テストとトラブルシューティング

この章は、次の項で構成されています。

テストメッセージを使用したメールフローのデバッグ：トレース

[システム管理（System Administration）]>[トレース（Trace）]ページを使用して（CLI の trace コマンドと同等）、テストメッセージの送信をエミュレートすることにより、システムを介したメッセージ フローをデバッグできます。[トレース（Trace）]ページ（および **trace** CLI コマンド）では、リスナーに受け入れられているようにメッセージをエミュレートし、現在のシステム設定（コミットしていない変更を含む）によって「トリガー」される、または影響を受ける機能の概要を出力できます。テスト メッセージは実際には送信されません。特に、Cisco アプライアンスで使用できる多数の高度な機能を組み合わせると、[トレース（Trace）]ページ（および **trace** CLI コマンド）は、強力なトラブルシューティングまたはデバッグ ツールとなります。

（注） トレースは、ファイル レピュテーション スキャンのテストには効果がありません。

[トレース（Trace）] ページ（および **trace** CLI コマンド）では、次の表に示されている入力パラメータのプロンプトが表示されますテーブル。

表 *1 : [*トレース（*Trace***）*]* ページに対する入力**

値	説明	例
ソース IP アドレス	リモートドメインの送信元を模倣するため、リモート クライアントの IP アドレスを入力します。これは、インターネット プロトコル バージョン 4（IPv4）またはバージョン 6（IPv6）アドレスを指定できます。 注：trace コマンドを実行すると、IP アドレスと完全修飾ドメイン名の入力が求められます。完全修飾ドメイン名が一致するかどうかを確認するための IP アドレスの逆引きは行われません。trace コマンドでは、完全修飾ドメイン名フィールドを空白にすることはできないため、DNS が一致を正しく逆引きしないシナリオはテストできません。	**203.45.98.109** **2001:0db8:85a3::8a2e:0370:7334**
ソース IP アドレスの完全修飾ドメイン名	模倣する完全修飾リモートドメイン名を入力します。ヌルのままにすると、送信元 IP アドレスに対してリバース DNS ルックアップが実行されます。	**smtp.example.com**
次の動作をトレースするリスナー	テストメッセージの送信をエミュレートするため、システムに設定されているリスナーのリストから選択します。	**InboundMail**
ネットワーク所有者の組織 ID	SenderBase ネットワーク オーナーに固有の ID 番号を入力するか、送信元 IP アドレスに関連付けられたネットワーク オーナー ID の検索を指示します。GUI を介して送信者グループにネットワーク オーナーを追加した場合は、この情報を表示できます。	**34**

値	説明	例
SenderBase レピュテーション スコア（SBRS スコア）	スプーフィング ドメインに与える SBRS スコアを入力するか、送信元IPアドレスに関連付けられた SBRS スコアの検索を指示します。このパラメータは、SBRS スコアを使用するポリシーをテストするときに役立ちます。手動で入力したSBRS スコアは、Context Adaptive Scanning Engine（CASE）に渡されないことに注意してください。詳細については、リスナーの送信者レピュテーション フィルタリング スコアのしきい値の編集を参照してください。	**-7.5**
エンベロープ送信者（Envelope Sender）	テストメッセージのエンベロープ送信者を入力します。	**admin@example.net**
エンベロープ受信者	テストメッセージの受信者のリストを入力します。複数のエントリを指定する場合は、カンマで区切ります。	**joe** **frank@example.com**
メッセージ本文	ヘッダーを含む、テスト メッセージのメッセージ本文を入力します。メッセージ本文の入力を終了するには、別の行にピリオドを入力します。「ヘッダー」は、メッセージ本文の一部とみなされるため（空白行により分割されます）、ヘッダーを省略したり、不十分な形式が含まれると、予期しないトレース結果となる可能性がある点に注意してください。	**To: 1@example.com** From: ralph Subject: Test **this is a test message** 。

値を入力したら、[トレースを開始（Start Trace）] をクリックします。メッセージに影響する、システムに設定されたすべての機能の概要が出力されます。

メッセージ本文は、ローカル ファイル システムからアップロードできます（CLI では、**/configuration** ディレクトリにアップロードしたメッセージ本文を使用してテストできます。Cisco アプライアンスにインポートするためにファイルを配置する方法の詳細については、FTP、SSH、および SCP アクセスを参照してください）。

概要が出力されると、生成されたメッセージの確認とテストメッセージの再実行を求められます。別のテスト メッセージを入力すると、[トレース（Trace）] ページおよび trace コマンドでは、以前に入力した前掲の表の値が使用されます。

（注） 次の表に示す、traceコマンドによってテストされる設定の各セクションは、順番どおりに実行されます。この順番は、ある機能の設定が他の機能にどのように影響するかを理解するうえで非常に役立ちます。たとえば、ドメイン マップ機能によって変換される受信者アドレスは、RAT によって評価されるアドレスに影響します。また、RAT の影響を受ける受信者は、エイリアス テーブルによって評価されるアドレスに影響する、というようになります。

表 *2:* トレースを実行したときの出力の表示

trace コマンド セクション	**出力**
ホスト アクセス テーブル（HAT）およびメール フロー ポリシーの処理	指定したリスナーに対するホスト アクセス テーブルの設定が処理されます。システムからは、入力したリモート IP アドレスおよびリモート ドメイン名と一致した HAT 内のエントリが報告されます。デフォルトのメール フロー ポリシーと送信者グループ、およびどちらが所定のエントリに一致したかを確認できます。 Cisco アプライアンスが（REJECT または TCPREFUSE アクセス ルールを介して）接続を拒否するように設定された場合、処理中の trace コマンドはその時点で終了します。 HAT プロパティの設定の詳細については、定義済みの送信者グループとメール フロー ポリシーの理解を参照してください。
エンベロープ送信者アドレスの処理 これらのセクションには、指定したエンベロープ送信者に対してアプライアンスの設定がどのように影響するかが要約されます（つまり、MAIL FROM コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。**`trace`** コマンドは、このセクションの前に「**`Processing MAIL FROM:`**」と出力します。	
デフォルト ドメイン	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ送信者に対するすべての変更がこのセクションに出力されます。 詳細については、電子メールを受信するためのゲートウェイの設定を参照してください。

