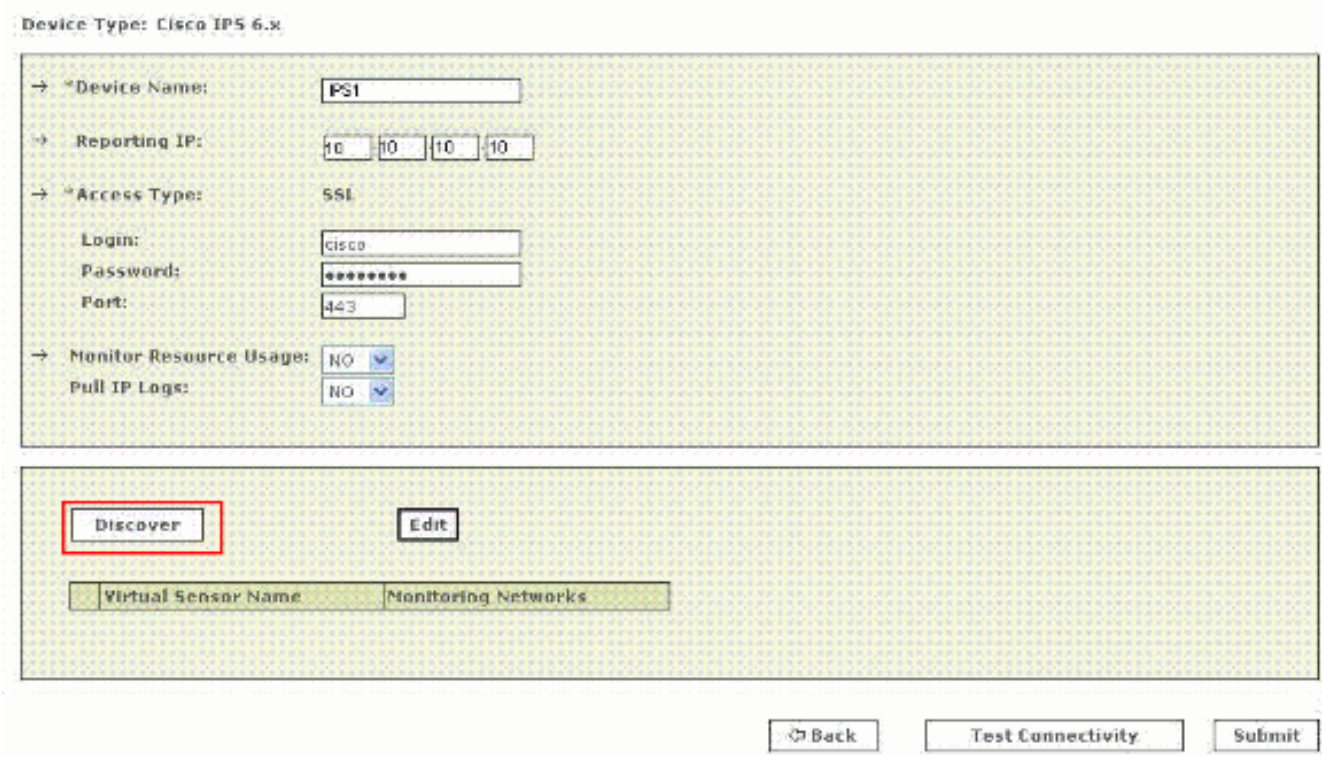


この設定はバーチャル センサー アラートのために生成されるそれらの口グを含む全体のセンサーに適用されます。

6. 設定を確認し、バーチャル センサーのディスカバリを有効に するために**接続を**『Test』 をクリック して下さい。

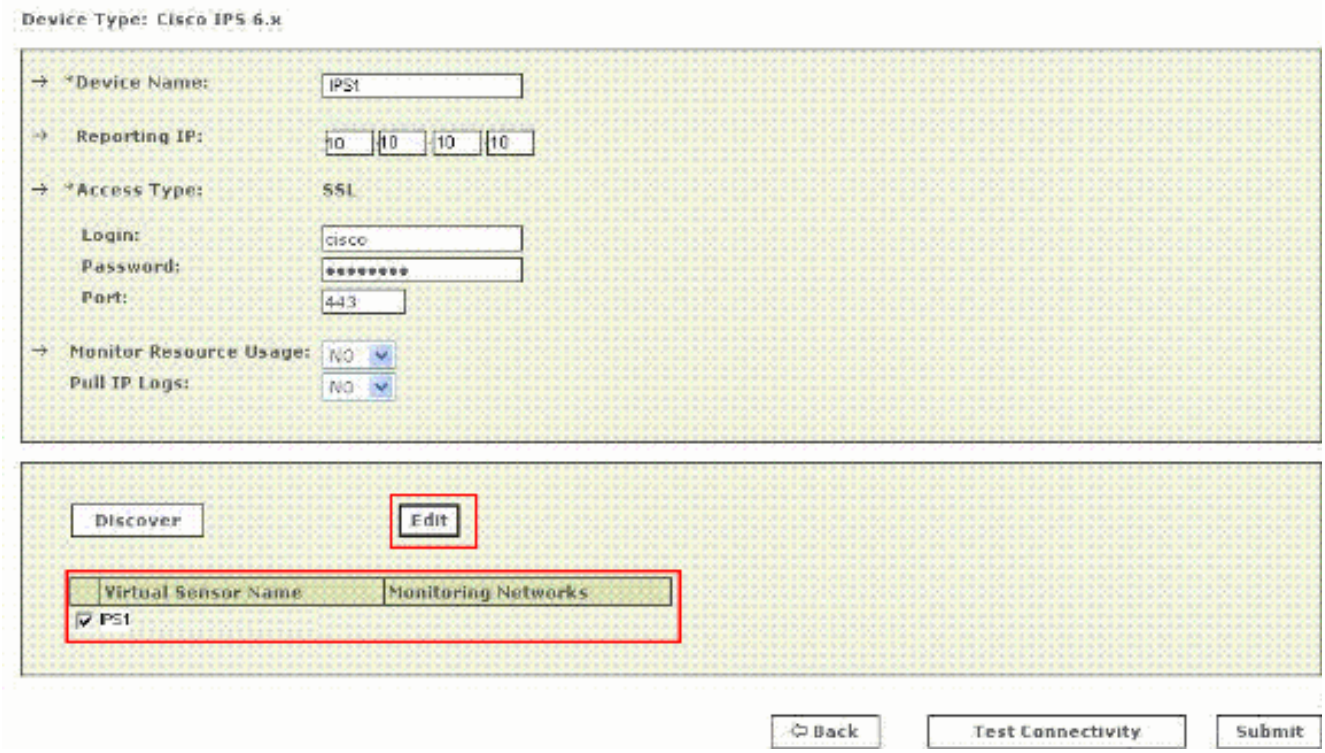


