トラブルシューティング

以下のトピックは、Firepower システムで発生する可能性のある問題を診断する方法について説明します。

トラブルシューティングのベストプラクティス

- 問題の修正を試みるために変更を加える前に、トラブルシューティング ファイルを生成して元の問題をキャプチャします。トラブルシューティング用のヘルス モニター レポート （18 ページ）およびサブセクションを参照してください。

  サポートのために Cisco TAC に連絡する必要が生じた場合に、このトラブルシューティング ファイルが必要になることがあります。

- メッセージセンターのエラーメッセージと警告メッセージを調べて、調査を開始します。システムメッセージ （2 ページ）を参照してください

- お使いの製品の製品ドキュメント ページの「Troubleshoot and Alerts」という見出しの下にある、該当するテクニカル ノートとその他のトラブルシューティング リソースを探します。
- トラブルシューティング プロセス中は、複数のコマンドが同時に実行されるため、CPU の使用率が高くなります。トラブルシューティングは、ネットワーク トラフィック量やユーザー数が少ない期間に行うことを推奨します。

システムメッセージ

システムで発生した問題を突き止める必要がある場合、調査の出発点となるのはメッセージセンターです。メッセージセンターでは、システムがシステムのアクティビティとステータスに関して継続的に生成するメッセージを表示できます。

メッセージセンターを開くには、メインメニューの [展開（Deploy）] メニューの隣にある [システムステータス（System Status）] アイコンをクリックします。このアイコンは、システムのステータスによって以下のように表示されます。

- **エラー**（  ）：1 つ以上のエラーと任意の数の警告がシステム上に存在することを示します。
- [警告（warning）]（  ）：1 つ以上の警告がシステム上に存在することを示します。エラーは発生していません。
- [成功（success）]（  ）：警告とエラーはいずれもシステム上に存在していないことを示します。

アイコンに数字が表示されている場合、その数字は現在のエラー メッセージまたは警告メッセージの数を示します。

メッセージセンターを閉じるには、Web インターフェイス内でメッセージセンターの外側をクリックします。

メッセージ センターに加え、Web インターフェイスには、ユーザーのアクティビティおよび進行中のシステム アクティビティに応じて即時にポップアップ通知が表示されます。ポップアップ通知のなかには 5 秒経過すると自動的に非表示になるものや、**表示を消す**（  ）をクリックして明示的に表示を消さなければならない「スティッキー」通知もあります。通知リストの最上部にある [表示を消す（Dismiss）] リンクをクリックすると、すべての通知をまとめて非表示にすることができます。

ヒント スティッキー以外のポップアップ通知の上にマウスのカーソルを合わせると、その通知はスティッキーになります。

システムはユーザーのライセンス、ドメイン、アクセス ロールに基づいて、どのメッセージをポップアップ通知やメッセージ センターに表示するか決定します。

メッセージ タイプ

Message Center では、システムのアクティビティとステータスをレポートするメッセージが 3 つのタブに編成されて表示されます。

展開（Deployments）

このタブには、システムの各アプライアンスの設定展開に関連する現在のステータスがドメイン別にグループ化されて表示されます。システムでは、次の展開ステータス値がこのタブでレポートされます。[履歴の表示（Show History）] をクリックして、展開ジョブに関する追加情報を取得できます。

- [実行中（Running）]（**回転中**）：設定は展開の処理中です。
- [成功（Success）]：設定は正常に展開されました。
- [警告（warning）]（⚠）：警告展開ステータスは、**警告システムステータスアイコン**とともに表示されるメッセージ数に含まれます。
- [失敗（Failure）]：設定は展開に失敗しました。展開が必要な設定変更を参照してください。失敗した展開は、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。

アップグレード

このタブには、管理対象デバイスのソフトウェア アップグレード タスクに関連する現在のステータスが表示されます。システムでは、次のアップグレードステータス値がこのタブでレポートされます。

- [進行中（In progress）]：アップグレードタスクが進行中であることを示します。
- [完了（Completed）]：ソフトウェア アップグレード タスクが正常に完了したことを示します。
- [失敗（Failed）]：ソフトウェア アップグレード タスクが完了しなかったことを示します。

