概要

ここでは、WBM の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

Guard 上で WBM にアクセスして WBM を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：1,024 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 の動作のための Guard の要件

WBM を使用する前に、『*Cisco Guard Configuration Guide*』の説明に従って Guard を正しくインストールしてください。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、Guard 上で次の項目が設定されていることを確認します。

- ネットワークの設定：Guard のネットワーク インターフェイスを設定します。使用しているネットワーク環境で動作するように Guard のインターフェイスを設定するまでは、Guard に接続できません。
- トラフィックの宛先変更：ゾーン保護がアクティブになっているときは、ゾーンのトラフィックを Guard に宛先変更します。トラフィックの宛先を変更すると、正当なトラフィックを Guard がネットワークにどのように再注入するかも定義されます。
- WBM サービスのイネーブル化とアクセスの許可：WBM ワークステーションから Guard へのアクセスをイネーブルにし、定義します。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。

高度な知識を持ったハッカーは、攻撃用の新たな不正手段を生み出し続けており、DDoS 攻撃は常に進化しています。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。したがって、DDoS 防御テクノロジーは、柔軟で適応力のある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 Guard

Cisco Guard は、分散型アップストリーム構成に ISP/MSP/ バックボーン レベルで配置して、ネットワーク全体を保護するための高パフォーマンス ネットワーク デバイスです。Guard 上でゾーン保護をイネーブルにすると、Guard がゾーンのトラフィックを自身に宛先変更して、トラフィックに異常がないかどうかの分析を開始します。Guard は DDoS 攻撃の構成要素をすべてブロックし、正当なトラフィックのみを目的のゾーンに転送します。Guard は、ゾーンのトラフィックを常に分析およびフィルタリングしながら透過的に通過させて、ゾーン トラフィックの特性と新たに発生する攻撃パターンに合せて調整された状態を維持します。

これらのタスクを達成するために、Guard は次の機能を備えています。

- トラフィックの宛先変更メカニズム。このメカニズムにより、ゾーンのトラフィックが Guard のラーニング システムと保護システムにリダイレクト（宛先変更）され、その後正当なトラフィック フローがゾーンに転送されます。Guard は、通常のネットワーク トラフィック フローを妨げることなくトラフィックを宛先変更します。
- 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、ゾーンの実行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しきい値レートとポリシーという形で参考値と保護の指示を与えることにより、保護システムをサポートします。また、Guard はオンデマンド保護を提供できます。この機能により、Guard がまだラーニング プロセスを完了しておらず、ゾーンのポリシーをゾーン トラフィックのパターンに合せて調整していないときにゾーンに対する攻撃が発生する状況にも対応できます。
- 正当なトラフィックと疑わしいトラフィックを区別し、悪意のあるトラフィックをフィルタリングする保護システム。Guard は、正当なトラフィックのみをゾーンに転送します。

Guard は、これらの機能を統合することにより、DDoS 攻撃発生時には保護の役割を果たし、通常時にはバックグラウンドに控えた状態を保つことができます。

WBM のインターフェイス

WBM は、さまざまな Guard 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 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、Guard とゾーンの動作の監視を実行できます。Guard の初期セットアップや Guard 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。CLI の使用の詳細については、『*Cisco Guard 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 のスクリーン ショットの例

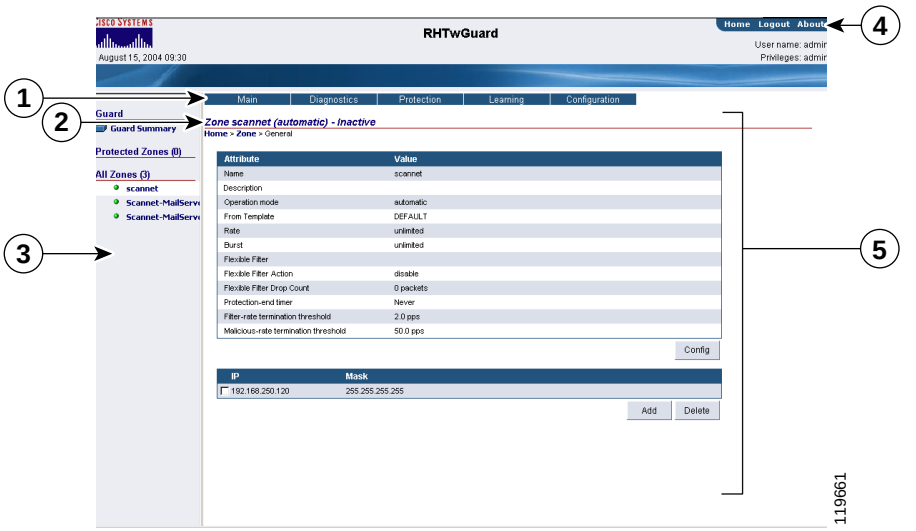

表 1-1　WBM のウィンドウの概要

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。 • Guard の要約メニュー：Guard の次の統計オプションおよび設定オプションにアクセスできます。 — Guard のステータスと診断ツール — 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 Guard 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）の **Guard 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**：Guard の要約画面と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。

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示されます。 • Home：Guard 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、ラーニングと保護をイネーブルにし、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、現在のゾーン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
	ゾーンが非アクティブです（ゾーンのトラフィックをラーニングしていないか、ゾーンを保護していません）。
	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。
	ゾーンがアクティブで、ゾーンの保護モードまたは保護とラーニング モードになっています。
	ゾーンがアクティブで、インタラクティブ保護モードで動作しています。新しいゾーン保護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。

- Guard の要約メニュー：Guard のよく使用される統計ツールおよび設定ツールにアクセスできます。Guard の要約メニューを表示するには、ナビゲーション領域の **Guard 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 Guard の要約メニュー レベルのマップを示します。

表 1-3　Guard の要約メニュー

レベル 1	レベル 2	レベル 3
Guard Summary	Main	Summary
		Protect IP
	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
		Drop Statistics
		Real time counters
		Start Packet-Dump
		Stop Packet-Dump
		Packet-Dump List
	Protection	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

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