CHAPTER 15

トラブルシューティング

セキュリティ管理アプライアンスからのカスタマー サポートへのアクセス

カスタマー サポートに連絡する必要がある場合、またはセキュリティ管理アプライアンスの機能をアクティブにする必要がある場合には、次のコマンドと機能が役立ちます。

- 「テクニカル サポート」（P.15-1）
- 「パケット キャプチャ」（P.15-4）

テクニカル サポート

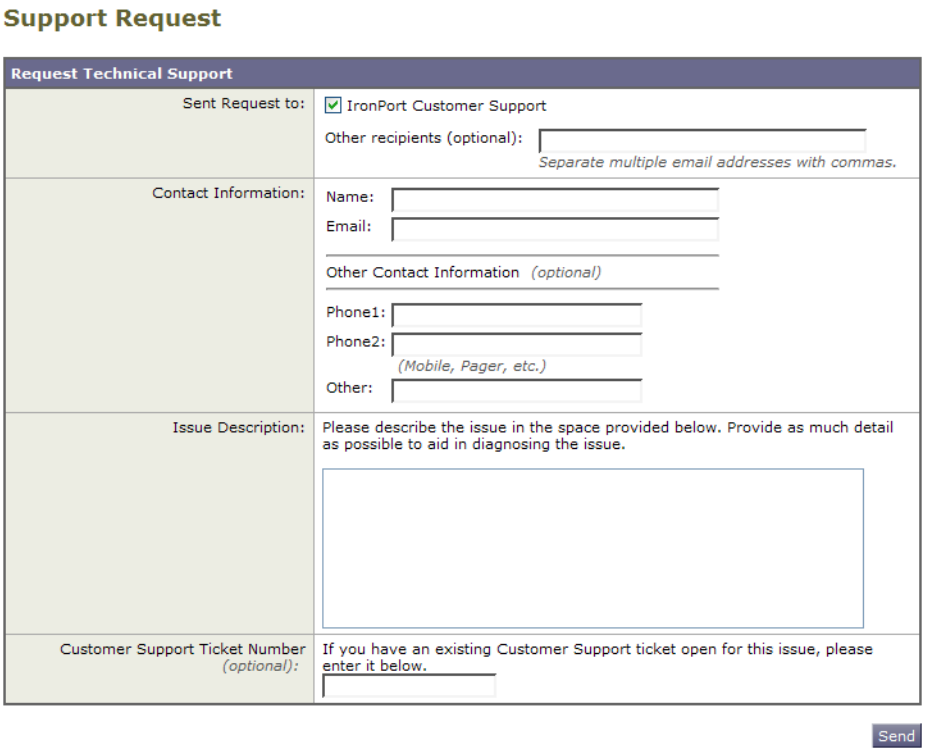
GUI の右上にある [Help and Support] メニューを使用して、Cisco IronPort カスタマー サポートに関連する機能にアクセスします。

テクニカル サポート機能には、[Open a Support Case] ページと [Remote Access] ページの 2 つのページが含まれます。

サポート要求

[Help and Support] > [Open a Support Case] ページ、または **supportrequest** コマンドを使用すると、アプライアンスの設定をカスタマー サポートまたは他のユーザに電子メールで送信したり、サポートを必要とする問題を説明するコメントを入力したりすることができます。**supportrequest** コマンドの詳細については、『*Cisco IronPort AsyncOS CLI Reference Guide*』を参照してください。このコマンドを使用するには、アプライアンスがインターネットにメールを送信できる必要があります。

図 15-1　[Support Request] ページ



Cisco IronPort カスタマー サポート要求を作成するには、次の手順を実行します。

ステップ 1　[Help and Support] > [Open a Support Case] ページで、連絡先情報（名前、電子メール アドレス、および電話番号）を入力します。

ステップ 2　問題の内容を入力します。

ステップ 3　オプションで、[Other recipients] フィールドに、追加受信者の電子メール アドレスを入力します。

デフォルトでは、フォームの上部にあるチェックボックスを選択した場合、サポート要求（コンフィギュレーション ファイルを含む）は、Cisco IronPort カスタマー サポートに送信されます。また、コンフィギュレーション ファイルを他の電子メール アドレスに送信することもできます。複数のアドレスを指定する場合は、カンマで区切ります。

