電子メールを受信するためのゲートウェイの設定

この章は、次の項で構成されています。

電子メールを受信するためのゲートウェイ設定の概要

Cisco Secure Email Cloud Gateway でリスナーを追加、変更、削除しないことをお勧めします。

電子メールゲートウェイは、組織のゲートウェイとして機能し、電子メール接続の提供、メッセージの受け入れ、それらの適切なシステムへのリレーを行います。電子メールゲートウェイは、インターネットからユーザのネットワーク内の受信者ホストへ、ユーザのネットワーク内のシステムからインターネットに電子メール接続を提供できます。通常、電子メール接続要求は Simple Mail Transfer Protocol（SMTP; シンプル メール転送プロトコル）を使用します。アプライアンスは、SMTP 接続をデフォルトで提供し、SMTP ゲートウェイとして機能し、ネットワークのメール エクスチェンジまたは「MX」とも呼ばれます。

電子メールゲートウェイは、着信 SMTP 接続要求を提供するためにリスナーを使用します。リスナーは、特定の IP インターフェイスで設定される電子メール処理サービスを記述します。リスナーは、インターネットまたはインターネットに到達しようとするユーザのネットワーク内のシステムから、アプライアンスに入る電子メールだけに適用されます。メッセージおよび接続が、メッセージを受け入れて受信者のホストにリレーするために満たす必要のある基準を、リスナーを使用して指定します。リスナーは、指定された各 IP アドレスを特定のポート上で実行する「SMTP デーモン」として見なすことができます。また、リスナーは電子メールゲートウェイが電子メールゲートウェイにメールを送信しようとするシステムと通信する方法を定義します。

次のタイプのリスナーを作成できます。

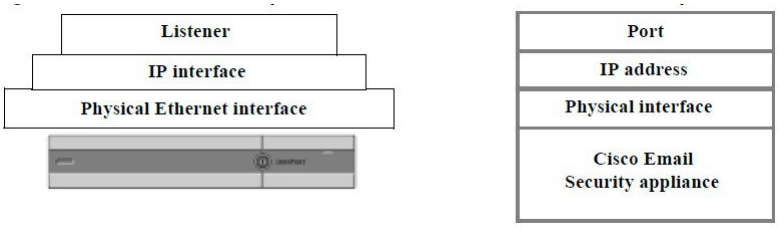
- **[パブリック（Public）]。**インターネットから着信するメール メッセージをリッスンし、受け入れます。パブリック リスナーは多数のホストからの接続を受信し、限られた数の受信者にメッセージを渡します。
- **[プライベート（Private）]。**ユーザのネットワーク内のシステムから（インターネット中でネットワークの外にいる受信者ではなく、通常内部グループウェアおよび電子メール サーバ（POP/IMAP）から）、電子メール メッセージをリッスンし、受け入れます。プライベート リスナーは、限られた（既知の）数のホストからの接続を受信し、多数の受信者にメッセージを渡します。

リスナーを作成するときは、次の情報も指定します。

- **リスナーのプロパティ。**すべてのリスナーに適用するグローバル プロパティおよび各リスナーに固有のプロパティを定義します。たとえば、リスナーに使用する IP インターフェイスおよびポート、そしてこれがパブリックまたはプライベートのリスナーのどちらかを指定することができます。この方法の詳細については、リスナーの使用 （3 ページ）を参照してください。
- **リスナーに接続が許可されているのはどのホストか。**リモート ホストからの着信接続を制御するルールを定義します。たとえば、リモート ホストを定義し、リスナーに接続できるかどうかを定義できます。この方法の詳細については、ホスト アクセス テーブルを使用した接続を許可するホストの定義を参照してください。
- **（パブリック リスナーのみ）リスナーがメッセージを受け入れるローカル ドメイン。**どの受信者がパブリック リスナーによって許可されるかを定義します。たとえば、組織で `currentcompany.com` ドメインを使用しているが、以前は `oldcompany.com` ドメインを使用していた場合は、currentcompany.com と `oldcompany.com` の両方のメッセージを受け入れることができます。この方法の詳細については、ドメイン名または受信者アドレスに基づく接続の許可または拒否を参照してください。

ホストアクセステーブルおよび受信者アクセステーブルを含むリスナーでの設定は、リスナーがSMTPカンバセーション中にSMTPサーバと通信する方法に影響します。これによって、接続が閉じる前に電子メールゲートウェイがスパムを送信するホストをブロックできます。