ヘルス（Health）

このタブには、システムの各アプライアンスの現在のヘルス ステータス情報がドメイン別にグループ化されて表示されます。ヘルス ステータスは、ヘルス モニタリングについてに記載されているように、ヘルス モジュールによって生成されます。システムでは、次の正常性ステータス値がこのタブでレポートされます。

- [警告（warning）]（⚠）：アプライアンス上のヘルスモジュールが警告制限を超え、問題が解決されていないことを示します。[ヘルスモニタリング（Health Monitoring）] ページには、これらの状態が**黄色い三角形**（⚠）で示されます。警告ステータスは、**警告システムステータスアイコン**とともに表示されるメッセージ数に含まれます。
- [クリティカル（Critical）]（❗）：アプライアンス上のヘルスモジュールが重大制限を超え、問題が解決されていないことを示します。[ヘルス モニタリング（Health

Monitoring）]ページには、これらの状態が[クリティカル（Critical）]（  ）アイコンで示されます。重大ステータスは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。

- **エラー**（）：アプライアンス上のヘルスモニタリングモジュールに障害が発生し、それ以降、正常に再実行されていないことを示します。[ヘルスモニタリング（Health Monitoring）] ページには、これらの状態が**エラーアイコン**で示されます。エラーステータスは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。

[ヘルス（Health）] タブのリンクをクリックして、[ヘルス モニタリング（Health Monitoring）] ページで関連の詳細情報を表示できます。現在のヘルス ステータス状態がない場合、[ヘルス（Health）] タブにメッセージは表示されません。

タスク

特定のタスク（設定のバックアップや更新のインストールなど）は、完了するまで時間がかかる可能性があります。このタブには、これらの長時間実行タスクのステータスが表示され、自分が開始したタスクや、適切なアクセス権がある場合は、システムの他のユーザーが開始したタスクが含まれることがあります。このタブには、各メッセージの最新の更新時間に基づいて時系列の逆順にメッセージが表示されます。一部のタスク ステータス メッセージには、問題となっているタスクについての詳細情報へのリンクが含まれています。システムでは、次のタスクステータス値がこのタブでレポートされます。

- [待機中（Waiting）]：別の進行中のタスクが完了するまで実行を待機しているタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [実行中（Running）]：進行中のタスクを示します。このメッセージ タイプでは、更新の経過表示バーが表示されます。
- [再試行中（Retrying）]：自動的に再試行しているタスクを示します。なお、すべてのタスクの再試行が許可されるわけではありません。このメッセージタイプでは、更新の経過表示バーが表示されます。
- [成功（Success）]：正常に完了したタスクを示します。
- [失敗（Failure）]：正常に完了しなかったタスクを示します。失敗したタスクは、**エラー システム ステータス アイコン**とともに表示されるメッセージ数に含まれます。
- [停止（Stopped）] または [中断（Suspended）]：システムアップデートのために中断されたタスクを示します。停止したタスクを再開することはできません。通常の動作が復元されたら、もう一度タスクを開始してください。
- [スキップ（Skipped）]：進行中のプロセスによって、タスクの開始が妨げられました。タスクの開始をもう一度試行してください。

新しいタスクが開始されると、新しいメッセージがこのタブに表示されます。タスクが完了すると（成功、失敗、または停止のステータス）、タスクを削除するまで、このタブには最終ステータスを示すメッセージが引き続き表示されます。[タスク（Tasks）]タブおよ

びメッセージデータベースがいっぱいにならないように、メッセージを削除することをお勧めします。

メッセージ管理

メッセージ センターから、以下を実行できます。

- ポップアップ通知の表示を選択します。
- システムデータベースからのタスクステータスメッセージをより多く表示します（削除されていないもので利用可能なものがある場合）。
- すべてのタスクマネージャ通知のレポートをダウンロードします。
- 個々のタスクのステータスメッセージを削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。
- タスクのステータスメッセージを一括で削除します。（これは、削除されたメッセージを確認できるすべてのユーザに影響します）。

ヒント シスコは、表示に加えてデータベースの不要なデータを削除するために、累積されたタスクのステータスメッセージを[タスク（Task）]タブから定期的に削除することを推奨します。データベースのメッセージ数が100,000に到達すると、削除したタスクのステータスメッセージが自動的に削除されます。

