CHAPTER 1

製品の概要

この章では、Cisco Traffic Anomaly Detector Module（Detector モジュール）Web-Based Manager（WBM）の概要を説明します。WBM は Detector モジュールのリモート操作と監視に使用できます。WBM は、HTML ページを Detector モジュール コマンドに変換することによって Detector モジュールと通信するグラフィカル ユーザ インターフェイスです。Detector モジュールの機能の中で、主に Detector モジュールの初期インストールと設定に関連するものには、CLI によってのみ設定でき、WBM では設定できないものがあります。CLI の使用方法の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。

ここでは、Detector モジュールの付属製品である Cisco Guard（Guard）について説明します。Guard は Distributed Denial of Service（DDoS; 分散型サービス拒絶）攻撃を検出および軽減するデバイスです。攻撃トラフィックをドロップし、正当なトラフィックをネットワークに再注入することで、トラフィックがゾーンを通過するときにゾーン トラフィックをクリーニングします。Detector モジュールは、ゾーンが攻撃を受けていると判断したときに、Guard の攻撃軽減サービスをアクティブにすることができます。また、Detector モジュールはゾーンの設定を Guard と同期させることもできます。Guard の詳細については、『*Cisco Anomaly Guard Module Configuration Guide*』または『*Cisco Guard Configuration Guide*』を参照してください。

この章は、次の項で構成されています。

ユーザ インターフェイス要件

ここでは、WBM クライアントの最小要件について説明します。この項は、次の内容で構成されています。

最小要件

Detector モジュール上で WBM にアクセスして WBM を使用するための最小要件は、次のとおりです。

- Microsoft Internet Exploler 5.5 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（SE）バージョン 5.0 以降：JRE は、リアルタイム カウンタの表示に必要です（「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 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 URL 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 SE** ページに移動して、**Java Runtime Environment (JRE) 5.0 Update 11** 以降を選択します。

ステップ 3　ライセンス契約に同意し、Java Runtime Environment（JRE）5.0 Update 11 以降をダウンロードします。

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。

WBM の動作に関する Detector モジュールの要件

WBM を使用する前に、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』で説明されているとおりに Detector モジュールが正しく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 を正しく動作させるために、Detector モジュール上で次の機能が設定されていることを確認します。

- ネットワーク インターフェイスの設定 : Detector モジュールのネットワーク インターフェイスを設定します。ネットワーキング環境での動作について、Detector モジュールのインターフェイスを設定するまでは、Detector モジュールに接続できません。
- WBM サービスのイネーブル化とアクセスの許可 : Detector モジュール上の WBM サービスをイネーブルにし、WBM クライアントから Detector モジュール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（「WBM のネットワーク アクセスの設定」の項を参照）。
- リモート Guard リストの設定 : Detector モジュールがゾーンのトラフィックで異常を検出したときに、Detector モジュールがアクティブにできるリモート Guard を定義します。
- Detector モジュールと各 Guard の間の通信チャネルの設定 : Detector モジュールとリモート Guard リストにある各 Guard との間に Secure Sockets Layer（SSL）通信チャネルまたは Secure Shell（SSH; セキュア シェル）通信チャネルを設定します。Detector モジュールは、ゾーンのトラフィックで異常を検出したときに、通信チャネルを使用して Guard をアクティブにできます。
- ゾーン トラフィックのコピー : ゾーン トラフィックのコピーを分析用に Detector モジュールに送信するように、スーパーバイザ エンジンを設定します。

Detector モジュールについて

Detector モジュールは、ネットワーク トラフィックのコピーを監視して、サーバ、ファイアウォール インターフェイス、ルータ インターフェイスなどのネットワーク要素（ゾーン）を対象に、DDoS 攻撃の兆候を継続的に検出します。

Detector モジュールは、独立した DDoS 検出および警告コンポーネントとして運用できますが、Detector モジュールの付属製品である Guard との併用に最も適しています。

Detector モジュールは、次のいずれかの製品にインストールすることができます。

- Catalyst 6500 シリーズ スイッチ
- Cisco 7600 シリーズ ルータ

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 Detector モジュールに送信するようにスイッチを設定する必要があります。

Detector モジュールは、一連のゾーン ポリシーを使用して、すべての着信ゾーン トラフィックのコピーを分析します。ゾーン ポリシーを使用すると、Detector モジュールは、ゾーンへの攻撃の兆候を示すトラフィック異常がないかどうかを識別できます。トラフィック異常を識別すると、Detector モジュールは syslog メッセージを発行して攻撃の存在を通知したり、Guard をアクティブにして攻撃を軽減させることができます。