trace コマンド セクション	出力
マスカレード	メッセージのエンベロープ送信者を変換するように指定した場合、ここに変更が表示されます。**listenerconfig -> edit -> masquerade -> config** サブコマンドを使用して、プライベート リスナーに対するエンベロープ送信者のマスカレードをイネーブルにします。 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。
エンベロープ受信者の処理 これらのセクションでは、指定したエンベロープ受信者に対してアプライアンスがどのように影響するかの要約を示します（つまり、RCPT TO コマンドがアプライアンスの設定によってどのように解釈されるかがわかります）。trace コマンドは、このセクションの前に「Processing Recipient List:」と出力します。	
デフォルト ドメイン	リスナーで、受信するメッセージのデフォルトの送信者ドメインを変更するように指定した場合は、エンベロープ受信者に対するすべての変更がこのセクションに出力されます。 詳細については、電子メールを受信するためのゲートウェイの設定を参照してください。
ドメイン マップの変換	ドメイン マップ機能によって、受信者アドレスが代替アドレスに変換されます。ドメイン マップの変更を指定しており、指定した受信者アドレスが一致した場合は、このセクションに変換が出力されます。 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。
受信者アクセス テーブル（RAT）	ポリシーとパラメータのほか、このセクションには、RAT 内のエントリに一致する各エンベロープ受信者が出力されます（たとえば、リスナーの RAT の制限をバイパスするように受信者が指定された場合など）。 受け入れる受信者の指定の詳細については、電子メールを受信するためのゲートウェイの設定を参照してください。
エイリアス テーブル	このセクションには、アプライアンスで設定されたエイリアス テーブル内のエントリに一致する各エンベロープ受信者（および 1 つまたは複数の受信者アドレスへの後続の変換）が出力されます。 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。

trace コマンド セクション	出力
Pre-Queue メッセージ操作 ここでは、メッセージの内容を受信した後、ワーク キュー上でメッセージがキューから出る前に、各メッセージにアプライアンスがどのように影響するかを示します。この処理は、最後の **250 ok** コマンドがリモート MTA に返される前に実行されます。 **trace** コマンドは、このセクションの前に「Message Processing:」と出力します。	
仮想ゲートウェイ	**altsrchost** コマンドを実行すると、エンベロープ送信者の完全アドレス、ドメイン、または名前、あるいは IP アドレスの一致に基づいて、特定のインターフェイスにメッセージが割り当てられます。エンベロープ送信者が **altsrchost** コマンドのエントリに一致すると、その情報がこのセクションに出力されます。 この時点で割り当てられた仮想ゲートウェイ アドレスは、メッセージ フィルタの処理によって上書きされる可能性があることに注意してください。 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。
バウンス プロファイル	バウンス プロファイルは、処理中の 3 つの時点で適用されます。ここが最初のポイントです。リスナーにバウンス プロファイルが割り当てられる場合は、プロセス内のこの時点で割り当てられます。その情報がこのセクションに出力されます。 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。
ワーク キュー操作 次の一連の機能は、ワーク キュー内のメッセージに対して実行されます。機能が実行されるのは、クライアントからのメッセージが受け入れられた後、そのメッセージが配信用として宛先キューに入れられる前です。status コマンドおよび status detail コマンドにより、「Messages in Work Queue」が報告されます。	
マスカレード	メッセージの [宛先:（To:）]、[差出人:（From:）]、および [CC:] ヘッダーが（リスナーから入力されたスタティック テーブルまたは LDAP クエリーを通じて）マスクされるように指定した場合は、ここに変更が表示されます。**listenerconfig -> edit -> masquerade -> config** サブコマンドを使用して、プライベート リスナーに対してメッセージヘッダーのマスカレードをイネーブルにします。 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。

trace コマンド セクション	出力
LDAP ルーティング	リスナーに対して LDAP クエリーがイネーブルになっている場合は、このセクションにLDAP許可、再ルーティング、マスカレード、およびグループ クエリーの結果が出力されます。 詳細については、LDAP クエリを参照してください。
メッセージ フィルタの処理	システムでイネーブルになっているすべてのメッセージフィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最終結果が「true」の場合、そのフィルタ内の各アクションが順番に実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。ルールが「false」と評価され、アクションのリストが else 句と関連付けられている場合、それらのアクションが代わりに評価されます。このセクションには、順番に処理されたメッセージ フィルタの結果が出力されます。 メッセージ フィルタを使用した電子メール ポリシーの適用を参照してください。
メール ポリシーの処理 メール ポリシーの処理セクションには、アンチスパム、アンチウイルス、アウトブレイク フィルタ機能と、指定されたすべての受信者に対する免責事項スタンプ機能が表示されます。複数の受信者が電子メール セキュリティ マネージャの複数のポリシーに一致する場合は、一致する各ポリシーが次の各セクションに繰り返し表示されます。文字列「Message Going to」は、どの受信者がどのポリシーと一致するかを定義します。	
スパム対策	このセクションには、アンチスパム スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチスパム スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。Cisco アプライアンスが、その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、**trace** コマンドの処理は停止します。 （注）システムでアンチスパム スキャンが使用できない場合、この手順は省略されます。アンチスパム スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 「スパムおよびグレイメールの管理」を参照してください。

trace コマンド セクション	出力
アンチウイルス	このセクションには、アンチウイルス スキャンの処理対象としてフラグが設定されていないメッセージが示されます。メッセージがリスナーに対するアンチウイルス スキャンによって処理されることになっている場合、メッセージは処理され、返された判定が出力されます。感染したメッセージを「クリーニング」するようにCiscoアプライアンスが設定されている場合は、その情報が表示されます。その判定に基づいてメッセージをバウンスまたはドロップするように設定されている場合は、その情報が出力され、trace コマンドの処理は停止します。 （注）システムでアンチウイルス スキャンが使用できない場合、この手順は省略されます。アンチウイルス スキャンを使用できても、ライセンス キーによってイネーブルになっていない場合は、その情報もこのセクションに出力されます。 アンチウイルスを参照してください。
コンテンツ フィルタの処理	システムでイネーブルになっているすべてのコンテンツ フィルタは、この時点でテスト メッセージによって評価されます。フィルタごとにルールが評価され、最終結果が「true」の場合、そのフィルタ内の各アクションが順番に実行されます。フィルタには他のフィルタがアクションとして含まれている場合があり、フィルタは無制限にネスティングされます。このセクションには、順番に処理されたコンテンツ フィルタの結果が出力されます。 コンテンツ フィルタを参照してください。
アウトブレイク フィルタの処理	このセクションには、アウトブレイク フィルタ機能をバイパスする添付ファイルのあるメッセージが示されます。メッセージが受信者に対するアウトブレイク フィルタによって処理されることになっている場合、メッセージは処理され、その評価が出力されます。アプライアンスが、判定に基づいてメッセージを隔離、バウンス、またはドロップするように設定されている場合、その情報が出力されて、処理が停止します。 アウトブレイク フィルタを参照してください。
フッター スタンプ	このセクションには、メッセージにフッター テキスト リソースが付加されたかどうかが示されます。テキスト リソースの名前が表示されます。テキスト リソースのメッセージの免責事項スタンプを参照してください。