図 *1:* リスナー、*IP* インターフェイス、物理イーサネット インターフェイスの関係



リスナーの使用

GUI の [ネットワーク（Network）] > [リスナー（Listeners）] ページまたは CLI の listenerconfig コマンドを使用してリスナーを設定します。

すべてのリスナーに適用されるグローバル設定を定義できます。詳細については、リスナーのグローバル設定 （5 ページ）を参照してください。

電子メールゲートウェイでリスナーを使用および設定する場合は、次のルールとガイドラインに留意してください。

- 設定済みの IP インターフェイスごとに複数のリスナーを定義できますが、各リスナーは異なるポートを使用する必要があります。
- デフォルトでは、リスナーは電子メール接続を提供するためのメール プロトコルとして SMTP を使用します。ただし、Quick Mail Queuing Protocol（QMQP）を使用して電子メール接続を提供するようにアプライアンスを設定することもできます。これを行うには、`listenerconfig` CLI コマンドを使用します。
- リスナーは、インターネットプロトコルバージョン4（IPv4）およびバージョン6（IPv6）アドレスの両方をサポートします。単一のリスナーでどちらかのプロトコルバージョンまたは両方を使用できます。リスナーは、接続ホストとしてメール配信に同じプロトコルバージョンを使用します。たとえば、リスナーが IPv4 と IPv6 の両方に設定され、IPv6 を使用してホストに接続する場合、リスナーは IPv6 を使用します。ただし、リスナーが IPv6 アドレスのみの使用を設定されている場合は、IPv4 アドレスのみを使用するホストに接続できません。
- 少なくとも 1 つのリスナー（デフォルト値）がシステム セットアップ ウィザードの実行後に 電子メールゲートウェイ上に設定されます。ただし、リスナーを手動で作成する場合、AsyncOS ではこれらのデフォルト IP レピュテーションスコア値は使用されません。
- **C170 および C190** アプライアンス：システム セットアップ ウィザードでは、デフォルトで、インターネットからの電子メールの受信と内部ネットワークからの電子メールの中継の両方を行うための、1 つのパブリック リスナーを順を追って設定します。つまり、1 つのリスナーで両方の機能を実行できます。
- 電子メールゲートウェイのテストおよびトラブルシューティングに利用するために、パブリックまたはプライベートリスナーの代わりに、「シンクホール」タイプのリスナーを作成できます。シンクホールリスナーの作成時に、メッセージを削除する前にそのメッセージをディスクに書き込むかどうかを選択します。（詳細については、「テストとトラブルシューティング」の章を参照してください。）メッセージを削除する前にディスクに書き込むと、受信レートおよびキューの速度の測定に役立ちます。メッセージをディスクに書き込まないリスナーは、メッセージ生成システムからの純粋な受信レートの測定に役立ちます。このリスナーのタイプは、CLI の `listenerconfig` コマンドを使用した場合にだけ利用できます。

図：3つ以上のイーサネットインターフェイスを持つ電子メールゲートウェイモデル上のパブリックおよびプライベートリスナーは、3つ以上のイーサネットインターフェイスを持つ電子メールゲートウェイモデル上でシステム セットアップ ウィザードによって作成される、標準的な電子メールゲートウェイ構成を示しています。2 つのリスナーが作成されます。あるイン

ターフェイス上でインバウンド接続を使用可能にするためのパブリック リスナーと、別の IP インターフェイス上でアウトバウンド接続を使用可能にするためのプライベート リスナーです。

図：2 つだけイーサネット インターフェイスを持つ 電子メールゲートウェイモデル上のパブリックリスナーは、イーサネット インターフェイスが 2 つだけの 電子メールゲートウェイモデル上でシステム セットアップ ウィザードによって作成される、標準的な電子メールゲートウェイ構成を示しています。インバウンド接続およびアウトバウンド接続の両方を提供するために、単一の IP インターフェイスで 1 つのリスナーが作成されます。