基本的なシステム情報の表示

[バージョン情報（About）]ページには、システムのさまざまなコンポーネントのモデル、シリアル番号、バージョン情報など、アプライアンスに関する情報が示されます。また、シスコの著作権情報も示されます。

手順

ステップ1 ページ上部のツールバーで、[ヘルプ（Help）]（  ）をクリックします。

ステップ2 [バージョン情報（About）]を選択します。

アプライアンス情報の表示

手順

[システム（System）]（⚙）>**[構成（Configuration）]**を選択します。

システムメッセージの管理

手順

ステップ1 [Notification（通告）]をクリックして、メッセージセンターを表示します。

ステップ2 次の選択肢があります。

- [展開（Deployments）]をクリックして、設定の展開に関連するメッセージを表示します。展開メッセージの表示 （7 ページ）を参照してください。展開メッセージを表示するには、管理者ユーザであるか、**デバイス設定の展開**権限が必要です。
- [アップグレード（Upgrades）]をクリックして、デバイスアップグレードタスクに関連するメッセージを表示します。「アップグレードメッセージの表示」を参照してください。「アップグレードメッセージの表示」を参照してください。これらのメッセージを表示するには、管理者ユーザーであるか、[更新（Updates）]権限が必要です。

  新しい推奨アップグレードバージョンが表示されます。[通知する（Remind Me）]オプションまたは[詳細（Details）]オプションを使用して、リマインダの設定または詳細情報の表示をそれぞれ選択できます。

- [正常性（Health）]をクリックして、Firewall Management Center とそれに登録したデバイスの状況に関連するメッセージを表示します。正常性メッセージの表示 （9 ページ）を参照してください。展開メッセージを表示するには、管理者ユーザーであるか、[正常性（Health）]権限が必要です。

  [正常性モニター（Health monitor）]リンクをクリックすると、[正常性モニター（Health Monitor）]ページに移動できます。

- [タスク（Tasks）]をクリックして、長時間実行タスクに関連するメッセージを表示または管理します。タスクメッセージの表示 （9 ページ）またはタスクメッセージの管理 （10 ページ）を参照してください。誰もがが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスクの表示**権限が必要です。[完了したタスクの削除（Remove completed tasks）]リンクをクリックすると、完了したタスクを通知から削除できます。
- [レポートのダウンロード（Download Report）]アイコンをクリックして、タスクマネージャにおけるすべての通知のレポートを生成します。[CSVのダウンロード（Download

CSV）] または [PDFのダウンロード（Download PDF）] を選択してレポートをダウンロードします。

- [通知を表示（Show Notifications）] スライダをクリックして、ポップアップ通知の表示を有効または無効にします。

展開メッセージの表示

展開メッセージを表示するには、管理者ユーザであるか、**デバイス設定の展開**権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [導入（Deployments）] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての展開ステータスを表示するには、[total] をクリックします。
- 任意の展開ステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- 展開の経過時間、開始時刻および停止時刻を表示するには、メッセージの時間経過インジケータ（たとえば、[1m 5s]）の上にカーソルを置きます。

ステップ 4 展開ジョブの詳細情報を表示するには、[show deployment history] をクリックします。

[展開の履歴（Deployment History）]テーブルには、左側の列に展開ジョブが新しい順にリストされています。

a) 展開ジョブを選択します。

右側の列のテーブルには、ジョブに含まれていた各デバイスと、デバイスごとの展開ステータスが表示されます。

b) デバイスからの応答、および展開中にデバイスに送信されたコマンドを表示するには、デバイスの [Transcript] カラムにあるダウンロードアイコンをクリックします。

トランスクリプトには、次のセクションが含まれています。

- [Snort を適用（Snort Apply）]：Snort 関連ポリシーから障害または応答が発生すると、メッセージがこのセクションに表示されます。通常、このセクションは空です。
- [CLIを適用（CLI Apply）]：このセクションは、Lina プロセスに送信されたコマンドを使用して設定される機能を対象にしています。
- [インフラストラクチャメッセージ（Infrastructure Messages）]：このセクションには、さまざまな導入モジュールのステータスが表示されます。