Detector モジュールは次のタスクを実行します。

- トラフィックのラーニング：アルゴリズムに基づいたプロセスを使用して、正常なゾーン トラフィックの特性（サービスとトラフィック レート）をラーニングします。ラーニング プロセス時、Detector モジュールは、デフォルトのゾーン トラフィック ポリシーとポリシーのしきい値を正常なゾーン トラフィックの特性に合せて変更します。トラフィックのポリシーとしきい値は、ゾーンのトラフィックが正常か異常（ゾーンへの攻撃を示す）かを判断するときに Detector モジュールによって使用される参照ポイントを定義します。
- トラフィック異常の検出：正常なトラフィックの特性に基づき、ゾーンのトラフィックの異常を検出します。

DDoS 攻撃について

DDoS 攻撃は、正当なユーザによる特定のコンピュータまたはネットワーク リソースへのアクセスを拒絶します。この攻撃は、悪意のある要求をターゲットに送信する個人が発信元です。悪意のある要求は、サービスを低下させ、コンピュータ サーバやネットワーク デバイス上のネットワーク サービスを混乱させ、ネットワーク リンクを不要なトラフィックで飽和させます。

この項は、次の内容で構成されています。

スプーフィングを利用した攻撃について

スプーフィングを利用した攻撃は DDoS 攻撃の一種です。この攻撃では、パケットのヘッダーに実際の送信元デバイスの IP アドレスではない IP アドレスが含まれています。スプーフィング パケットの送信元 IP アドレスは、ランダムな場合も特定のアドレスに集中している場合もあります。スプーフィングを利用した攻撃により、ターゲット サイトのリンクとそのサイトのサーバ リソースが飽和します。コンピュータ ハッカーは、スプーフィングを利用した大量の攻撃を単一のデバイスからでも容易に生成できます。

スプーフィング以外の攻撃について

スプーフィング以外の攻撃（クライアント攻撃）は、ほとんどが実際の TCP 接続を伴う TCP ベースの攻撃で、ネットワーク リンクやオペレーティング システムではなく、サーバのアプリケーション レベルで機能を低下させます。

多数のクライアント（ゾンビ）からのクライアント攻撃では、個別のどのクライアントも異常を発生させることなくサーバ アプリケーションの機能を低下させる場合があります。ゾンビ プログラムは、ターゲット サイトにアクセスする正当なブラウザを模倣しようとします。

ゾーンとゾーン ポリシーについて

Detector モジュールがトラフィック異常を監視するゾーンは、次の要素のいずれかです。

- ネットワーク サーバ、ネットワーク クライアント、ルータ
- ネットワーク リンク、サブネット、またはネットワーク全体
- 個々のインターネット ユーザまたは企業
- インターネット サービス プロバイダー（ISP）
- これらの要素の任意の組み合せ

新しいゾーンを作成する場合は、ゾーンに名前を付け、ゾーンにネットワーク アドレスを設定します。Detector モジュールは、ゾーンのトラフィックの異常を検出するために、ポリシーおよびポリシーしきい値のデフォルト セットを使用してゾーンを設定します。詳細については、第 6 章「ポリシー テンプレートの設定」の「ポリシー テンプレートについて」および第 8 章「ゾーンのポリシーの管理」の「ゾーンのポリシーについて」の項を参照してください。

Detector モジュールは、ゾーンのネットワーク アドレスの範囲が重なっていなければ、複数のゾーンのトラフィックを同時に監視できます。

WBM インターフェイスについて

WBM は、Detector モジュール設定と管理機能へのアクセスを提供するブラウザベースのグラフィカル ユーザ インターフェイス（GUI）です。WBM では、CLI 機能のサブセットが提供され、ゾーンの設定の作成と変更、ゾーン保護の管理、Detector モジュールとゾーンの動作の監視を実行できます。Detector モジュールの機能の中で、主に Detector モジュールの初期インストールと設定に関連するものには、CLI によってのみ設定でき、WBM では設定できないものがあります。CLI の使用方法の詳細については、『*Cisco Traffic Anomaly Detector Module Configuration Guide*』を参照してください。

