CHAPTER 17

IronPort M-Series セキュリティ管理アプライアンス

IronPort M-Series アプライアンスは、他の IronPort アプライアンスと組み合わせて使用する、外部または「オフボックス」のスパム検疫として機能することを特に目的とした、IronPort アプライアンスの特別なモデルです。この章では、IronPort M-Series アプライアンスのネットワーク プランニング、システム セットアップ、および一般的な用途を説明します。

この章は、次の内容で構成されています。

概要

IronPort M-Series セキュリティ管理アプライアンスを使用すると、IronPort 電子メール セキュリティ アプライアンスの機能を補完できます。IronPort M-Series セキュリティ管理アプライアンスは、企業のポリシー設定値および監査情報をモニタする外部または「オフボックス」の場所として機能することを目的としています。ハードウェア、オペレーティング システム（AsyncOS）、および補助サービスを組み合わせて重要なポリシーと実行時データの集中化と統合を行うことにより、IronPort C-Series と X-Series の電子メール セキュリティ アプライアンスで使用するレポート情報および監査情報を管理者およびエンドユーザが管理するための単一インターフェイスになります。IronPort M-Series アプライアンスを使用すると、IronPort 電子メール セキュリティ アプライアンスの性能を十分に引き出すことができ、配置の柔軟性を高めることで企業ネットワーク

の整合性が保護されます。セキュリティ運用を単一の IronPort M-Series アプライアンスから行うように調整することも、複数のアプライアンス間で負荷を分散するように調整することもできます。

セキュリティ管理アプライアンスの AsyncOS には次の機能が含まれています。

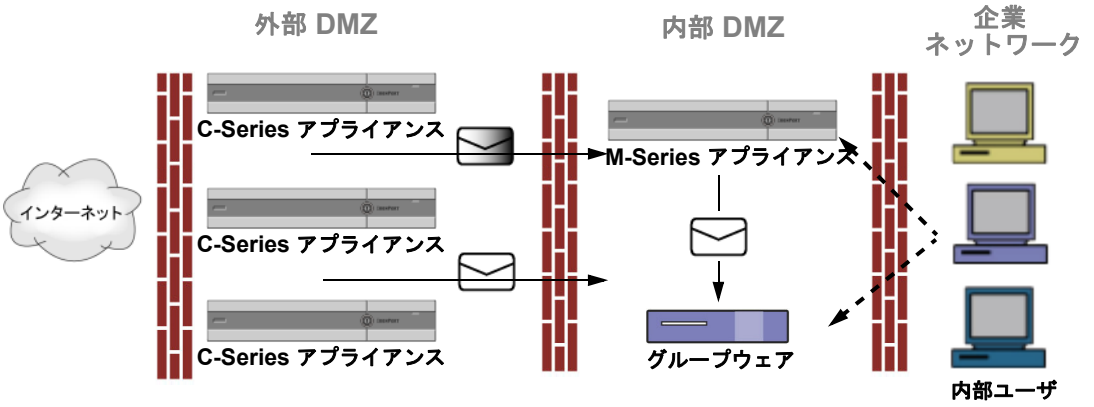
- 外部 IronPort スパム検疫。エンドユーザ向けのスパム メッセージおよび陽性と疑わしいスパム メッセージを保持しており、エンドユーザおよび管理者は、スパムとフラグ付けされたメッセージをレビューしてから最終的な決定を下すことができます。
- 中央集中型レポーティング。複数の電子メール セキュリティ アプライアンスから集約されたデータに対してレポートを実行します。
- 中央集中型トラッキング。複数の電子メール セキュリティ アプライアンスを横断して電子メール メッセージを追跡します。

IronPort セキュリティ管理アプライアンスの設定および使用については、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。

ネットワーク プランニング

IronPort M-Series アプライアンスを使用すると、エンドユーザ インターフェイス（メール アプリケーションなど）を、さまざまな DMZ 内のよりセキュアなゲートウェイ システムから切り離すことができます。2 層ファイアウォールの使用によって、ネットワーク プランニングの柔軟性が高まり、エンドユーザが外部 DMZ に直接接続することを防止できます（図 17-1 を参照）。