7. 定義されたバーチャル センサーを検出するために**検出するを**クリックして下さい。



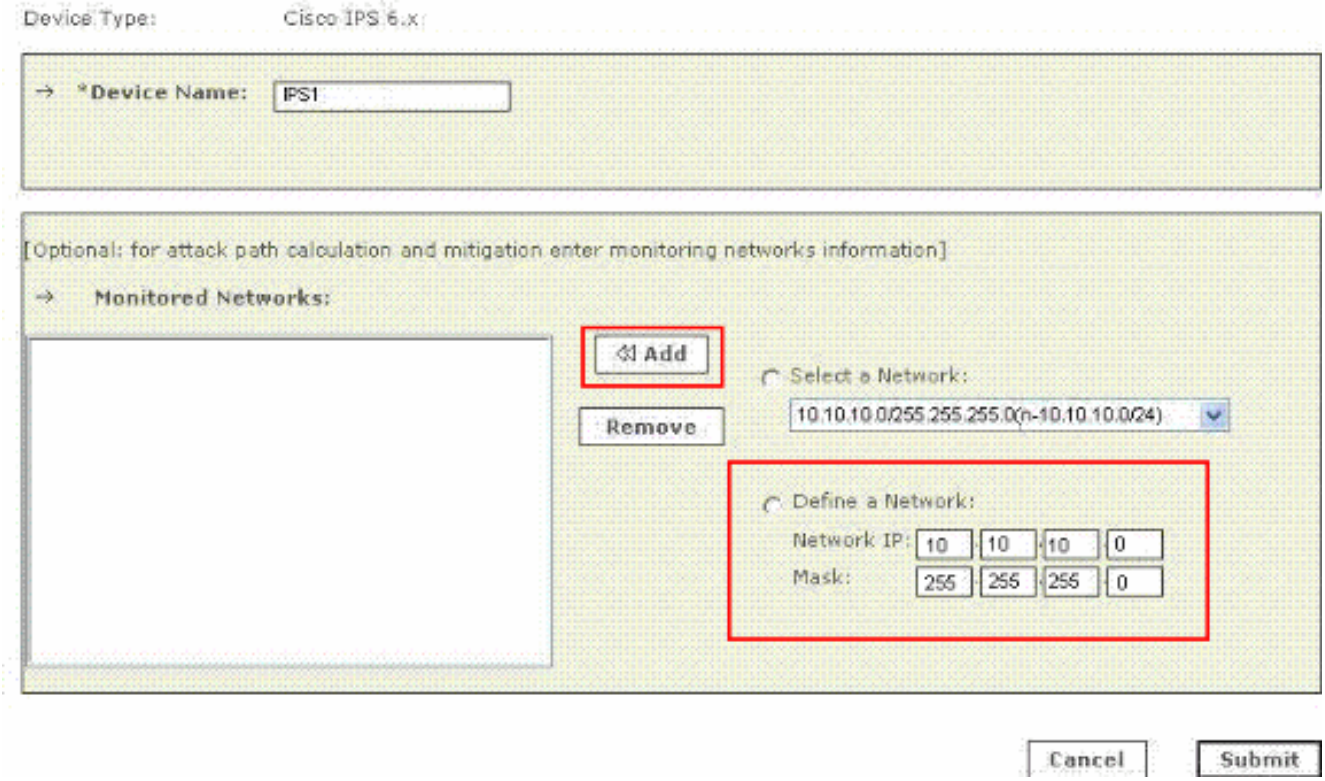
注: MARS は行うセンサーへの変更をに気づいていないです。 バーチャル センサー設定への変更を行なう、MARS のバーチャル センサー詳細をリフレッシュするためにそのセンサー設定 ページの**検出するを**クリックして下さい。