図 *2：3* つ以上のイーサネット インターフェイスを持つ電子メールゲートウェイモデル上のパブリックおよびプライベートリスナー

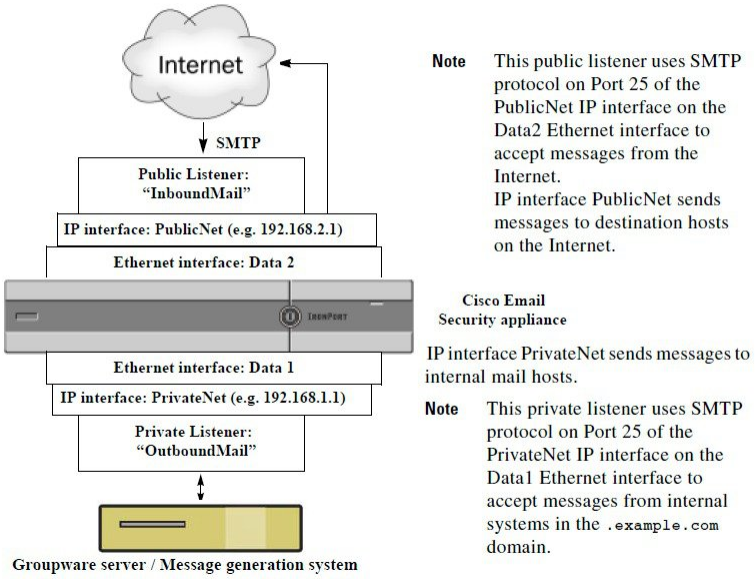
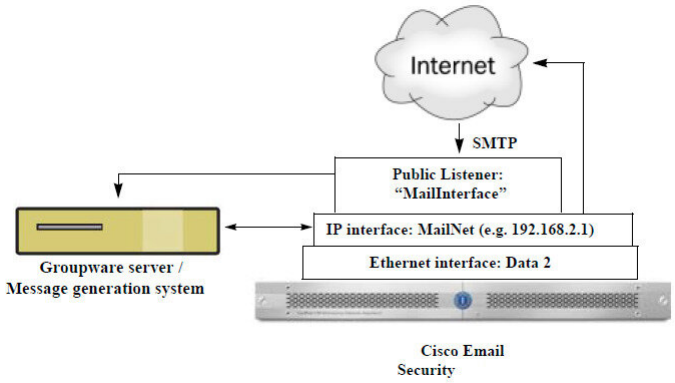


図 *3：2* つだけイーサネット インターフェイスを持つ電子メールゲートウェイモデル上のパブリックリスナー



（注） このパブリック リスナーは、イーサネット インターフェイス Data2 上の IP インターフェイス PublicNet のポート 25 上で SMTP プロトコルを使用し、インターネットからのメッセージを受信し、.example.com ドメイン内の内部システムからのメッセージを中継します。IP インターフェイス MailNet は、インターネット上の宛先ホストと内部のメール ホストにメッセージを送信します。

リスナーのグローバル設定

リスナーのグローバル設定は、電子メールゲートウェイで設定されたすべてのリスナーに影響します。リスナーが、インターネット プロトコル バージョン 4（IPv4）およびバージョン 6（IPv6）アドレスの両方を持つインターフェイスを使用する場合、リスナーの設定は IPv4 および IPv6 トラフィックの両方に適用されます

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listeners）] を選択します。

ステップ 2 **[グローバル設定を編集（Edit Global Settings）]** をクリックします。

ステップ 3 次の表に定義された設定を変更します。

表 *1*: リスナーのグローバル設定

グローバル設定	説明
最大同時接続数（Maximum Concurrent Connections）	リスナーに同時に接続できる最大数を設定します。C3x0 および C6x0 モデルのデフォルト値は 300 で、C1x0 モデルのデフォルト値は 50 です。リスナーが IPv4 と IPv6 の両方の接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 300 の場合、IPv4 および IPv6 接続の最大同時接続数が合計 300 を超えることはできません。
最大 TLS 同時接続数（Maximum Concurrent TLS Connections）	すべてのリスナーでの同時 TLS 接続の最大数を設定します。デフォルト値は 100 です。リスナーが IPv4 と IPv6 の両方の TLS 接続を受け入れる場合、接続数は 2 つの間で分配されます。たとえば最大同時接続数が 100 の場合、IPv4 および IPv6 の TLS 接続の最大同時接続数が合計 100 を超えることはできません。