図 17-1　IronPort M-Series アプライアンスを含む一般的なネットワーク設定



大規模な企業データ センターでは、外部 IronPort スパム検疫として機能している 1 台の IronPort M-Series アプライアンスを、1 台または複数台の IronPort C-Series または X-Series アプライアンスで共有できます。さらに、ローカル使用のために独自のローカル IronPort アプライアンス検疫を保守するリモート オフィスをセットアップできます（C-Series または X-Series アプライアンス上でローカル IronPort スパム検疫を使用）。

図 17-1 に、IronPort M-Series アプライアンスおよび複数の DMZ を含む、通常のネットワーク設定を示します。インターネットからの着信メールは、外部 DMZ の IronPort アプライアンスによって受信されます。正規のメールは、内部 DMZ の MTA（グループウェア）に従って、最終的に企業ネットワーク内のエンドユーザまで送信されます。

スパムおよび陽性と疑わしいスパム（メール フロー ポリシー設定値に基づく）は、IronPort M-Series アプライアンスのスパム検疫エリアに送信されます。次にエンドユーザが検疫エリアにアクセスして、スパムを削除し、自分宛に配信されるメッセージを解放することを選択できます。IronPort スパム検疫エリアに残っているメッセージは、設定可能な期間の経過後に自動的に削除されます（『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照）。

メール フローおよび IronPort M-Series アプライアンス

メールは、他の IronPort（C-Series および X-Series）アプライアンスから IronPort M-Series アプライアンスに送信されます。IronPort M-Series アプライアンスにメールを送信するように設定された IronPort アプライアンスは、その

M-Series アプライアンスからリリースされるメールの受信を自動的に予測し、このようなメッセージを逆戻りして受信した場合は再処理を行いません。メッセージは、HAT などのポリシーやスキャン設定をバイパスして配信されます。これを機能させるために、IronPort M-Series アプライアンスの IP アドレスが変わらないようにしてください。IronPort M-Series アプライアンスの IP アドレスが変わると、受信側の C-Series または X-Series のアプライアンスは、メッセージを他の着信メッセージであるものとして処理します。IronPort M-Series アプライアンスの受信と配信では、常に同じ IP アドレスを使用する必要があります。

IronPort M-Series アプライアンスでは、IronPort スパム検疫設定で指定されている IP アドレスから検疫対象のメールを受け入れます。IronPort M-Series アプライアンスでローカル検疫を設定するには、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。IronPort M-Series アプライアンスのローカル検疫エリアは、そこにメールを送信する他の IronPort アプライアンスからは、*外部*検疫エリアとして参照されることに注意してください。

IronPort M-Series アプライアンスによって解放されたメールは、スパム検疫設定の定義に従って、プライマリ ホストおよびセカンダリ ホスト（IronPort アプライアンスまたは他のグループウェア ホスト）に配信されます（『*IronPort AsyncOS for Security Management User Guide*』を参照）。したがって、IronPort M-Series アプライアンスにメールを配信する IronPort アプライアンスの数に関係なく、解放されるすべてのメール、通知、およびアラートが単一のホスト（グループウェアまたは IronPort アプライアンス）に送信されます。IronPort M-Series アプライアンスからの配信によってプライマリ ホストが過負荷にならないように注意してください。

モニタリング サービスの設定

中央集中型レポーティングまたは中央集中型トラッキングのためや、外部 IronPort スパム検疫としてセキュリティ管理アプライアンスを使用するには、まず、電子メール セキュリティ アプライアンス上にモニタリング サービスを設定（構成）する必要があります。

電子メール セキュリティ アプライアンス上にモニタリング サービスを設定するときは、セキュリティ管理アプライアンス上でモニタリング サービスをイネーブルにする必要もあります。詳細については、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。

モニタリング サービスは、電子メール トラフィックに関するレポートを実行したり、メッセージ ルーティングを追跡したり、スパムの疑いがあるメッセージおよびスパム メッセージを外部 IronPort スパム検疫エリアに配信したりするために使用します。次の 1 つまたは複数のサービスを設定できます。

- **中央集中型レポーティング。**詳細については、「中央集中型レポーティングを使用するための電子メール セキュリティ アプライアンスの設定」（P.17-567）を参照してください。
- **中央集中型トラッキング。**詳細については、「中央集中型トラッキングを使用するための電子メール セキュリティ アプライアンスの設定」（P.17-569）を参照してください。
- **IronPort スパム検疫。**詳細については、「外部 IronPort スパム検疫を使用するための電子メール セキュリティ アプライアンスの設定」（P.17-570）を参照してください。