trace コマンド セクション	出力
配信操作 次の各セクションには、メッセージが配信されるときに発生する動作が示されます。trace コマンドは、このセクションの前に「Message Enqueued for Delivery」と出力します。	
ドメインおよびユーザごとのグローバル配信停止	trace コマンドの入力として指定した受信者が、グローバル配信停止機能に示されている受信者、受信者ドメイン、または IP アドレスに一致すると、未登録の受信者アドレスがこのセクションに出力されます。 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。
最終結果 すべての処理が出力されると、最終結果が表示されます。CLI では、「Would you like to see the resulting message?」という問いに対して **y** と入力して、結果のメッセージを表示します。	

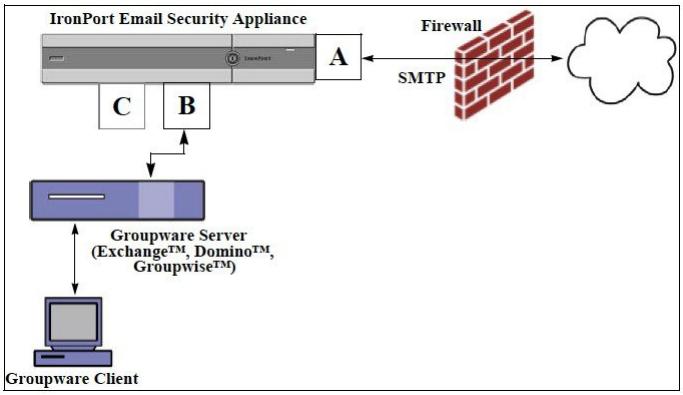
アプライアンスのテストにリスナーを使用

「ブラック ホール」リスナーは、メッセージ生成システムをテストし、受信パフォーマンスの簡単な測定ができます。ブラック ホール リスナーには、キューイングおよび非キューイングの 2 種類があります。

- キューイング リスナーは、メッセージをキューに保存しますが、その後メッセージをただちに削除します。メッセージ生成システムのインジェクション部分全体のパフォーマンスを測定する場合は、キューイング リスナーを使用します。
- 非キューイング リスナーはメッセージを承認した後、保存しないですぐに削除します。メッセージ生成システムからアプライアンスまでの接続のトラブルシューティングを行う場合は、非キューイング リスナーを使用します。

たとえば次の図では、ブラック ホール リスナー「C」を作成して、「B」というプライベート リスナーをミラーリングします。非キューイング版では、グループウェア クライアントからグループウェア サーバを経由してアプライアンスまでのシステムのパフォーマンス パスをテストします。キューイング版は、同じ方法およびメッセージをキューに入れて SMTP 経由で配信するためのアプライアンスの機能をテストします。

図 *1:* エンタープライズ ゲートウェイに対するブラック ホール リスナー



次の例では、listenerconfig コマンドを使用して、管理インターフェイス上で BlackHole_1 という名前のブラック ホール キューイング リスナーを作成します。リスナーのためのこのホスト アクセステーブル（HAT）は、次のホストからの接続を受け入れるように編集されています。

- **yoursystem.example.com**
- **10.1.2.29**
- **badmail.tst**
- **.tst**

（注） 最後のエントリである .tst により、.tst ドメイン内にあるすべてのホストから BlackHole_1 という名前のリスナーに電子メールを送信できるようになります。

例

```
mail3.example.com> listenerconfig

Currently configured listeners:

1. InboundMail (on PublicNet, 192.168.2.1) SMTP Port 25 Public

2. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]> new

Please select the type of listener you want to create.

1. Private
```

```
2. Public

3. Blackhole

[2]> 3

Do you want messages to be queued onto disk? [N]> y

Please create a name for this listener (Ex: "OutboundMail"):

[]> BlackHole_1

Please choose an IP interface for this Listener.

1. Management (192.168.42.42/24: mail3.example.com)

2. PrivateNet (192.168.1.1/24: mail3.example.com)

3. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Choose a protocol.

1. SMTP

2. QMQP

[1]> 1

Please enter the IP port for this listener.

[25]> 25

Please specify the systems allowed to relay email through the IronPort C60.

Hostnames such as "example.com" are allowed.

Partial hostnames such as ".example.com" are allowed.

IP addresses, IP address ranges, and partial IP addressed are allowed.

Separate multiple entries with commas.


[]> yoursystem.example.com, 10.1.2.29, badmail.tst, .tst

Do you want to enable rate limiting per host? (Rate limiting defines
the maximum number of recipients per hour you are willing to receive from a remote
domain.) [N]> n

Default Policy Parameters

==========================

Maximum Message Size: 100M

Maximum Number Of Connections From A Single IP: 600

Maximum Number Of Messages Per Connection: 10,000

Maximum Number Of Recipients Per Message: 100,000
```

```
Maximum Number Of Recipients Per Hour: Disabled

Use SenderBase for Flow Control: No

Spam Detection Enabled: No

Virus Detection Enabled: Yes

Allow TLS Connections: No

Allow SMTP Authentication: No

Require TLS To Offer SMTP authentication: No

Would you like to change the default host access policy? [N]> n

Listener BlackHole_1 created.

Defaults have been set for a Black Hole Queuing listener.

Use the listenerconfig->EDIT command to customize the listener.

Currently configured listeners:

1. BlackHole_1 (on Management, 192.168.42.42) SMTP Port 25 Black Hole Queuing

2. InboundMail (on PublicNet, 192.1681.1) SMTP Port 25 Public

3. OutboundMail (on PrivateNet, 192.168.1.1) SMTP Port 25 Private

Choose the operation you want to perform:

- NEW - Create a new listener.

- EDIT - Modify a listener.

- DELETE - Remove a listener.

- SETUP - Change global settings.

[]>
```

