概要

ここでは、Cisco Traffic Anomaly Detector Module の Web-Based Manager（WBM）インターフェイスの概要について説明します。この章は、次の項で構成されています。

クライアントの要件

この項では、WBM クライアントの最小要件について説明し、次の情報および手順を示します。

最小要件

Detector モジュールの WBM にアクセスして使用するためのクライアントの最小要件は次のとおりです。

- Microsoft Internet Exploler 5.0 以降：HTML、テーブル、Cookie、JavaScript、およびフレームをサポートしている必要があります。
- Sun Microsystems Java 2 Runtime Environment（JRE）Standard Edition バージョン 1.4.2_04：JRE は、リアルタイム カウンタの表示にのみ必要です（「Java 2 Runtime Environment のインストール」の項を参照）。
- モニタの解像度：1024 x 768 ピクセル以上にすることをお勧めします。

Java 2 Runtime Environment のインストール

リアルタイム カウンタを表示するには、Java 2 Runtime Environment（JRE）をインストールする必要があります。JRE を Sun Microsystems の Web サイトからダウンロードしてインストールするには、次の手順を実行します。

ステップ 1　Web ブラウザで www.sun.com を開きます。Sun Microsystems のホーム ページが表示されます。

ステップ 2　**Downloads** > **Java 2 Standard Edition** を選択して、ダウンロード ページに移動します。バージョン番号を選択して、使用するバージョンのダウンロード サイトを開きます。

ステップ 3　J2SE JRE をダウンロードします。

J2SE v < *バージョン番号* > JRE カテゴリまで下方向にスクロールして、**Download J2SE JRE** を選択します。

（注）　J2SE SDK は選択しないでください。

ステップ 4　ダウンロードしたファイルを実行して、Sun Microsystems によるオンライン インストールの手順に従います。

ステップ 5　使用しているブラウザを JRE がサポートしていることを確認します。次の操作を実行します。

1. 使用しているマシン上で **Start** > **Settings** > **Control Panel** を選択して、Windows のコントロール パネルを開きます。コントロール パネルが表示されます。
2. Java Plug-in を見つけて、ダブルクリックします。Java(TM) Control Panel が表示されます。
3. Advanced タブをクリックします。<APPLET> tag support セクションを開いて、使用しているブラウザの隣にあるチェックボックスをオンにします。

（注）　JRE の以前のバージョンがインストールされていた場合、サポートされているブラウザは別のタブに表示されます。Browser タブをクリックし、Settings の下で、使用しているブラウザの隣にあるチェックボックスをオンにします。

4. Apply をクリックして、設定を保存します。
5. ブラウザを再起動します。

WBM 動作用の Detector モジュールの要件

WBM を使用する前に、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』に記述されているように、Detector モジュールが適切にインストールされていることを確認します。初期設定プロセスは、CLI を使用して実行する必要があります。WBM が正常に動作するために、次の項目が Detector モジュールに設定されていることを確認してください。

- ゾーン トラフィックのコピー：（CLI 機能）ネットワーク スイッチがゾーンに送信されたトラフィックをキャプチャし、そのコピーを分析用に Detector モジュールに送信できるようにします。
- リモート Guard リスト：（CLI 機能）Detector モジュールがトラフィックの異常を検出したときにアクティブにする Guard デバイスのリストを Detector モジュールに提供します。
- SSL 接続：（CLI 機能）Detector と Cisco Anomaly Guard Module との間に安全なチャネル接続を提供します。
- WBM サービスのイネーブル化とアクセスの許可：（CLI 機能）WBM サービスをアクティブにし、WBM ワークステーションから WBM サービスへのアクセスを許可します。この動作を設定するための CLI の手順については、このマニュアルにも記載されています（第 2 章「WBM のイネーブル化と起動」の「WBM へのネットワーク アクセスの設定」の項を参照）。

DDoS 攻撃とは

Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃は、コンピュータ ハッカーが、何千もの信頼のおけないコンピュータ（ゾンビ）に自動化されたスクリプトを実行させ、ネットワーク リソースを偽のサービス要求によって使用できなくする攻撃です。DDoS 攻撃には、Web サーバに偽のホーム ページ要求を大量に送信して正当な消費者がアクセスできないようにしたり、Domain Name System（DNS; ドメイン ネーム システム）サーバのアベイラビリティと正確性を損なわせようとするものなどがあります。ゾンビは、多くの場合、個人によって開始されますが、実際に攻撃用コードを実行しているものは、複数の組織によって管理される複数の自律システム上に分散しており、その数は何十万にも及ぶ可能性があります。