中央集中型レポーティングを使用するための電子メール セキュリティ アプライアンスの設定

電子メール セキュリティ アプライアンスに対する中央集中型レポーティングの設定は随時行うことができます。通常は、セキュリティ管理アプライアンスで監視機能をイネーブルにしてから中央集中型レポーティングを設定します。

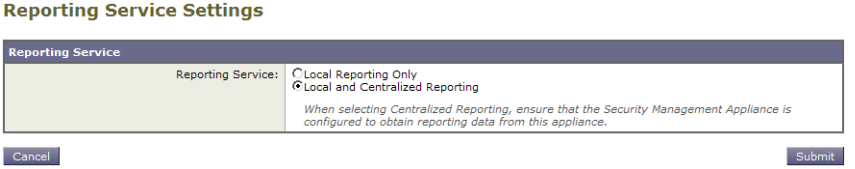
（注） 中央集中型レポーティングをイネーブルにする前に、十分なディスク容量が監視サービスに割り当てられていることを確認してください。

電子メール セキュリティ アプライアンスで中央集中型レポーティングをイネーブルにする手順は、次のとおりです。

ステップ 1　[Security Services] > [Reporting] をクリックします。

[Reporting Service Settings] ページが表示されます。

図 17-2　[Reporting Service Settings] ページ



ステップ 2　[Reporting Service] セクションで [Local and Centralized Reporting] オプションを選択します。

ステップ 3　変更を送信して確定します。

（注）　中央集中型レポーティングを使用するには、電子メール セキュリティ アプライアンスおよびセキュリティ管理アプライアンスで監視機能をイネーブルにする必要があります。セキュリティ管理アプライアンス上での中央集中型レポーティングのイネーブル化については、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。

中央集中型レポーティング モード

中央集中型レポーティングを使用するように電子メール セキュリティ アプライアンスを設定し、管理対象アプライアンスとしてセキュリティ管理アプライアンスに追加すると、電子メール セキュリティ アプライアンスは、中央集中型レポーティング モードで動作するようになります。電子メール セキュリティ アプライアンスが中央集中型レポーティング モードになっている場合、そのアプライアンスのスケジュール済みレポートは中断され、そのアプライアンスのスケジュール済みレポートの設定ページやアーカイブされたレポートを利用できません。また、そのアプライアンスで保存するデータは 1 週間分だけになります。月次レポートおよび年次レポート用の新規データは、セキュリティ管理アプライアンスに保存されます。電子メール セキュリティ アプライアンスにある月次レポート用の既存データは、セキュリティ管理アプライアンスに転送されません。中央集中型レポーティングをディセーブルにすると、電子メール セキュリティ アプライアンスで新規月次レポート データの保存が開始されます。

電子メール セキュリティ アプライアンスで中央集中型レポーティングをディセーブルにすると、スケジュール済みレポートが再開されて、アーカイブされたレポートを利用できるようになります。中央集中型レポーティングをディセーブルにした場合に、電子メール セキュリティ アプライアンスでは、過去の時間および日ごとのデータだけが表示され、過去の週ごとや月ごとのデータは表示されません。これは、一時的な変更です。十分なデータが蓄積されれば、過去の週お

よび月のレポートが表示されます。電子メール セキュリティ アプライアンスを中央集中型レポーティング モードに戻した場合、過去の週のデータはインタラクティブ レポートに表示されます。

中央集中型トラッキングを使用するための電子メール セキュリティ アプライアンスの設定

電子メール セキュリティ アプライアンスは、ローカル（オンボックス）トラッキングまたは中央集中型トラッキングのいずれかを使用するように設定できます。

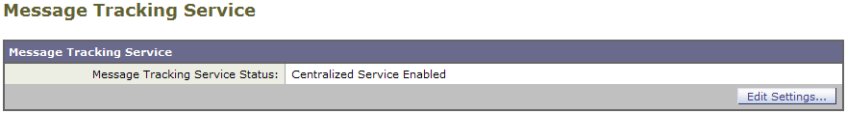
（注） 1 台の電子メール セキュリティ アプライアンスで中央集中型とローカルの両方のトラッキングをイネーブルにはできません。