（注） commit コマンドを実行して、これらの変更が有効になるようにしてください。

キューイング タイプのブラック ホール リスナーを設定して、HAT でインジェクション システムからの接続を受け入れるよう変更したら、インジェクション システムを使用して、アプライアンスへの電子メールの送信を開始します。status、status detail、および rate コマンドを使用して、システムのパフォーマンスをモニタします。また、グラフィカル ユーザ インターフェイス（GUI）でシステムをモニタすることもできます。詳細については、以下を参照してください。

- CLI を使用したモニタリング
- GUI での他のタスク

ネットワークのトラブルシューティング

アプライアンスにネットワーク接続の問題があると思われる場合は、アプライアンスが適切に動作していることを確認します。

アプライアンスのネットワーク接続テスト

手順

ステップ 1 システムに接続し、管理者としてログインします。正常にログインできると、次のメッセージが表示されます。

```
Last login: day month date hh:mm:ss from IP address

Copyright (c) 2001-2003, IronPort Systems, Inc.

AsyncOS x.x for Cisco


Welcome to the Cisco Messaging Gateway Appliance(tm)
```

ステップ 2 status コマンドまたは status detail コマンドを使用します。

```
mail3.example.com> status
```

または

```
mail3.example.com> status detail
```

status コマンドは、電子メール動作についてモニタされる情報のサブセットを返します。返される統計情報は、カウンタとゲージの2つのカテゴリにグループ化されます。レートなどの電子メールの動作についての全般的なモニタリング情報については、status detail コマンドを使用します。カウンタは、システム内の各種イベントの現在までの合計を示します。カウンタごとに、そのカウンタのリセット以降、最後のシステム再起動以降、およびシステムの存続期間に発生したイベントの合計数を表示できます。（詳細については、CLI を使用したモニタリング を参照してください）。

ステップ 3 mailconfig コマンドを使用して、機能している既知のアドレスに電子メールを送信します。

mailconfig コマンドによって、アプライアンスで有効な設定のすべてが含まれる、人が読み取ることのできるファイルが作成されます。このファイルをアプライアンスから機能する既知の電子メールアドレスに送信して、アプライアンスがネットワークで電子メールを送信できることを確認します。

```
mail3.example.com> mailconfig
```

```
Please enter the email address to which you want to send the
configuration file.


Separate multiple addresses with commas.

[]> user@example.com

Do you want to include passphrases? Please be aware that a configuration without
passphrases will fail when reloaded with loadconfig. [N]> y


The configuration file has been sent to user@example.com.

mail3.example.com>
```

トラブルシューティング

アプライアンスがネットワーク上でアクティブであることが確認されたら、次のコマンドを使用して、ネットワークの問題をピンポイントで特定します。

- `netstat` コマンドを使用すると、次のようなネットワーク接続（着信と発信の両方）、ルーティング テーブル、ネットワーク インターフェイスのさまざまな統計情報が表示されます。
  - アクティブなソケットのリスト
  - ネットワーク インターフェイスの状態
  - ルーティング テーブルの内容
  - リッスン キューのサイズ
  - パケット トラフィック情報
- `diagnostic -> network -> flush` コマンドを使用すると、ネットワークに関連するすべてのキャッシュをフラッシュできます。
- `diagnostic -> network -> arpshow` コマンドを使用すると、システムの ARP キャッシュを表示できます。
- `packetcapture` コマンドを使用すると、コンピュータが接続されているネットワーク上で送受信されている TCP/IP や他のパケットを傍受して表示できます。

  `packetcapture` を使用するには、ネットワーク インターフェイスとフィルタを設定します。このフィルタでは、UNIX の `tcpdump` コマンドと同じ形式を使用します。パケットの捕捉を開始するには start を、停止するには stop を使用します。捕捉を停止した後、SCP または FTP を使用して /pub/captures ディレクトリからファイルをダウンロードする必要があります。詳細については、パケット キャプチャの実行 （29 ページ）を参照してください。

- アプライアンスでネットワーク上にアクティブな接続があり、ネットワーク上の特定のセグメントに到達できることを確認するには、動作している既知のホストに対して ping コマンドを使用します。

  ping コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストできます。

```
mail3.example.com> ping

Which interface do you want to send the pings from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host you wish to ping.

[]> anotherhost.example.com

Press Ctrl-C to stop.

PING anotherhost.example.com (x.x.x.x): 56 data bytes

64 bytes from 10.19.0.31: icmp_seq=9 ttl=64 time=0.133 ms

64 bytes from 10.19.0.31: icmp_seq=10 ttl=64 time=0.115 ms

^C

--- anotherhost.example.com ping statistics ---

11 packets transmitted, 11 packets received, 0% packet loss

round-trip min/avg/max/stddev = 0.115/0.242/1.421/0.373 ms
```

（注） ping コマンドを終了するには、Ctrl+C を使用する必要があります。

- traceroute コマンドを使用すると、アプライアンスからネットワーク ホストへの接続をテストして、ネットワークのホップに関するルーティングの問題をデバッグできます。

```
mail3.example.com> traceroute

Which interface do you want to trace from?

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)
```

```
4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 1

Please enter the host to which you want to trace the route.

[]> 10.1.1.1

Press Ctrl-C to stop.

traceroute to 10.1.1.1 (10.1.1.1), 64 hops max, 44 byte packets

1 gateway (192.168.0.1) 0.202 ms 0.173 ms 0.161 ms

2 hostname (10.1.1.1) 0.298 ms 0.302 ms 0.291 ms

mail3.example.com>
```

- `diagnostic -> network -> smtpping` コマンドを使用すると、リモートの SMTP サーバをテストできます。
- `nslookup` コマンドを使用すると、DNS の機能を検査できます。

  `nslookup` コマンドでは、アプライアンスが、動作している DNS（ドメイン ネーム サービス）サーバからホスト名と IP アドレスを解決して到達できることを確認できます。

```
mail3.example.com> nslookup

Please enter the host or IP to resolve.

[]> example.com

Choose the query type:

1. A

2. CNAME

3. MX

4. NS

5. PTR

6. SOA

7. TXT

[1]>

A=192.0.34.166 TTL=2d
```

表 *3 : DNS* の機能の確認：クエリーのタイプ

A	ホストのインターネット アドレス
CNAME	エイリアスの正規の名前

MX	メール エクスチェンジャ
NS	指定したゾーンのネーム サーバ
PTR	クエリーがインターネットアドレスの場合はホスト名、そうでない場合は他の情報に対するポインタ
SOA	ドメインの「権限開始」情報
TXT	テキスト情報