グローバル設定	説明
受信カウンタリセット時間（Injection Counters Reset Period）	インジェクション制御カウンタがリセットされた場合に調整できます。多数の IP アドレスのカウンタを管理している非常にビジーなシステムの場合、カウンタをより頻繁に（たとえば、60 分間隔ではなく 15 分間隔で）リセットするように設定します。これにより、データが管理不能なサイズにまで増大したり、システムのパフォーマンスに影響を与えたりすることを回避できます。 現在のデフォルト値は 1 時間です。最小 1 分（60 秒）から最大 4 時間（14,400 秒）までの期間を指定できます。 インジェクション制御期間を参照してください。
受信接続のタイムアウトまでの待ち時間（Timeout Period for Unsuccessful Inbound Connections）	AsyncOS が失敗した着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 失敗した接続は SMTP カンバセーションとなり、正常なメッセージ インジェクションが発生することなく、SMTP コマンドまたは ESMTP コマンドが発行され続けます。指定したタイムアウトに達した場合は、次のエラーが送信され、接続が解除されます。 「421 Timed out waiting for successful message injection, disconnecting.」 正常なメッセージ インジェクションが発生するまで、接続に失敗したと見なされます。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 5 分です。
すべてのインバウンド接続の合計時間制限（Total Time Limit for All Inbound Connections）	AsyncOS が着信接続が閉じられるまでそのままの状態にする有効期間を設定します。 この設定は、最大許容接続時間を適用することにより、システム リソースを保持するためのものです。この最大接続時間の約 80% が経過すると、次のメッセージが表示されます。 「421 Exceeded allowable connection time, disconnecting.」 電子メールゲートウェイは、接続が最大接続時間の 80% を超えると、接続がメッセージの途中で切断されることを防ぐために接続を切断しようとします。着信接続を最大接続時間の 80% に到達する期間開いている場合、発生する可能性がある問題です。時間制限を指定する場合、このしきい値に注意してください。 パブリック リスナーの SMTP 接続にのみ使用できます。デフォルト値は 15 分です。
件名の最大サイズ（Maximum size of subject）	件名のサイズが指定された制限内であるメッセージが承認され、その他のメッセージは拒否されます。この値を 0 に設定すると、制限は適用されません。

グローバル設定	説明
HAT 遅延拒否（HAT delayed rejections）	メッセージ受信者レベルでHAT拒否を実行するかどうかを設定します。デフォルトでは、HATによって拒否された接続はSMTPカンバセーションの開始時にバナー メッセージをともなって終了されます。 HAT「拒否」設定で電子メールが拒否されると、AsyncOS では SMTP カンバセーションの開始時ではなく、メッセージ受信者レベル（RCPT TO）で拒否を実行できます。この方法でメッセージを拒否することで、メッセージの拒否が遅延されメッセージがバウンスするため、AsyncOS は拒否されたメッセージに関するより詳細な情報を取得できます。たとえば、ブロックされたメッセージのアドレスおよび各受信者のアドレスからメールを表示できます。また、HAT 拒否の遅延によって、送信側 MTA が何度も再試行される可能性も小さくなります。 HAT 遅延拒否をイネーブルにすると、次の動作が発生します。 MAIL FROM コマンドが許可されるが、メッセージオブジェクトは作成されない。 電子メールの送信のためのアクセスが拒否されたというメッセージが表示され、すべての RCPT TO コマンドが拒否される。 SMTP AUTH を使用して送信側 MTA が認証される場合、RELAY ポリシーが許可され、メールを通常どおりに送信できる。 CLI の `listenerconfig --> setup` コマンドからのみ設定できます。