電子メール セキュリティ アプライアンスで中央集中型トラッキングをイネーブルにする手順は、次のとおりです。

ステップ 1　[Security Services] > [Message Tracking] をクリックします。

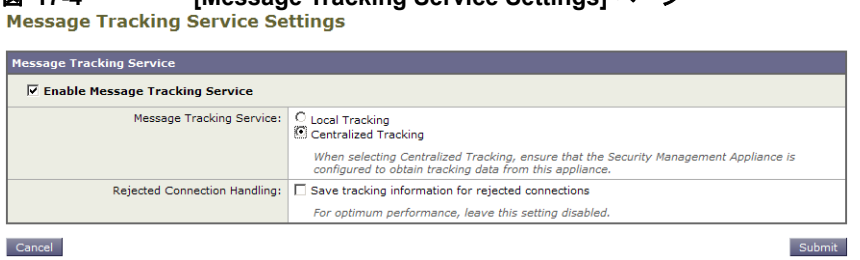
[Message Tracking Service] ページが表示されます。

図 17-3　[Message Tracking Service] ページ



ステップ 2　[Message Tracking Service] セクションで [Edit Settings] をクリックします。

図 17-4　[Message Tracking Service Settings] ページ



ステップ 3　[Enable Message Tracking Service] チェックボックスを選択します。

ステップ 4　[Centralized Tracking] オプションを選択します。

ステップ 5　必要に応じて、拒否された接続の情報を保存するチェックボックスを選択します。

（注）　拒否された接続のトラッキング情報を保存すると、セキュリティ管理アプライアンスのパフォーマンスに悪影響を与えるおそれがあります。

ステップ 6　変更を送信して確定します。

（注）　中央集中型トラッキングを使用するには、電子メール セキュリティ アプライアンスおよびセキュリティ管理アプライアンスで監視機能をイネーブルにする必要があります。セキュリティ管理アプライアンス上での中央集中型トラッキングのイネーブル化については、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。

外部 IronPort スパム検疫を使用するための電子メール セキュリティ アプライアンスの設定

セキュリティ管理アプライアンスを IronPort スパム検疫として使用するには、電子メール セキュリティ アプライアンスで外部スパム検疫機能をイネーブルにする必要があります。外部スパム検疫エリアに接続するために電子メール セキュリティ アプライアンスで使用する、IP アドレスとポート番号を指定する必要もあります。

電子メール セキュリティ アプライアンスでセキュリティ管理アプライアンスを外部 IronPort スパム検疫として使用できるようにする手順は、次のとおりです。

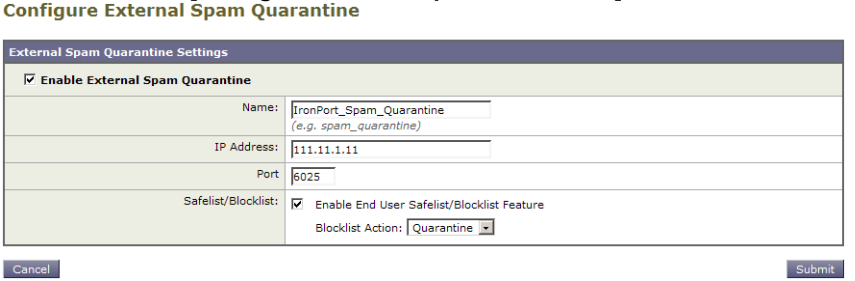
ステップ 1　[Security Services] > [External Spam Quarantine] をクリックします。

[External Spam Quarantine] ページが表示されます。

ステップ 2　[Configure] をクリックします。

[Configure External Spam Quarantine] ページが表示されます。

図 17-5　[Configure External Spam Quarantine] ページ



ステップ 3　[External Spam Quarantine] セクションで、[Enable External Spam Quarantine] チェックボックスを選択します。

ステップ 4　[Name] フィールドにセキュリティ管理アプライアンスの名前を入力します。

ステップ 5　IP アドレスおよびポート番号を入力します。セキュリティ管理アプライアンスの IP アドレスおよびポート番号は、[IronPort Spam Quarantine] ページで設定します。

ステップ 6　必要に応じて、エンドユーザ セーフリスト/ブロックリスト機能をイネーブルにするチェックボックスを選択し、適切なブロックリスト アクションを指定します。

ステップ 7　変更を送信して確定します。

IronPort スパム検疫およびエンドユーザ セーフリスト/ブロックリスト機能の詳細については、『*Cisco IronPort AsyncOS for Email Daily Management Guide*』の「Quarantines」の章を参照してください。M-Series アプライアンスで IronPort スパム検疫を使用する場合の詳細については、『*IronPort AsyncOS for Security Management User Guide*』を参照してください。