DDoS 攻撃は、高度な技術を持つハッカーが新しい有害なプログラムを作成するのに伴い、進化を続けています。また、これらの攻撃スクリプトはインターネット上で容易に入手でき、ネットワークに関する技術知識があまりない人物がごく普通に実行しています。このため、DDoS 防御テクノロジーは柔軟かつ臨機応変なものである必要があります。DDoS 防御システムは、攻撃の対象となるネットワーク要素の正当なトラフィック フローに影響を与えずに、仕掛けられる DDoS 攻撃を検出し、悪意のあるトラフィックと正当なトラフィックを識別できる必要があります。

Cisco Traffic Anomaly Detector Module

Cisco Traffic Anomaly Detector Module は、異常の検出と保護のアクティベーションのためのデバイスです。Detector モジュールは、Cisco Anomaly Guard Module との併用に最も適していますが、独立した DDoS 検出および警告コンポーネントとしても運用できます。

Detector モジュールは常時トラフィックを監視し、ゾーンのトラフィック特性に合せて細かく調整された状態で、新たに発生する攻撃パターンに備えます。

これらのタスクを達成するために、Detector モジュールは次の機能を備えています。

- アルゴリズムに基づいたラーニング システム。このラーニング システムは、ゾーンのトラフィックをラーニングし、ゾーンの設定を特定のトラフィック特性に合せて変更し、ゾーンのトラフィック ポリシーとポリシーしきい値レートという形で参考値と指示を与えることにより、Detector の攻撃検出機能をサポートします。
- Cisco Anomaly Guard Module をリモートでアクティブにしてゾーンを保護状態に置くか、または Detector の syslog にトラフィックの異常を記録する攻撃通知システム。

これらの機能を統合しているため、Detector はネットワークの動作を阻害せずにバックグラウンドで DDoS 攻撃検出処理を実行できます。

WBM のインターフェイス

WBM は、CLI の一部の機能を提供することによって、ユーザによるゾーン設定の作成と変更、ゾーン トラフィック異常の検出の管理、および Detector モジュールとゾーンの動作の監視を可能にしています。Detector モジュールの初期セットアップや Detector モジュールのネットワーク レベルのセットアップなどの手順に関係する設定パラメータは、CLI を使用した場合のみアクセスできます。WBM を使用して設定することはできません。CLI の使用の詳細については、『*Cisco Traffic Anomaly Detector Configuration Guide*』を参照してください。