ステップ 4　この問題に関してすでにカスタマー サポート チケットをお持ちの場合は、ページの下部にチケット番号を入力してください。

ステップ 5　[Send] をクリックします。

トラブル チケットが自動的に作成されます。詳細については、「シスコのテクニカル サポート」（P.1-5）を参照してください。

リモート アクセス

アプライアンスへの Cisco IronPort カスタマー サポート リモート アクセスを許可するには、[Remote Access] ページを使用します。

リモート アクセスをイネーブルにするには、次の手順を実行します。

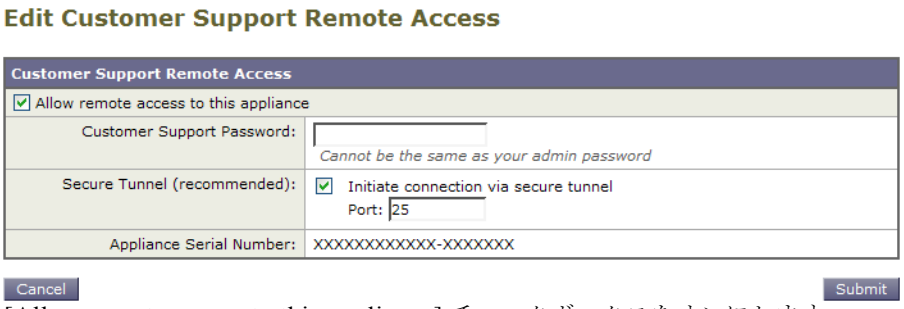
ステップ 1　セキュリティ管理アプライアンス GUI の右側で、[Help and Support] > [Remote Access] を選択します。

[Customer Support Remote Access] ウィンドウが表示されます。

ステップ 2　[Edit Remote Access Settings] を選択します。

[Edit Customer Support Remote Access] ページが表示されます。

図 15-2　[Edit Customer Support Remote Access] ページ



ステップ 3　[Allow remote access to this appliance] チェックボックスをオンにします。

ステップ 4　カスタマー サポート パスワードを入力します。

ステップ 5　カスタマー サポート エンジニアから変更指示がない限り、[Secure Tunnel] チェックボックスは選択状態のままにし、ポート番号も 25 のままにします。

ステップ 6　[Submit] をクリックし、[Commit] をクリックして変更を保存します。

リモート アクセスをイネーブルにすると、デバッグとシステムへの一般的なアクセスのために、カスタマー サポートが使用する特別なアカウントが有効になります。これは、Cisco IronPort カスタマー サポートがシステムの設定、設定の理解、および問題レポートの調査でお客様を補助するなどの作業に使用します。また、CLI で **techsupport** コマンドを使用することもできます。

セキュアなトンネルの使用をイネーブルにすると、アプライアンスが、指定されたポートを介してサーバ **upgrades.cisco.com** への SSH トンネルを作成します。デフォルトでは、この接続はポート 25 で行われます。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、このポートは大部分の環境で機能します。**upgrades.cisco.com** への接続が確立されたら、カスタマー サポートは SSH トンネルを使用してアプライアンスへのアクセスを取得できます。ポート 25 を介した接続が許可されている限り、これにより、大部分のファイアウォールの制限がバイパスされます。また、CLI で **techsupport tunnel** コマンドを使用することもできます。

リモート アクセス モードとトンネル モードの両方で、パスワードが必要です。これは、システムへのアクセスに使用されるパスワードではないことを理解しておくことが重要です。そのパスワードとシステムのシリアル番号がカスタマー サポート担当者に提供された後で、アプライアンスへのアクセスに使用されるパスワードが生成されます。

テクニカル サポート トンネルがイネーブルになると、**upgrades.cisco.com** に 7 日間接続されたままになります。7 日の経過後も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。SSH トンネル接続に設定されたタイムアウトはリモート アクセス アカウントに適用されません。リモート アクセス アカウントは、特に非アクティブ化するまでアクティブのままになります。

パケット キャプチャ

場合によっては、セキュリティ管理アプライアンスの問題発生時に Cisco IronPort カスタマー サポートに問い合わせたときに、セキュリティ管理アプライアンスとのネットワーク状況について尋ねられることがあります。セキュリティ管理アプライアンスでは、アプライアンスが接続されたネットワークで送受信されている TCP/IP と他のパケットを傍受および表示できます。

パケット キャプチャを実行して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したりする場合があります。

アプライアンスは、取り込んだパケット アクティビティをファイルに保存し、そのファイルをローカルに格納します。パケット キャプチャ ファイルの最大サイズ、パケット キャプチャの実行時間、およびキャプチャを実行するネットワーク インターフェイスを設定できます。また、フィルタを使用して、特定のポートからのトラフィックや特定のクライアントまたはサーバの IP アドレスからのトラフィックにパケット キャプチャを制限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 [Help and Support] > [Packet Capture] ページに、ハード ドライブ上に格納された完全なパケット キャプチャ ファイルの一覧が表示されます。パケット キャプチャ プロセスの実行中は、[Packet Capture] ページに、ファイル サイズや経過時間などの現在の統計情報を示すことにより、進行中のキャプチャのステータスが表示されます。