ステップ 4 変更を送信し、保存します。

次のタスク

関連項目

- 複数のエンコーディングが含まれるメッセージの設定 （7 ページ）

複数のエンコーディングが含まれるメッセージの設定

次のパラメータのメッセージのエンコード方式を変更する際の、電子メールゲートウェイの動作を定義できます。

- ヘッダー
- タグなしの ASCII 以外のヘッダー
- フッターまたはヘッダーのエンコード方式の不一致

この動作を設定するには、CLI で localeconfig コマンドを使用します。

（注） Web インターフェイスを使用してこの動作を設定することはできません。

CLI トランスクリプトのサンプルについては、免責事項スタンプと複数エンコード方式を参照してください。

Web インターフェイスを使用してリスナーを作成することによる接続要求のリスニング

手順

ステップ 1 [ネットワーク（Network）] > [リスナー（Listener）] を選択します。

ステップ 2 [リスナーを追加（Add Listener）] をクリックします。

ステップ 3 次の表に定義されている設定を設定します。

表 *2:* リスナー設定

名前	リスナーには、簡単に参照できるように一意の名前を付けてください。リスナー用に定義する名前では、大文字と小文字が区別されます。AsyncOS では、複数のリスナーに同一の名前を付けることはできません。
リスナーのタイプ（Type of Listener）	次のリスナー タイプのいずれかを選択します。 • **[パブリック（Public）]。**パブリック リスナーには、インターネットから電子メールを受信するためのデフォルト特性が含まれます。 • **[プライベート（Private）]。**プライベート リスナーは、プライベート（内部）ネットワークで使用することを目的としています。
インターフェイス（Interface）	リスナーを作成する設定済み電子メールゲートウェイの IP インターフェイスおよび TCP ポートを選択します。インターフェイスで使用する IP アドレスのバージョンによって、リスナーは IPv4 アドレス、IPv6 アドレス、または両方のバージョンからの接続を受け入れます。デフォルトでは、SMTP ではポート 25 を使用し、QMQP ではポート 628 を使用します。
バウンス プロファイル	バウンス プロファイルを選択します（CLI の `bounceconfig` コマンドを使用して作成されたバウンス プロファイルをリストから選択できます。新しいバウンス プロファイルの作成を参照）。
上記の免責条項（Disclaimer Above）	電子メールの上または下に添付する免責条項を選択します（[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページまたは CLI の `textconfig` コマンドで作成された文章をリストから選択できます。「テキスト リソース」の章を参照）。

下記の免責条項（Disclaimer Below）	電子メールの上または下に添付する免責条項を選択します（[メールポリシー（Mail Policies）] > [テキストリソース（Text Resources）] ページまたは CLI の `textconfig` コマンドで作成された文章をリストから選択できます。「テキスト リソース」の章を参照）。
SMTP 認証プロファイル（SMTP Authentication Profile）	SMTP 認証プロファイルを指定します。
証明書	リスナーへの TLS 接続のための証明書を指定します（[ネットワーク（Network）] > [証明書（Certificates）] ページまたは CLI の `certconfig` コマンドで追加された証明書をリストから選択できます。他の MTA との暗号化通信の概要を参照）。

ステップ 4 （任意）次の表で定義される SMTP「`MAIL FROM`」および「`RCPT TO`」コマンドでの解析の制御の設定を行います。

設定	説明
アドレス パーサー タイプ（Address Parser Type）	次のパーサータイプのいずれかを使用して、 電子メールゲートウェイが RFC2821 規格にどの程度厳密に準拠するかを選択します。 **Strict モード**： • Strict モードは RFC 2821 に準拠します。Strict モードでは、アドレス解析が RFC 2821 の規格に準拠しますが、次の例外および追加機能があります。 • 「MAIL FROM：<joe@example.com>」のように、コロンの後にスペースを挿入できます。 • ドメイン名に下線を使用できます。 • 「MAIL FROM」コマンドおよび「RCPT TO」コマンドでは、大文字と小文字が区別されます。 • ピリオドは特殊な用途に使用できません（たとえば、RFC 2821 では「J.D.」のようなユーザ名を作成できません）。 以下の追加オプションの一部は、イネーブルにできますが、そうすると、RFC 2821 に技術的に違反します。 **Loose モード**： Loose 解析は基本的に AsyncOS の以前のバージョンからの既存の動作です。電子メール アドレスの「検索」を最優先し、次のことを行います。 • コメントの無視。ネストされたコメント（カッコで囲まれている）がサポートされ、それらは無視されます。 • 「RCPT TO」コマンドおよび「MAIL FROM」コマンドで指定された電子メール アドレスの前後には山カッコが不要です。 • 複数のネストされた山カッコを使用できます（最も深いネスト レベルの電子メール アドレスが検索される）。
8 ビットユーザ名を許可（Allow 8-bit User Names）	イネーブルにすると、（エスケープ処理なしで）アドレスのユーザ名部分に 8 ビットの文字を使用できます。
8 ビットドメイン名を許可（Allow 8-bit Domain Names）	イネーブルにすると、アドレスのドメイン部分に 8 ビットの文字を使用できます。

設定	説明
部分ドメインを許可（Allow Partial Domains）	イネーブルにすると、部分ドメインを使用できます。部分ドメインは完全なドメインではなく、ドットなしのドメインです。 次のアドレスは、部分ドメインの例です。 • foo • foo@ • foo@bar デフォルトのドメイン機能を正常に動作させるために、このオプションをイネーブルにする必要があります。 [デフォルトドメインを追加（Add Default Domain）]：完全修飾ドメイン名ではなく、デフォルトのドメインを電子メール アドレスに使用します。[SMTPアドレス解析オプション（SMTP Address Parsing options）] で [部分ドメインを許可（Allow Partial Domains）] がイネーブルになっていない限り、このオプションはディセーブルです。これは「デフォルト送信者ドメイン」を送信者のアドレスおよび完全修飾ドメイン名を含まない受信者のアドレスに追加することによって、リスナーがリレーする電子メールを変更する方法に影響します（言い換えると、リスナーの「そのままの」アドレスの処理方法をカスタマイズできます）。 従来のシステムで、送信者アドレスに企業のドメインを追加（付加）せずに電子メールを送信する場合、これを使用してデフォルトの送信者ドメインを追加できます。たとえば、従来のシステムでは電子メールの送信者として自動的に文字列「joe」のみが入力された電子メールが作成されます。デフォルトの送信者ドメインを変更すると、「@yourdomain.com」が「joe」に付加され、完全修飾送信者名 joe@yourdomain.com が作成されます。
ソース ルーティング（Source Routing）	「MAIL FROM」アドレスおよび「RCPT TO」アドレスで送信元ルーティングが検出された場合の動作を決定します。送信元ルーティングは、複数の「@」文字を使用してルーティングを指定する、電子メール アドレスの特殊な形式です（例：@one.dom@two.dom:joe@three.dom）。「reject」を設定すると、アドレスは拒否されます。「strip」を設定すると、アドレスの送信元ルーティング部分が削除され、メッセージが通常どおり挿入されます。