8. チェックボックスをバーチャル センサー名前の隣で選択し、各々のバーチャル センサーのための監視されたネットワークを定義するために『Edit』 をクリック して下さい。 この場合 IPS モジュール ページはここに示されているように提示されます。



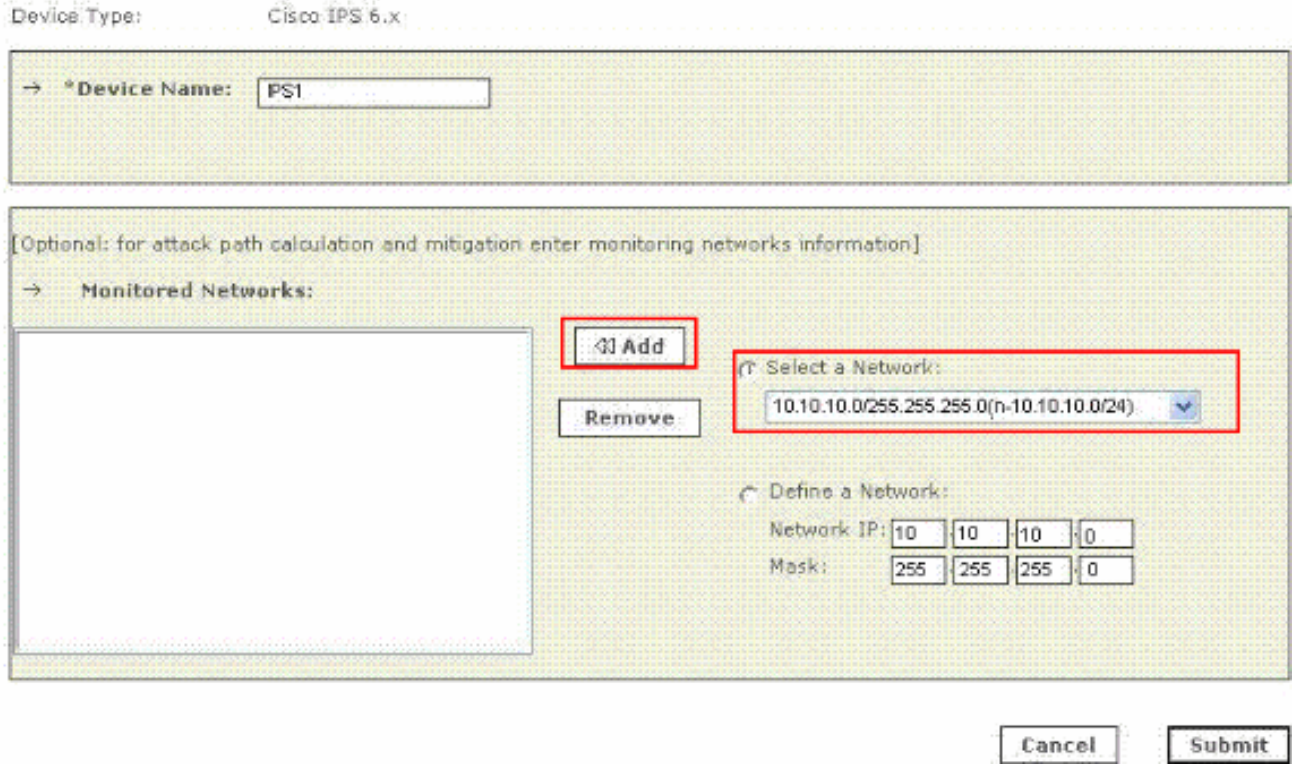
9. 不正侵入パス計算および軽減に関しては、センサーによって監察されるネットワークを規定して下さい。 手動で ネットワークを定義するために**定義をネットワーク** Radio ボタン選択して下さい。 それからネットワークを定義するためにこれらのステップを完了して下さい :**ネットワーク IP** フィールドでネットワーク アドレスを入力して下さい。**Mask フィールド**で対応した ネットワーク マスク値を入力して下さい。監視されたネットワーク フィールドに特定のネットワークを移動するために『Add』 をクリック して下さい。より多くのネッ