[Download File] ボタンを使用してパケット キャプチャ ファイルをダウンロードし、デバッグやトラブルシューティングのために電子メールで Cisco IronPort カスタマー サポートに転送できます。また、1 つまたは複数のファイルを選択して、[Delete Selected Files] をクリックすることにより、パケット キャプチャ ファイルを削除することもできます。

（注）　CLI では、**packetcapture** コマンドを使用します。このコマンドは、UNIX の **tcpdump** コマンドと類似しています。

パケット キャプチャの開始

パケット キャプチャを開始するには、次の 2 つの方法があります。

- 「コマンド ライン プロンプトからのパケット キャプチャの開始」（P.15-4）
- 「GUI からのパケット キャプチャの開始」（P.15-4）

コマンド ライン プロンプトからのパケット キャプチャの開始

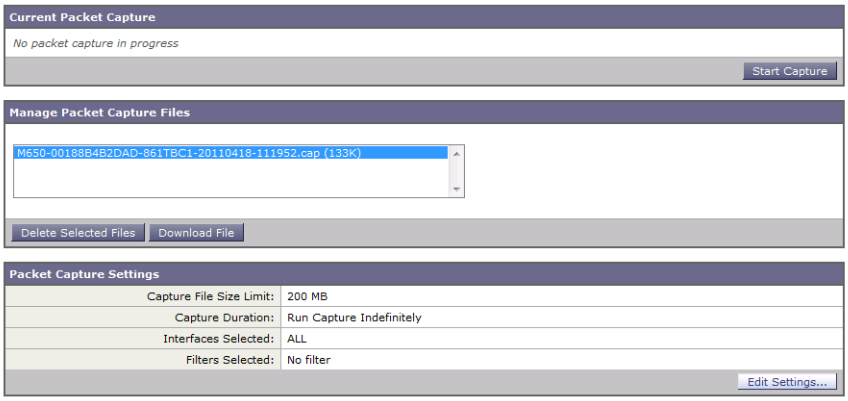
パケット キャプチャを開始するには、コマンド ライン プロンプトから **packetcapture > start** コマンドを入力します。実行中のパケット キャプチャを停止する必要がある場合は、**packetcapture > stop** コマンドを実行します。アプライアンスは、セッションが終了するとパケット キャプチャを停止します。

GUI からのパケット キャプチャの開始

セキュリティ管理アプライアンス上でパケット キャプチャを開始するには、次の手順を実行します。

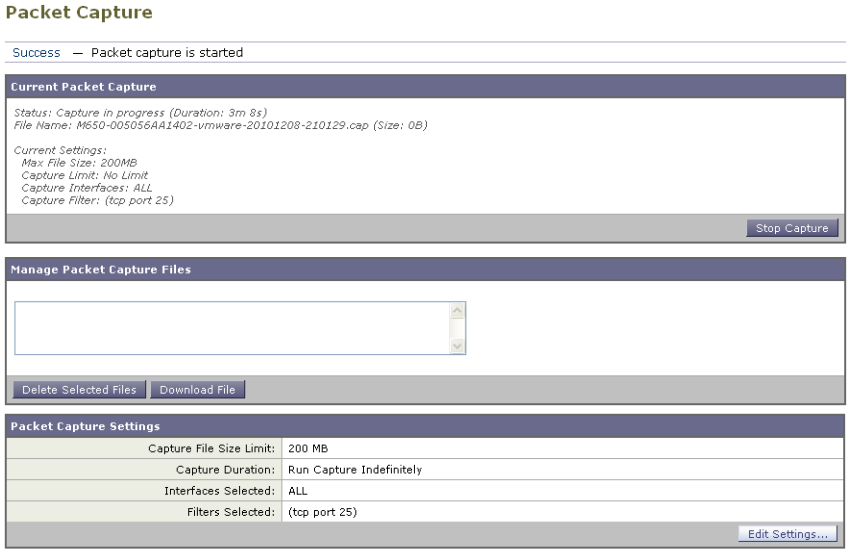
ステップ 1　セキュリティ管理アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

ステップ 2　[Packet Capture] ページが表示されます。



ステップ 3　[Start Capture] を選択します。

ステップ 4　次の図に、実行中のパケット キャプチャ プロセスを示します。



実行中のキャプチャを停止するには、[Stop Capture] をクリックします。以前に開始されたキャプチャは、セッション間で維持されます。

（注）　GUI では、GUI で開始されたパケット キャプチャだけが表示されます。**packetcapture > start** コマンドを使用してコマンド ライン プロンプトから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、コマンド ラインでは、**packetcapture > start** コマンドを使用してコマンド ライン プロンプトから開始された現在のパケット キャプチャの実行ステータスだけが表示されます。キャプチャは一度に 1 つだけ実行できます。