設定	説明
不明なアドレス文字（Unknown Address Literals）	システムで処理できないアドレス リテラルを受信したときの動作を決定します。現在は、IPv4 以外のすべてです。そのため、たとえばIPv6 アドレス リテラルの場合、プロトコル レベルで拒否するか、受信後すぐにハードバウンスを行うことができます。 リテラルが含まれる受信者アドレスは即時ハード バウンスの原因となります。送信者アドレスは配信される場合があります。メッセージを配信できない場合、ハードバウンスがハードバウンスされます（二重ハードバウンス）。 拒否された場合、送信者と受信者のアドレスがプロトコル レベルですぐに拒否されます。
ユーザ名で次の文字を拒否（Reject These Characters in User Names）	文字（たとえば、% や !）を含むユーザ名を入力すると、拒否されます。

ステップ 5 （任意）次の表に定義されているリスナーの動作をカスタマイズするための高度な設定を設定します。

設定	説明
最大同時接続数（Maximum Concurrent Connections）	許可される最大接続数。
TCPリッスン用キューサイズ（TCP Listen Queue Size）	SMTP サーバが受け入れる前に AsyncOS で管理される接続のバックログ。
CR と LF の取り扱い（CR and LF Handling）	そのままの CR（復帰）文字および LF（改行）文字を含むメッセージの処理方法を選択します。 • **[正常（Clean）]**。メッセージを許可しますが、そのままの CR 文字および LF 文字を CRLF 文字に変換します。 • **[拒否（Reject）]**。メッセージを拒否します。 • **[許可（Allow）]**。メッセージを許可します。

設定	説明
Receivedヘッダーを追加（Add Received Header）	すべての受信メールにReceived:ヘッダーを追加します。また、リスナーは各メッセージにReceived:ヘッダーを追加してリレーする電子メールを変更します。Received:ヘッダーが含まれないようにするには、このオプションを使用してディセーブルにします。 （注） Received:ヘッダーは、ワーク キューの処理ではメッセージに追加されません。このヘッダーは配信のためにメッセージがキューから出たときに追加されます Received:ヘッダーをディセーブルにすると、インフラストラクチャの外部に送信されるすべてのメッセージで内部サーバのIPアドレスまたはホスト名が表示されることによって、ネットワークのトポロジが公開されないようにすることができます。Received:ヘッダーをディセーブルにする際には注意が必要です。
SenderBase IPプロファイルを使用（Use SenderBase IP Profiling）	[SenderBase IPプロファイルを使用（SenderBase IP Profiling）] をイネーブルにするかどうかを選択し、次のように設定を行います。 • **[接続ごとのSenderBaseタイムアウト（SenderBase Timeout per Connection）]**。SMTP接続ごとのSenderBase情報をアプライアンスがどのくらいの期間キャッシュするかを定義します。

ステップ6 （任意）次の表に定義されているこのリスナーに関連付けられたLDAPクエリーを制御する設定を行います。

リスナーのLDAPクエリーをイネーブルにするには、次の設定を使用します。このオプションを使用する前に、LDAPクエリーを作成しておく必要があります。クエリーの各タイプには、設定するための個別のサブセクションがあります。クエリーのタイプをクリックしてサブセクションを展開します。