この項は、次の内容で構成されています。

WBM ブラウザ ウィンドウについて

図 1-1 および表 1-1 に、WBM ウィンドウの各セクションを示します。

図 1-1　WBM 画面の各セクション

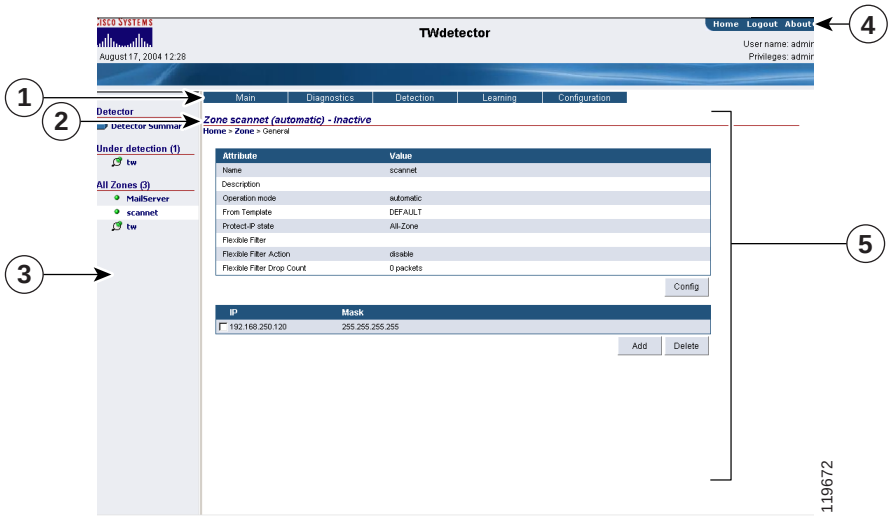

表 1-1　WBM ウィンドウの各セクション

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 の要約メニュー：次の Detector モジュールの統計オプションと設定オプションにアクセスできます。 — Detector モジュールのステータス ツールと診断ツール — 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表示領域の間にあるフレーム バーをドラッグします。
4	情報領域：現在のユーザのユーザ名と特権レベルを表示し、次のリンクを示します。 • Home：Detector の要約画面に戻ります。 • Enable：ユーザ特権レベル間を移動します。 • Logout：WBM セッションを閉じます（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。 • シスコシステムズのアイコン：cisco.com の Detector モジュールのホームページへのリンクです。
5	作業領域：選択した情報を表示します。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 アイコンについて

WBM では、ゾーンの現在のステータスを示すためにアイコンが使用されています。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、各ステータス アイコンが表す内容の説明を示します。

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。Detector モジュールは、ゾーン トラフィックをラーニングしていないか、ゾーン トラフィックの異常を監視していません。
	ゾーンはアクティブで、ラーニング プロセスのフェーズです。Detector モジュールは、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を実行しています。
	ゾーンはアクティブです。Detector モジュールは、ゾーン トラフィックの異常を監視しているか、ゾーン トラフィックの異常の監視とゾーン トラフィックのラーニングを同時に実行しています。
	ゾーンはアクティブです。Detector モジュールはゾーンに対する攻撃を監視中です。ユーザの注意を必要とする新しいゾーン保護推奨事項を使用できます。

WBM のナビゲーション マップについて

メニューまたはナビゲーション パスを使用して、画面階層内を移動できます（表 1-1 のセクション 2 を参照）。メニューの選択項目は、ドロップダウン リストで示されます。現在の表示で使用できない選択項目は、グレー表示されています。

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

- Detector の要約メニュー：一般的な Detector モジュールの統計ツールと設定ツールにアクセスできます。Detector 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、Detector の要約メニュー レベルのマップを示します。

表 1-3　Detector の要約メニュー

レベル 1	レベル 2	レベル 3
Main	Summary	
Diagnostics	Counters	Device counters
		Real-time counters
	Event log	
	Device Resources	
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、ゾーン メニューの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
Main	Summary	
	Create zone	
	Save as. . .	
Diagnostics	Counters	Zone Counters
		Real-time counters
	Event log	
	Attack reports	Attack Summary
		HTTP Zombies
	Statistics	Policy statistics
		Drop Statistics
	Packet-Dump	Start Packet-Dump
		Stop Packet-Dump
		Packet-Dump List
Detection	Detect	
	Deactivate	
	Dynamic Filters	
	Recommendations	
Learning	Construct Policies	
	Tune Thresholds	
	Deactivate	
	Stop Learning	
	Accept	
	Snapshot	
	Snapshot List	
Configuration	General	
	Filters	User Filters
		Bypass Filters
		Flex-Content Filters
	Policy Templates	View
		Add Service
		Remove Service
	Policies	View
		Compare Policies
		Learning Parameters