パケット キャプチャ設定の編集

パケット キャプチャ設定の編集には、次の 2 つの方法があります。

- 「コマンド ライン プロンプトからのパケット キャプチャ設定の編集」（P.15-6）

- 「GUI からのパケット キャプチャ設定の編集」（P.15-6）

コマンド ライン プロンプトからのパケット キャプチャ設定の編集

CLI でパケット キャプチャ設定を編集するには、コマンド ライン プロンプトから **packetcapture > setup** コマンドを実行します。

GUI からのパケット キャプチャ設定の編集

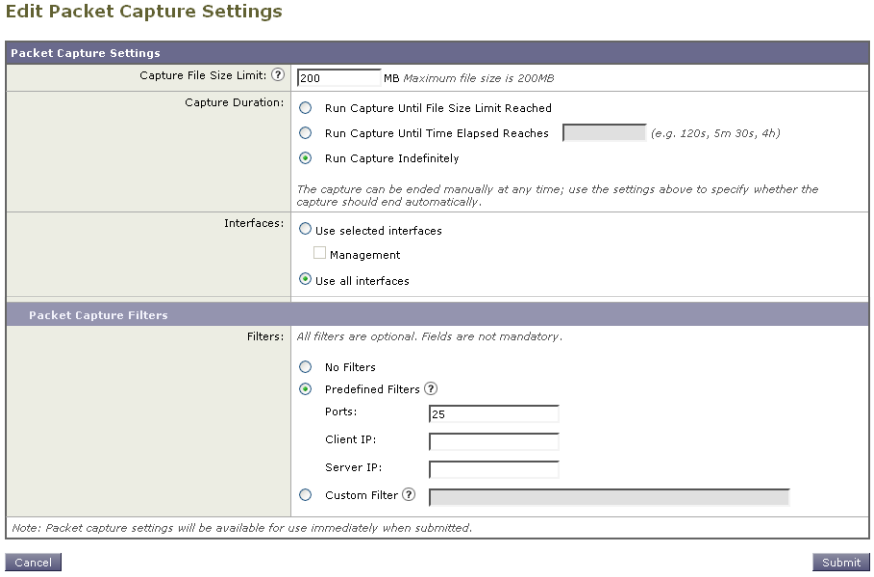
GUI からパケット キャプチャ設定を編集するには、次の手順を実行します。

ステップ 1　セキュリティ管理アプライアンス上で、[Help and Support] > [Packet Capture] を選択します。

パケット キャプチャ

ステップ 2　[Edit Settings] を選択します。

ステップ 3　[Edit Packet Capture Settings] ページが表示されます。



ステップ 4　表 15-1 に、設定可能なパケット キャプチャの項目を示します。

表 15-1　パケット キャプチャ設定オプション

オプション	説明
Capture file size limit	すべてのパケット キャプチャ ファイルの最大ファイル サイズ（メガバイト単位）。
Capture Duration	パケット キャプチャの実行時間を選択します。 • [Run Capture Until File Size Limit Reached]。パケット キャプチャは、ファイル サイズ制限に到達するまで実行されます。 • [Run Capture Until Time Elapsed Reaches]。パケット キャプチャは、設定された時間が経過するまで実行されます。時間は秒単位（s）、分単位（m）、または時間単位（h）で入力できます。単位を指定せずに時間の長さを入力すると、AsyncOS は、デフォルトで秒を使用します。このオプションは GUI でのみ使用できます。 **（注）** 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。全体の時間が経過する前にパケット 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。 • [Run Capture Indefinitely]。パケット キャプチャは、手動で停止するまで実行されます。 **（注）** 手動でパケット キャプチャを停止する前にパケット 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 キャプチャはいつでも手動で停止できます。
Interface	パケット キャプチャを実行するネットワーク インターフェイスを選択します。
Filters	パケット キャプチャで保存されるデータの量を削減するために、パケット キャプチャにフィルタを適用するかどうかを選択します。 事前定義されたフィルタを使用してポート、クライアント IP、またはサーバ IP（GUI のみ）でフィルタリングすることも、`host 10.10.10.10 && port 80` など、UNIX の **tcpdump** コマンドでサポートされる任意の構文を使用してカスタム フィルタを作成することもできます。

ステップ 5　[Submit] をクリックして、ページ上の変更を送信します。

（注） 新しいパケット キャプチャ設定を送信した後、AsyncOS でそれらが使用されます。この場合、変更を保存する必要はありません。