- `tophosts` コマンドを CLI または GUI から使用して、「Active Recipients」の順にソートします。

  `tophosts` コマンドからは、キューにある上位 20 の受信者のリストが返されます。このコマンドは、ネットワーク接続の問題が、電子メールを送信しようとしている 1 台のホストまたは 1 つのホスト グループに限定されるかどうかを確認するのに役立ちます（詳細については、「電子メール キューの構成の確認」を参照してください）

```
mail3.example.com> tophosts

Sort results by:

1. Active Recipients

2. Connections Out

3. Delivered Recipients

4. Soft Bounced Events

5. Hard Bounced Recipients

[1]> 1

Status as of: Mon Nov 18 22:22:23 2003

ActiveConn.Deliv.SoftHard

# Recipient HostRecipOutRecip.BouncedBounced

1 aol.com36510255218

2 hotmail.com29071982813

3 yahoo.com13461231119

4 excite.com9838494

5 msn.com8427633 29

^C
```

- tophosts コマンドの結果として得られたリストの最上位のドメインに対して `hoststatus` コマンドを実行し、詳しく調べます。

`hoststatus` コマンドは、特定の受信者ホストに関する電子メール動作のモニタリング情報を返します。AsyncOS キャッシュに格納されている DNS 情報と、受信者ホストから最後に返されたエラーも表示されます。返されるデータは、最後に実行した `resetcounters` コマンドからの累積です。（詳細については、メールホストのステータスのモニタリングを参照してください）。

最上位のドメインに対して `hoststatus` コマンドを実行すると、アプライアンスまたはインターネットのいずれかに対する DNS 解決のパフォーマンスの問題を切り分けることができます。たとえば、最上位のアクティブな受信ホストに対して `hoststatus` コマンドを実行したとき、発信側の多数の接続が保留状態で表示された場合は、特定のホストがダウン状態または到達不能でないかどうか、またアプライアンスがすべてのホストあるいは大半のホストに接続不可能でないかどうかを確認してください。

- ファイアウォールの権限を確認します。

  アプライアンスが正しく機能するためには、ポート 20、21、22、23、25、53、80、123、443、および 628 を開く必要がある場合があります（ファイアウォール情報を参照）。

- ネットワーク上のアプライアンスから、dnscheck@ironport.com に対して電子メールを送信します。

  システムの基本的な DNS チェックを実行するために、ネットワーク内から dnscheck@ironport.com に電子メールを送信します。オートレスポンダによる電子メールによって、次の 4 つのテストについての結果と詳細が返されます。

DNS PTR レコード：Envelope From の IP アドレスがドメインの PTR レコードと一致するか。

DNS A レコード：ドメインの PTR レコードが Envelope From の IP アドレスと一致するか。

HELO マッチ：`SMTP HELO` コマンドにリストされたドメインが、Envelope From の DNS ホスト名と一致するか。

遅延バウンス メッセージを受け入れるメール サーバ：`SMTP HELO` コマンドのリストにあるドメインに、そのドメインの IP アドレスを解決する MX レコードがあるか。

リスナーのトラブルシューティング

電子メールのインジェクションに問題があると疑われる場合は、次の方法を使用します。

- インジェクションを行っている IP アドレスを確認し、`listenerconfig` コマンドを使用して許可されているホストを確認します。

  作成したリスナーに接続できるよう IP アドレスが許可されていますか。`listenerconfig` コマンドを使用して、リスナーのホスト アクセス テーブル（HAT）を確認します。次のコマンドを使用して、リスナーの HAT を出力します。

  ```
  listenerconfig -> edit -> listener_number -> hostaccess -> print
  ```

  HAT は、IP アドレス、IP アドレスのブロック、ホスト名、ドメインなどを使用して、接続を拒否するよう設定できます。詳細については、「接続が許可されているホストの指定」を参照してください。

また、limitsサブコマンドを使用して、リスナーに許可されている接続の最大数を確認することもできます。

```
listenerconfig -> edit -> listener_number -> limits
```

- インジェクションを行っているマシンから、Telnet または FTP を使用して、アプライアンスに手動で接続します。次に例を示します。

```
injection_machine% telnet appliance_name
```

アプライアンス内で telnet コマンドを使用して、リスナーから実際のアプライアンスに接続することもできます。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.

1. Auto

2. Management (192.168.42.42/24: mail3.example.com)

3. PrivateNet (192.168.1.1/24: mail3.example.com)

4. PublicNet (192.168.2.1/24: mail3.example.com)

[1]> 3

Enter the remote hostname or IP.

[]> 193.168.1.1

Enter the remote port.

[25]> 25

Trying 193.168.1.1...

Connected to 193.168.1.1.

Escape character is '^]'.
```

あるインターフェイスから他のインターフェイスに接続できない場合は、アプライアンスの Management、Data1、Data2 インターフェイスからネットワークに接続している方法に問題がある可能性があります。詳細については、FTP、SSH、および SCP アクセスを参照してください。リスナーのポート 25 に対して telnet を実行して、SMTP コマンドを手動で入力できます（このプロトコルを熟知している場合）。

- IronPort のテキスト メール ログおよびインジェクション デバッグ ログを調べて、受信エラーがあるかどうかを確認します。

インジェクション デバッグ ログには、アプライアンスと、システムに接続している指定のホスト間の SMTP 会話が記録されます。インジェクション デバッグ ログは、インターネットから接続を開始するクライアントとアプライアンス間の通信に関する問題をトラブルシューティングするのに役立ちます。このログでは、2 つのシステム間で伝送されたすべてのバイトが記録され、接続ホストに「送信」または接続ホストから「受信」に分類されます。

詳細については、テキスト メール ログの使用およびインジェクション デバッグ ログの使用を参照してください。

アプライアンスからの電子メール配信のトラブルシューティング

アプライアンスからの電子メールの配信に問題があると疑われる場合は、次の方法を試してください。

- 問題がドメインに限定されたものであるかどうかを判断します。

  `tophosts` コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

  「Active Recipients」の順にソートすると、問題のあるドメインが返されますか。

  「Connections Out」の順にソートしたとき、リスナーに指定されている最大接続数に達しているドメインがありますか。リスナーに対するデフォルトの最大接続数は 600 です。システム全体でのデフォルトの最大接続数は 10,000 です（`deliveryconfig` コマンドで設定します）。リスナーに対する最大接続数は、次のコマンドで確認できます。

