はじめに

内容

このドキュメントでは、Cisco IPS 7.0 CLI を使用してセンサーを設定する方法について説明します。次の項目について説明します。

対象読者

このマニュアルは、次の作業を実行する必要のある管理者を対象にしています。

- CLI を使用した侵入防御用のセンサーの設定。
- IPS センサーによるネットワークのセキュリティ保護。
- ネットワークへの侵入に対する防御とそれに続くアラートのモニタ。

マニュアルの構成

このマニュアルの構成は、次のとおりです。

項	タイトル	説明
1	「CLI 設定ガイドについて」	CLI 設定ガイドの目的について説明します。
2	「センサーへのログイン」	各種センサーへのログイン方法について説明します。
3	「センサーの初期化」	**setup** コマンドを使用してセンサーを初期化する方法について説明します。
4	「センサーのセットアップ」	CLI を使用してセンサーを初期設定する方法について説明します。
5	「インターフェイスの設定」	無差別、インライン、インライン VLAN ペア、および VLAN グループ インターフェイスの設定方法について説明します。

項	タイトル	説明
6	「仮想センサーの設定」	仮想センサーの設定方法について説明します。
7	「イベント アクション規則の設定」	センサーでイベント アクション規則ポリシーを設定する方法について説明します。
8	「シグニチャの定義」	シグニチャの追加方法、複製方法、および編集方法について説明します。
9	「異常検出の設定」	センサーで異常検出ポリシーを設定する方法について説明します。
10	「グローバル相関の設定」	センサーでグローバル相関機能を設定する方法について説明します。
11	「外部製品インターフェイスの設定」	CSA MC 用に外部製品のインターフェイスを設定する方法について説明します。
12	「IP ロギングの設定」	センサーで IP ロギングを設定する方法について説明します。
13	「インターフェイスのライブ トラフィックの表示とキャプチャ」	センサー インターフェイス上のライブ トラフィックを表示およびキャプチャする方法について説明します。
14	「Attack Response Controller でのブロッキングとレート制限の設定」	Cisco ルータおよびスイッチにブロッキングおよびレート制限を設定する方法、およびマスター ブロッキング センサーを設定する方法について説明します。
15	「SNMP の設定」	センサーで SNMP を設定する方法について説明します。
16	「コンフィギュレーション ファイルの操作」	センサーでコンフィギュレーション ファイルを使用する方法について説明します。
17	「センサーの管理タスク」	センサーの動作を維持し、最新の状態にしておくために役立つ各種の管理手順について説明します。
18	「AIM IPS の設定」	AIM IPS の設定方法について説明します。
19	「AIP SSM の設定」	AIP SSM の設定方法について説明します。
20	「IDSM2 の設定」	IDSM2 の設定方法について説明します。
21	「NME IPS の設定」	NME IPS の設定方法について説明します。
22	「ソフトウェアの入手」	最新の IPS ソフトウェアの入手方法、および命名規則について説明します。
23	「システム イメージのアップグレード、ダウングレード、およびインストール」	センサーをアップグレードして、各種センサーのイメージを再作成する方法について説明します。
A	「システム アーキテクチャ」	IPS システム アーキテクチャについて説明します。
B	「シグニチャ エンジン」	IPS シグニチャ エンジンと、そのパラメータについて説明します。
C	「トラブルシューティング」	IPS ハードウェアおよびソフトウェアのトラブルシューティングに役立つヒントを示します。
D	「CLI のエラー メッセージ」	CLI エラー メッセージを示します。

項	タイトル	説明
E	「オープン ソース ライセンス ファイル」	IPS で使用されているオープン ソース ライセンス ファイルを示します。
用語集	「Glossary」	Cisco IPS に関連する用語を示します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、*イタリック体*フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{ x | y | z }	必ずいずれか 1 つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x | y | z]	いずれか 1 つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。

ヒント 「*問題解決に役立つ情報*」です。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

ワンポイントアドバイス *時間を節約する方法*です。ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 **「*警告*」の意味です。人為ミスを予防するための注意事項が記述されています。**

関連資料

Cisco IPS 7.0 の詳細については、次の URL で、以下に示すマニュアルを参照してください。

http://www.cisco.com/en/US/products/hw/vpndevc/ps4077/tsd_products_support_series_home.html

- 『*Documentation Roadmap for Cisco Intrusion Prevention System 7.0*』
- 『*Release Notes for Cisco Intrusion Prevention System 7.0*』
- 『*Installing and Using Cisco Intrusion Prevention System Device Manager 7.0*』
- 『*Installing and Using Cisco Intrusion Prevention System Manager Express 7.0*』
- 『*Cisco Intrusion Prevention System Command Reference 7.0*』
- 『*Installing Cisco Intrusion Prevention System Appliances and Modules 7.0*』
- 『*Installing and Removing Interface Cards in Cisco IPS 4260 and IPS 4270-20*』
- 『*Regulatory Compliance and Safety Information for the Cisco Intrusion Prevention System 4200 Series Appliance Sensor*』

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダーアプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。