LDAP クエリー作成の詳細については、LDAP クエリを参照してください。

クエリーのタイプ	説明
アクセプト クエリ	アクセプト クエリの場合は、使用するクエリをリストから選択します。LDAP アクセプトをワーク キューの処理中に実行するか、SMTP カンバセーションで実行するかを指定できます。 ワーク キューの処理中に LDAP アクセプトを実行する場合、一致しない受信者に対する動作として、バウンスまたはドロップに指定します。 SMTP カンバセーションで LDAP アクセプトを実行する場合、LDAP サーバに到達できない場合にメールを処理する方法を指定します。メッセージを許可するか、コードとカスタム応答で接続をドロップするかを選択できます。最後に、SMTP カンバセーションで Directory Harvest Attack Prevention（DHAP;ディレクトリ獲得攻撃防止）のしきい値に達した場合に接続をドロップするかどうかを選択します。 SMTP カンバセーションで受信者の検証を行うと、複数の LDAP クエリー間の遅延を低減できます。したがって、対話形式の LDAP アクセプトをイネーブルにした場合、ディレクトリ サーバの負荷が増大することに注意してください。 詳細については、LDAP クエリの概要を参照してください。
ルーティング クエリ	ルーティング クエリーの場合は、リストからクエリーを選択します。詳細については、LDAP クエリの概要を参照してください。
クエリのマスカレード	マスカレード クエリーの場合は、リストからクエリーを選択して、From または CC ヘッダー アドレスといった、マスカレードするアドレスを選択します。 詳細については、LDAP クエリの概要を参照してください。
グループ クエリ	グループ クエリーの場合は、リストからクエリーを選択します。詳細については、LDAP クエリの概要を参照してください。

ステップ 7 変更を送信し、保存します。

次のタスク

関連項目

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM （15 ページ）

部分ドメイン、デフォルト ドメイン、不正な形式の MAIL FROM

エンベロープ送信者検証をイネーブルにした場合、またはリスナーのSMTPアドレス解析オプションで部分ドメインの許可をディセーブルにした場合、リスナーのデフォルトドメイン設定が使用されなくなります。

これらの機能は互いに排他的です。

CLIを使用してリスナーを作成することによる接続要求のリスニング

次の表に、リスナーの作成および編集に関連するタスクに使用するlistenerconfigサブコマンドの一部を示します。

表 *3:* リスナーを作成するタスク

リスナーを作成するタスク	コマンドおよびサブコマンド
新しいリスナーの作成	`listenerconfig -> new`
リスナーのグローバル設定の編集	`listenerconfig -> setup`
リスナーのバウンス プロファイルの指定	`bounceconfig, listenerconfig-> edit -> bounceconfig`
リスナーへの免責条項の関連付け	`textconfig, listenerconfig -> edit -> setup -> footer`
SMTP 認証の設定	`smtpauthconfig, listenerconfig -> smtpauth`
SMTP アドレス解析の設定	`textconfig, listenerconfig -> edit -> setup -> address`
リスナーのデフォルト ドメインの設定	`listenerconfig -> edit -> setup -> defaultdomain`
Received: ヘッダーの電子メールへの追加	`listenerconfig -> edit -> setup -> received`
そのままの CR および LF 文字の CRLF への変更	`listenerconfig -> edit -> setup -> cleansmtp`
ホスト アクセス テーブルの修正	`listenerconfig -> edit -> hostaccess`
ローカル ドメインまたは特定のユーザ（RAT）への電子メールの受け入れ（パブリック リスナーのみ）	`listenerconfig -> edit -> rcptaccess`

リスナーを作成するタスク	コマンドおよびサブコマンド
リスナーの暗号化カンバセーション（TLS）	`certconfig, listenerconfig -> edit`
証明書の選択（TLS）	`listenerconfig -> edit -> certificate`

listenerconfig コマンドの詳細については、『CLI Reference Guide for AsyncOS for Cisco Secure Email Gateway』を参照してください。

電子メールのルーティングおよび配信設定の詳細については、ルーティングおよび配信機能の設定を参照してください。

関連項目

HAT の詳細パラメータ （16 ページ）

HAT の詳細パラメータ

次の表では、HAT 詳細パラメータの構文を定義しています。以下の数値については、後ろに **k** を追加してキロバイトを表すか、後ろに **M** を追加してメガバイトを表すことができます。文字のない値はバイトと見なされます。アスタリスクが付いたパラメータは、次の表に示す変数構文をサポートしています。