  ```
  listenerconfig -> edit -> listener_number -> limits
  ```

  リスナーに対する接続が、`destconfig` コマンドによってさらに制限されていませんか（システムの最大数または仮想ゲートウェイ アドレスによる）。`destconfig` による接続の制限を確認するには、次のコマンドを使用します。

  ```
  destconfig -> list
  ```

- `hoststatus` コマンドを使用します。

  `tophosts` コマンドの結果として得られたリストの最上位のドメインに対して `hoststatus` コマンドを実行し、詳しく調べます。

  ホストが使用可能で、接続を受け入れていますか。

  指定したホストに対する特定の MX レコードのメール サーバに問題がありませんか。

  `hoststatus` コマンドでは、特定のホストに対する 5XX エラー（Permanent Negative Completion Reply）がある場合に、ホストから返された直前の「5XX」のステータス コードと説明が表示されます。このホストに対する直前の発信 TLS 接続が失敗した場合は、`hoststatus` コマンドで失敗した理由が表示されます。

- ドメインのデバッグ、バウンス、およびテキスト メールの各ログを設定および確認して、受信ホストが使用可能かどうかをチェックします。

  ドメイン デバッグ ログには、アプライアンスと指定の受信者ホスト間の SMTP 会話でのクライアントとサーバの通信が記録されます。このタイプのログ ファイルは、特定の受信ホストに関する問題のデバッグに使用できます。

詳細については、ドメイン デバッグ ログの使用を参照してください。

バウンス ログには、バウンスされた各受信者に関するすべての情報が記録されます。

詳細については、バウンス ログの使用を参照してください。

テキスト メール ログには、電子メールの受信、電子メールの配信、およびバウンスの詳細が記録されます。これらのログは、特定のメッセージの配信を理解し、システムパフォーマンスを分析するうえで有益な情報源となります。

詳細については、テキスト メール ログの使用を参照してください。

- `telnet` コマンドを使用して、アプライアンスから問題のあるドメインに接続します。

```
mail3.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. Management (192.168.42.42/24: mail3.example.com)
3. PrivateNet (192.168.1.1/24: mail3.example.com)
4. PublicNet (192.168.2.1/24: mail3.example.com)
[1]> 1
Enter the remote hostname or IP.
[]> problemdomain.net
Enter the remote port.

[25]> 25
```

- 必要に応じて `tlsverify` コマンドを使用して発信 TLS 接続を確立し、宛先ドメインに関する TLS 接続の問題をデバッグすることができます。接続を確立するには、検証するドメインと宛先ホストを指定します。AsyncOS では、必要な（検証）TLS 設定に基づいて TLS 接続を確認します。

```
mail3.example.com> tlsverify

Enter the TLS domain to verify against:
[]> example.com
Enter the destination host to connect to. Append the port (example.com:26) if you are
not connecting on port 25:
[example.com]> mxe.example.com:25
Connecting to 1.1.1.1 on port 25.
Connected to 1.1.1.1 from interface 10.10.10.10.
Checking TLS connection.
```

```
TLS connection established: protocol TLSv1, cipher RC4-SHA.

Verifying peer certificate.

Verifying certificate common name mxe.example.com.

TLS certificate match mxe.example.com

TLS certificate verified.

TLS connection to 1.1.1.1 succeeded.

TLS successfully connected to mxe.example.com.

TLS verification completed.
```

パフォーマンスのトラブルシューティング

アプライアンスのパフォーマンスに関する問題があると疑われる場合は、次の方法を使用してください。

- rate コマンドと `hostrate` コマンドを使用して、現在のシステムのアクティビティを確認します。

  rate コマンドは、電子メール動作に関するリアルタイム モニタリング情報を返します。詳細については、リアルタイム アクティビティの表示を参照してください。

  `hostrate` コマンドは、特定のメール ホストに関するリアルタイムのモニタリング情報を返します。

- status コマンドを使用して、これまでのレートを比較して、状態の悪化を確認します。

- `status detail` コマンドを使用して、メモリの使用率を確認します。

  `status detail` コマンドを使用すると、システムのメモリ、CPU、ディスク I/O の使用率を、素早く確認できます。

（注） メモリの使用率は、常に45%未満である必要があります。メモリの使用率が 45% を超えると、アプライアンスは「リソース節約モード」に入ります。これによって「バックオフ」アルゴリズムが起動され、リソースのオーバーサブスクリプションが防止され、電子メールによる次のアラートが送信されます。

```
This system (hostname: hostname) has entered a 'resource conservation' mode in order
 to
prevent the rapid depletion of critical system resources.