トワークを定義する必要がある場合前の手順を繰り返して下さい。



注: これは必要とされなくて利用可能なオプション機能で、スキップすることができます。

10. **選り抜きを**順序で**ネットワーク** Radio ボタン選択しますデバイスに接続するネットワークをクリックして下さい。 それからネットワークを選択するためにこれらのステップを完了して下さい:**選り抜き**からネットワークを**ネットワーク** リスト選択して下さい。監視されたネットワーク フィールドに特定のネットワークを移動するために『Add』 をクリック して下さい。ネットワークを『More』 を選択 する必要がある場合前の手順を繰り返して下さい。



注: これは必要とされなくて利用可能なオプション機能で、スキップすることができます。

11. **ステップ 8** から各々のバーチャル センサーのための**ステップ 10 を**繰り返して下さい。
12. 変更を保存するために『SUBMIT』 をクリック して下さい。 デバイス名はセキュリティお

よびモニタリング 情報リストの下で現われます。 送信するオペレーションはデータベーステーブルの変更を記録します。 しかし、それは MARS アプライアンスの作業 メモリに変更をロードしません。 アクティブ化オペレーション負荷は作業 メモリに変更を入れました。

13. MARS がこのデバイスからのイベントを sessionize 始めることを可能にするために『Activate』 をクリック して下さい。MARS はこのモジュールによって生成されるイベントを sessionize、それらのイベントを定義されたインスペクションを使用して評価し、ルールを廃棄し始めます。 アクティベーションが一致条件としてデバイスのレポート IP アドレスと問い合わせることができる前に MARS にデバイスによって送達されるイベント。 アクティブ化をレポートおよび軽減デバイス参照して下さい。 アクティブ化操作に関する詳細については。

MARS が Cisco IPS デバイスからのイベントを引っ張ることを確認して下さい

それはよくありますデータフローを確認するためにネットワークの良性 イベントを作成するように。 Cisco IPS デバイスと MARS 間のデータフローを確認するためにこれらのステップを完了して下さい:

1. Cisco IPS デバイスで、2000 年および 2004 年シグニチャを有効に し、警告 して下さい。 シグニチャ モニタ ICMP メッセージ（ping）。
2. Cisco IPS デバイスが受信しているサブネットのデバイスを ping して下さい。 イベントは MARS によって生成され、引っ張られます。
3. イベントが MARS Webインターフェイスに現われることを確認して下さい。 Cisco IPS デバイスによってクエリを行うことができます。
4. データ・フローが確認されれば、Cisco IPS デバイスの 2000 年および 2004 のシグニチャを無効に することができます。**注:** テスト接続オペレーションが MARS Webインターフェイスで Cisco IPS デバイスの設定の間に失敗しなかった場合、通信は有効に なります。 このタスクは更にアラートが正しく生成され、引っ張られることを確認することを可能にします。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- Cisco Security Monitoring，Analysis and Response System サポートページ
- Cisco Intrusion Prevention System に関するサポート ページ
- シスコのセキュリティ モニタリング、分析および応答システム - 互換性情報
- Requests for Comments（RFC）
- テクニカル サポートとドキュメント – Cisco Systems