WBM のブラウザ ウィンドウ

図 1-1 に、WBM のウィンドウ画面の例を示します。図の中に引き出し線で示されている各セクションについては、表 1-1 で説明します。

図 1-1　　WBM の画面の例

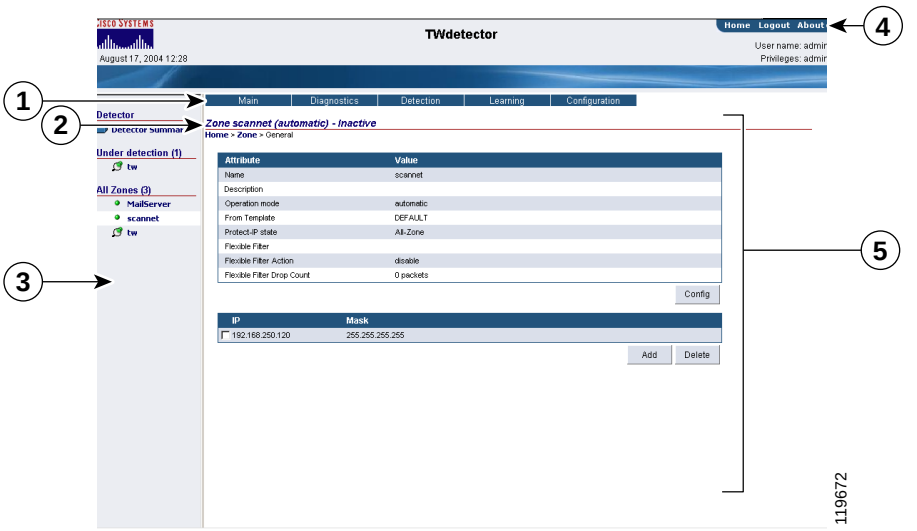

表 1-1　WBM のウィンドウの概要

セクション	機能
1	**メイン メニュー バー**：ナビゲーション ペインで選択されたリンクのメイン メニューを表示します。このセクションには、次の 2 つのメニュー バーのいずれかが表示されます。 • Detector モジュールの要約メニュー : Detector モジュールの次の統計オプションおよび設定オプションへのアクセスを提供します。 — Detector モジュールのステータス ツールおよび診断ツール — 定義済みゾーンのリスト — ユーザ プロファイル マネージャ Detector モジュールの要約メニューを表示するには、ナビゲーション ペイン（3）にある **Detector Summary** をクリックします。 • ゾーンのメイン メニュー : ゾーンの詳細情報および設定オプションにアクセスできます。 個々のゾーンのメニューを表示するには、ナビゲーション領域（3）に表示されている目的のゾーンをクリックします。
2	**ナビゲーション パス**：作業領域（5）に表示された画面へのパスを表示します。パスの特定のセクションに移動するには、パスの目的のセクションをクリックします。
3	**ナビゲーション領域**：Detector モジュールの要約画面およびゾーンのステータス画面へのリンクのリストを表示します。リストにあるリンクをクリックすると、関連するステータス情報が作業領域（5）に表示されます。ナビゲーション領域で選択したリンクは、白色の枠で強調表示されます。 ナビゲーション領域のサイズを変更するには、ナビゲーション領域と作業領域の間にあるフレーム バーをドラッグします。

表 1-1　WBM のウィンドウの概要（続き）

セクション	機能
4	**情報領域**：次のリンクと情報が表示されます。 • Home：Detector モジュールの要約画面に戻ります。 • Logout：現在の WBM セッションを終了します。System Login 画面が表示されます。 • About：WBM　ソフトウェアに関する情報を表示します。ソフトウェアのバージョン番号、システムのシリアル番号、およびソフトウェア ライセンス契約が含まれています。 • Current user：現在のユーザの名前、およびこのユーザに割り当てられているユーザ特権レベルを表示します。
5	**作業領域：**選択した情報が表示されます。作業領域では、さまざまなゾーン設定パラメータを定義し、ラーニングと検出をイネーブルにし、統計情報を表示します。作業領域のサイズを変更するには、ナビゲーション領域と作業領域の間にあるフレーム バーをドラッグします。

ゾーンのステータス アイコン

WBM では、アイコンを使用してゾーンの現在のステータスを表現しています。ステータス アイコンは、ナビゲーション領域とゾーンのステータス バーに表示されます。表 1-2 に、各種のゾーン ステータス アイコンの説明を示します。

表 1-2　ゾーンのステータス アイコン

アイコン	ステータス
	ゾーンは非アクティブです（ゾーン トラフィックのラーニングおよび異常検出を実行していません）。
	ゾーンはアクティブで、ラーニング プロセスのポリシー構築フェーズまたはしきい値調整フェーズに入っています。
	ゾーンはアクティブで、異常検出モード、または検出とラーニング モードになっています。
	ゾーンはアクティブで、インタラクティブ検出モードで動作しています。新しいゾーン検出の推奨事項が参照可能になっています。

WBM のナビゲーション マップ

この項の表では、2 つの WBM メニュー バーから使用できるさまざまなリンクの一覧と配置を示します。

- Detector モジュール要約メニュー：Detector モジュールの一般的な統計ツールおよび設定ツールへのアクセスを提供します。Detector モジュールの要約メニューを表示するには、ナビゲーション領域の **Detector Summary** または情報領域の **Home** をクリックします。表 1-3 に、さまざまな Detector 要約メニューのレベルのマップを示します。

表 1-3　Detector 要約メニュー

レベル 1	レベル 2	レベル 3
Detector Summary	Main	Summary
	Diagnostics	Counters
		Event log
		Real time counters
	Zones	Zone list
		Create zone
		Template list
		Compare zone policies
	Users	User list
		Create user
		Change password

- ゾーン　メニュー：個々のゾーンの統計ツールおよび設定ツールにアクセスできます。ゾーン メニューを表示するには、ナビゲーション領域に表示されている目的のゾーンをクリックします。表 1-4 に、さまざまなゾーン メニュー レベルのマップを示します。

表 1-4　ゾーン メニュー

レベル 1	レベル 2	レベル 3
Zone	Main	Summary
		Create zone
		Save as. . .
	Diagnostics	Counters
		Event log
		Attack reports
		HTTP Zombies
		Policy statistics
		Real time counters
		Start Packet-Dump
		Stop Packet-Dump
		Packet-Dump List
	Detection	Detect
		Deactivate
		Dynamic Filters
		Recommendations
	Learning	Construct Policies
		Tune Threshold
		Deactivate
		Stop Learning
		Accept
		Snapshot
		Snapshot List

表 1-4　ゾーン メニュー（続き）

レベル 1	レベル 2	レベル 3
Zone （続き）	Configuration	General
		User Filters
		Bypass Filters
		Flex-Content Filters
		Policy Templates
		Add Service
		Remove Service
		Policy
		Compare Policies
		Learning Parameters