RAM utilization for this system has exceeded the resource conservation threshold of
 45%.
The allowed injection rate for this system will be gradually decreased as RAM
```

`utilization approaches 60%.`

この状況は、配信機能が低下していて、大量のインジェクションが行われているときにのみ発生します。メモリの使用率が 45% を超えたときには、キュー内のメッセージの数を調べて、特定のドメインがダウン状態または配信不可能になっていないかどうかを確認します（`hoststatus` コマンドまたは `hostrate` コマンドを使用します）。また、システムのステータスも確認して、配信が中断されないようにします。インジェクションが停止しても、依然としてメモリの使用率が高い場合は、シスコ カスタマー サポートにご連絡ください。

- 問題が 1 つのドメインに限定されていますか。

  `tophosts` コマンドを使用して、電子メール キューに関する直近の情報を入手して、特定の受信者のドメインに配信の問題が生じていないかを確認します。

  キューのサイズを確認します。このサイズを制御したり、問題が生じている特定のドメインの受信者に対処するために、電子メールキューにあるメッセージを削除、バウンス、中断、またはリダイレクトすることができます。詳細については、電子メール キューの管理を参照してください。以下のコマンドを使用します。

  - `deleterecipients`
  - `bouncerecipients`
  - `redirectrecipients`
  - `suspenddel / resumedel`
  - `suspendlistener / resumelistener`

  `tophosts` コマンドを使用して、ソフト バウンスおよびハード バウンスの数を確認します。[ソフト バウンスしたイベント数（Soft Bounced Events）]（オプション 4）または [ハード バウンスした受信者（Hard Bounced Recipients）]（オプション 5）でソートします。特定のドメインに対するパフォーマンスに問題があることが疑われる場合は、上記のコマンドを使用して、そのドメインへの配信を制御します。

Web インターフェイスの外観およびレンダリングの問題

Internet Explorer の互換モードの上書きを参照してください。

アラートへの応答

- アラート：C380 または C680 ハードウェアでの [バッテリ再学習タイムアウト（Battery Relearn Timed Out）]（RAID イベント）　（24 ページ）
- その他のディスク使用量がクォータに近づいているというアラートのトラブルシューティング　（24 ページ）

アラート：C380 または C680 ハードウェアでの [バッテリ再学習タイムアウト（Battery Relearn Timed Out）]（RAID イベント）

問題

C380 または C680 ハードウェアで「バッテリ再学習タイムアウト」（RAID イベント）アラートを受信しました。

解決方法

このアラートは、問題を示している場合と示していない場合があります。バッテリ再学習タイムアウト自体は、RAID コントローラに問題があることを示すものではありません。コントローラは、後続の再学習で回復します。以降 48 時間他の RAID アラートに関する電子メールを監視して、この問題が他の問題の副作用ではないことを確認してください。システムから他の RAID 関連のアラートが表示されない場合は、この警告を無視してかまいません。

その他のディスク使用量がクォータに近づいているというアラートのトラブルシューティング

問題

その他のディスク使用量がクォータに近づいているというアラートを受信しました。

解決方法

クォータを増やすか、ファイルを削除できます。その他のクォータのディスク領域の管理を参照してください。

ハードウェア問題のトラブルシューティング

ハードウェア アプライアンスの前面/背面パネルのライトは、アプライアンスの状態およびステータスを示します。これらのインジケータの説明については、『*Cisco x90s Series Content Security Appliances Installation and Maintenance Guide*』など、http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html から入手できるハードウェア ガイドを参照してください。

温度範囲など、アプライアンスの仕様についてもこれらのマニュアルで確認できます。

アプライアンスの電源のリモート リセット

アプライアンスのハード リセットが必要な場合は、サードパーティの Platform Management（IPMI）ツールを使用してアプライアンス シャーシをリモートからリブートできます。

制約事項

- リモート電源管理は、特定のハードウェアでのみ使用できます。

詳細については、リモート電源再投入の有効化を参照してください。

- この機能を使用する場合は、使用が必要になる前に、あらかじめ有効にしておく必要があります。

  詳細については、リモート電源再投入の有効化を参照してください。

- 次の IPMI コマンドのみがサポートされています。
  - **status、on、off、cycle、reset、diag、soft**
  - サポートされていないコマンドを発行すると、「権限不足」エラーが発生します。

はじめる前に

- IPMI バージョン 2.0 を使用してデバイスを管理できるユーティリティを取得し、設定します。
- サポートされている IPMI コマンドの使用方法を理解します。IPMI ツールのマニュアルを参照してください。

手順

ステップ 1 IPMI を使用して、必要なクレデンシャルと共に、先に設定したリモート電源管理ポートに割り当てられた IP アドレスに、サポートされている電源の再投入コマンドを発行します。

たとえば、IPMI をサポートする UNIX タイプのマシンからは、次のようなコマンドを発行します。