表 *4 : HAT* 詳細パラメータの構文

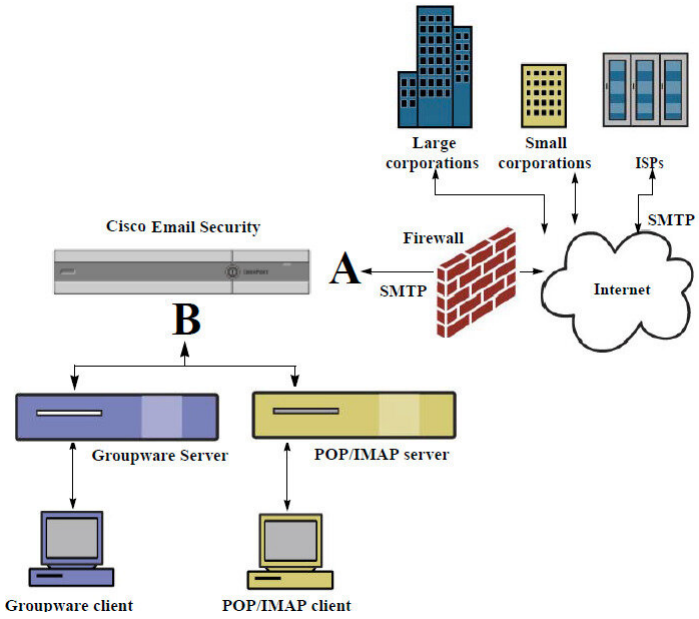
パラメータ	構文	値	値の例
接続あたりの最大メッセージ数	`max_msgs_per_session`	番号	`1000`
メッセージあたりの最大受信者数	`max_rcpts_per_msg`	番号	`10000` `1k`
最大メッセージ サイズ	`max_message_size`	番号	`1048576` `20M`
このリスナーに許可された最大同時接続数	`max_concurrency`	番号	`1000`
SMTP バナー コード	`smtp_banner_code`	番号	`220`
SMTP バナー テキスト（*）	`smtp_banner_text`	文字列	`Accepted`
SMTP 拒否バナー コード	`smtp_banner_code`	番号	`550`

パラメータ	構文	値	値の例
SMTP 拒否バナー テキスト（*）	`smtp_banner_text`	文字列	`Rejected`
SMTPバナーホスト名を上書き	`use_override_hostname`	on | off | default	`default`
	`override_hostname`	文字列	`newhostname`
TLS を使用	`tls`	on | off | required	`on`
スパム対策スキャンの使用	`spam_check`	on | off	`off`
ウイルス スキャンの使用	`virus_check`	on | off	`off`
1時間あたりの最大受信者数	`max_rcpts_per_hour`	番号	`5k`
1時間あたりのエラーコードの最大受信者数	`max_rcpts_per_hour_code`	番号	`452`
1時間あたりのテキストの最大受信者数（*）	`max_rcpts_per_hour_text`	文字列	`Too manyrecipients`
SenderBase の使用	`use_sb`	on | off	`on`
IP レピュテーションスコアの定義	`sbrs[`*`value1`*`:`*`value2`*`]`	-10.0 ～ 10.0	`sbrs[-10:-7.5]`
ディレクトリ獲得攻撃防止：1時間あたりの最大無効受信大数	`dhap_limit`	番号	`150`

エンタープライズ ゲートウェイ構成

この設定では、エンタープライズ ゲートウェイの設定はインターネットからメールを受け取り、グループウェア サーバ、POP/IMAP サーバまたは他の MTA に電子メールをリレーします。エンタープライズ ゲートウェイは、それと同時に、グループウェア サーバおよびその他の電子メール サーバからの SMTP メッセージを受け付け、インターネット上の受信者に中継します。

図 *4:* エンタープライズ ゲートウェイのパブリック リスナーとプライベート リスナー



この設定では、少なくとも 2 つのリスナーが必要です。

- インターネットからのメールだけを受け入れるように設定されたリスナー 1 つ
- 内部グループウェアおよび電子メール サーバ（POP/IMAP）からのメールだけを受け入れるように設定されたリスナー 1 つ

異なるパブリック ネットワークとプライベート ネットワーク用に個別のパブリック リスナーとプライベート リスナーを作成することで、セキュリティ、ポリシー強制、レポーティング、管理用に電子メールを区別できます。たとえば、パブリック リスナーで受信した電子メールは、設定されたスパム対策エンジンおよびウイルス対策スキャンエンジンによってデフォルトでスキャンされますが、プライベート リスナーで受信される電子メールはスキャンされません。

図：エンタープライズ ゲートウェイのパブリックリスナーとプライベートリスナーは、このエンタープライズ ゲートウェイ構成の電子メールゲートウェイで構成されている 1 つのパブリック リスナー（A）と 1 つのプライベートリスナー（B）を示しています。