```
ipmitool -I lan -H 192.0.2.1 -U remoteresetuser -P password chassis
power reset
```

ここで **192.0.2.1** は、リモート電源管理ポートに割り当てられた IP アドレスであり、**remoteresetuser** およびパスワードは、この機能を有効にしたときに入力したクレデンシャルです。

ステップ 2 アプライアンスが再起動されるまで、少なくとも 11 分間待ちます。

テクニカル サポートの使用

仮想アプライアンスのテクニカル サポート

仮想アプライアンスのテクニカル サポートを受けるための要件は、http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-installation-guides-list.html にある『Cisco Content Security Virtual Appliance Installation Guide』に記載されています。

アプライアンスからのサポート ケースのオープンおよび更新

はじめる前に

- 緊急の問題の場合、この方法は使用しないでください。代わりに、シスコ カスタマー サポートに示されるその他の方法の 1 つを使用してサポートください。

  次の手順は、情報が必要であるまたは回避策があるけれども代替策を使用したいといった問題に限り使用します。

- ヘルプに関しては別の選択肢を検討してみてください。
  - ナレッジ ベース
  - シスコ サポート コミュニティ
- アプライアンスからシスコ テクニカル サポートに直接アクセスするには、Cisco.com ユーザ ID がこのアプライアンスのサービス契約に関連付けられている必要があります。Cisco.com プロファイルに現在関連付けられているサービス契約の一覧を参照するには、Cisco.com Profile Manager（https://sso.cisco.com/autho/forms/CDClogin.html）にアクセスしてください。Cisco.com のユーザ ID がない場合は、登録して ID を取得してください。Cisco アカウントの登録を参照してください。

  Cisco.com ユーザ ID とサポート契約 ID は、安全な場所に保存してください。

- この手順を使用してサポート事例を開くと、アプライアンスの設定ファイルがシスコ カスタマー サポートに送信されます。アプライアンスの設定を送信したくない場合、別の方法を使用してカスタマー サポートにお問い合わせください。
- クラスタ設定では、サポート要求と保存されたそれらの値はマシンに固有のものです。
- アプライアンスがインターネットに接続され電子メールを送信できる必要があります。
- 既存の事例に関する情報を送信する場合は、ケース番号を確認してください。

手順

ステップ 1 アプライアンスにログインします。

ステップ 2 [ヘルプとサポート（Help and Support）]>[テクニカルサポートに問い合わせる（Contact Technical Support）] を選択します。

ステップ 3 フォームに入力します。

ステップ 4 [送信（Send）] をクリックします。

（注） CCO ユーザ ID と最後に入力された契約 ID は、将来使用できるようにアプライアンスに保存されます。

シスコのテクニカル サポート担当者のリモート アクセスの有効化

シスコのカスタマーアシスタンスのみ、次の方法を使用してアプライアンスにアクセスできます。

インターネット接続されたアプライアンスへのリモート アクセスの有効化

サポートは、この手順でアプライアンスと **upgrades.ironport.com** のサーバ間で作成される SSH トンネル経由でアプライアンスにアクセスします。

はじめる前に

インターネットから到達可能なポートを識別します。デフォルトでは、ポート 25 で、このポートは大部分の環境で機能します。システムは、電子メールメッセージを送信するために、このポートを介して一般的なアクセスを行う必要があるためです。このポート経由の接続は、ほとんどのファイアウォール設定で許可されます。

手順

ステップ 1 アプライアンスへのログイン

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 [有効（Enable）] をクリックします。

ステップ 4 情報を入力します。

オプション	説明
シード文字列（Seed String）	シード文字列は、シスコ カスタマー サポートがこのアプライアンスにアクセスするための安全な共有秘密を生成するために使用されます。

オプション	説明
セキュア トンネル（Secure Tunnel）	リモート アクセス接続にセキュア トンネルを使用するために、このチェックボックスをオンにします。 接続ポートを入力します。 デフォルトでは、ポート 25 です。このポートはほとんどの環境で機能します。

ステップ 5 [送信（Submit）] をクリックします。

次のタスク

サポート担当者のリモート アクセスが必要なくなったときは、テクニカル サポートのトンネルの無効化 （29 ページ）を参照してください。

インターネットに直接接続されていないアプライアンスへのリモートアクセスの有効化

インターネットに直接接続されていないアプライアンスの場合、インターネットに接続されている第 2 のアプライアンスを介してアクセスされます。

はじめる前に

- アプライアンスは、インターネットに接続されている第 2 のアプライアンスにポート 22 で接続する必要があります。
- インターネットに接続されているアプライアンスで該当のアプライアンスへのサポート トンネルを作成するには、インターネット接続されたアプライアンスへのリモート アクセスの有効化 （27 ページ）の手順を実行します。

手順

ステップ 1 サポートが必要なアプライアンスのコマンドライン インターフェイスから、**techsupport** コマンドを入力します。

ステップ 2 **sshaccess** と入力します。

ステップ 3 プロンプトに従います。

次のタスク

サポート担当者のリモートアクセスが必要なくなったときは、次のトピックを参照してください。

- リモート アクセスの無効化 （29 ページ）
- テクニカル サポートのトンネルの無効化 （29 ページ）

テクニカル サポートのトンネルの無効化

有効にした techsupport トンネルは、upgrades.ironport.com に 7 日間接続されたままになります。その後、確立された接続は切断されませんが、いったん切断されるとトンネルに再接続できません。

トンネルを手動で無効にします。

手順

ステップ 1 アプライアンスへのログイン

ステップ 2 GUI ウィンドウの右上にある、[ヘルプとサポート（Help and Support）] > [リモートアクセス（Remote Access）] を選択します。

ステップ 3 [無効（Disable）] をクリックします。

リモート アクセスの無効化

techsupport コマンドを使用して作成したリモート アクセス アカウントは、非アクティブ化されるまでアクティブのままです。

手順

ステップ 1 コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2 sshaccess と入力します。

ステップ 3 disable と入力します。

サポートの接続状態の確認

手順

ステップ 1 コマンドライン インターフェイスから、techsupport コマンドを入力します。

ステップ 2 status と入力します。

パケット キャプチャの実行

パケット キャプチャは、サポート担当者が TCP/IP データおよびその他にアプライアンスから出入りするパケットを表示できるようにします。これはネットワーク設定をデバッグしたり、

どのようなネットワーク トラフィックがアプライアンスに到達または送出されているかを検出することができます。

手順

ステップ 1 [ヘルプとサポート（Help and Support）] > [パケットキャプチャ（Packet Capture）] を選択します。

ステップ 2 パケット キャプチャ設定の指定：

a) [パケットキャプチャ設定（Packet Capture Settings）] セクションで、[設定を編集（Edit Settings）] をクリックします。

b) （任意）パケット キャプチャの期間、制限およびフィルタを入力します。

サポート担当者が、これらの設定の方法を説明する場合があります。

時間の単位を指定しないでキャプチャ期間を入力すると、AsyncOS はデフォルトで秒を使用します。

[フィルタ（Filters）] セクションで次を実行します。

- カスタム フィルタは、UNIX の tcpdump コマンドでサポートされた任意の構文（host 10.10.10.10 && port 80 など）を使用できます。
- クライアント IP は、E メール セキュリティ アプライアンスを介してメッセージを送信するメール クライアントなどのアプライアンスに接続しているマシンの IP アドレスです。
- サーバ IP は、アプライアンスがメッセージを配信する Exchange サーバなどのアプライアンスが接続しているマシンの IP アドレスです。
- クライアントとサーバの IP アドレスを使用して、中間に E メール セキュリティ アプライアンスがある特定のクライアントと特定のサーバ間のトラフィックを追跡できます。

c) [送信（Submit）] をクリックします。

ステップ 3 [キャプチャを開始（Start Capture）] をクリックします。

- キャプチャは一度に 1 つだけ実行できます。
- パケット キャプチャが実行されている場合、[パケットキャプチャ（Packet Capture）] ページには、実行中のキャプチャのステータス（ファイル サイズや経過時間などの現在の統計情報）が表示されます。
- GUI に表示されるのは GUI で開始されたパケット キャプチャだけで、CLI で開始されたパケット キャプチャは表示されません。同様に、CLI には CLI で開始された現在のパケット キャプチャのステータスだけが表示されます。
- パケット キャプチャ ファイルは 10 個の部分に分割されます。パケット キャプチャが終了する前にパケット キャプチャ ファイルが最大サイズ制限に到達した場合は、そのファイルの最も古い部分が削除され（データが破棄されます）、現在のパケット キャプチャデー

タで新しい部分が開始されます。パケット キャプチャ ファイルは一度に 1/10 だけ破棄されます。

- GUI で開始されたキャプチャはセッション間で維持されます。（CLI で実行したキャプチャは、セッションが終了したときに停止します）。

ステップ 4 キャプチャを指定した期間実行するようにします。またはキャプチャを無期限に実行する場合、[キャプチャを停止（Stop Capture）] をクリックして停止します。

ステップ 5 パケット キャプチャ ファイルへアクセスします。

- [パケットキャプチャファイルの管理（Manage Packet Capture Files）] リストでファイルをクリックして、[ファイルのダウンロード（Download File）] をクリックします。
- アプライアンスの captures サブ ディレクトリ内のファイルにアクセスするには、FTP または SCP を使用します。

次のタスク

サポートでファイルを使用できるようにします。

- アプライアンスへのリモート アクセスを許可した場合、Technician が FTP または SCP を使用してパケット キャプチャ ファイルにアクセスできます。シスコのテクニカル サポート担当者のリモート アクセスの有効化 （27 ページ）を参照してください。
- 電子メールでファイルをサポートに送信します。