[CLIを適用（CLI Apply）] セクションでは、展開トランスクリプトには、デバイスに送信されたコマンド、およびデバイスから返された応答が含まれます。これらの応答は、通知メッセージやエラーメッセージの場合があります。失敗した展開では、コマンドを含むエラーを示すメッセージを探します。これらのエラーを調べることは、FlexConfig ポリシーを使用してカスタマイズされた機能を設定している場合に特に有用になる場合があります。これらのエラーは、コマンドを設定しようとしている FlexConfig オブジェクトのスクリプトを修正するのに役立つ場合があります。

（注）
管理対象機能に送信されるコマンドと、FlexConfig ポリシーから生成されるコマンドとの間のトランスクリプトには違いはありません。

たとえば、次のシーケンスは、論理名が outside の GigabitEthernet0/0 を設定するコマンドを Firewall Management Center が送信したことを示しています。デバイスは、自動的にセキュリティ レベルを 0 に設定したことを応答しました。Firewall Threat Defense は、何に対してもセキュリティレベルを使用しません。

```
========= CLI APPLY =========

FMC >> interface GigabitEthernet0/0
FMC >>  nameif outside
FTDv 192.168.0.152 >> [info] : INFO: Security level for "outside" set to 0 by default.
```

アップグレードメッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[更新（Updates）] 権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [アップグレード（Upgrades）] をクリックします。

ステップ 3 次を実行できます。

- 現在のすべてのアップグレードタスクを表示するには、[合計（Total）] をクリックします。
- 特定のステータスを持つメッセージのみを表示するには、そのステータスの値をクリックします。

- アップグレードタスクの詳細を表示するには、[デバイスの管理（Device Management）] をクリックします。

正常性メッセージの表示

展開メッセージを表示するには、管理者ユーザーであるか、[正常性（Health）] 権限が必要です。

手順

ステップ 1 [Notification（通告）] をクリックして、メッセージセンターを表示します。

ステップ 2 [正常性（Health）] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべての正常性ステータスを表示するには、[合計（total）] をクリックします。シビラティ（重大度）の内訳（つまり、警告、クリティカル、およびエラー）も表示されます。
- 任意のステータスに関するメッセージのみを表示するには、そのステータスの値をクリックします。
- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3日前（3 day(s) ago）]）の上にカーソルを置きます。
- 特定のメッセージの詳細な正常性ステータス情報を表示するには、メッセージをクリックします。
- [ヘルスモニタリング（Health Monitoring）] ページの完全な正常性ステータスを表示するには、[ヘルスモニター（Health Monitor）] をクリックします。

関連トピック

ヘルス モニタリングについて

タスクメッセージの表示

誰もがが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスクの表示**権限が必要です。

手順

ステップ 1 [通告（Notification）] をクリックして、メッセージセンターを表示します。

ステップ 2 [Tasks] をクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのタスクのステータスを表示するには、[Total] をクリックします。ステータス（待機中、実行中、再試行中、成功、失敗）に基づいてタスクを表示するには、それらをクリックします。
- 任意のステータスのタスクに関するメッセージのみを表示するには、そのステータスの値をクリックします。

（注）
停止したタスクのメッセージは、タスクのステータスメッセージの合計リストにのみ表示されます。停止したタスクではフィルタリングできません。

- メッセージが最も最近更新された時刻を表示するには、そのメッセージの相対時間インジケータ（たとえば [3 日前（3 day(s) ago）]）の上にカーソルを置きます。
- タスクに関する詳細を表示するには、メッセージ内のリンクをクリックします。
- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。

タスクメッセージの管理

誰もがが自分のタスクを表示できます。他のユーザのタスクを表示するには、管理者ユーザであるか、**他のユーザのタスクの表示**権限が必要です。

手順

ステップ 1 [System Status] アイコンをクリックして、メッセージセンターを表示します。

ステップ 2 [タスク（Tasks）] をクリックします。

ステップ 3 次の選択肢があります。

- さらにタスクのステータス メッセージが表示可能な場合は、メッセージ リストの下部にある [さらにメッセージを取得する（Fetch more messages）] をクリックして取得します。
- 完了したタスク（ステータスが停止、成功、または失敗のタスク）に関する 1 つのメッセージを削除するには、メッセージの横にある **削除**（×） をクリックします。
- すべての完了しているタスク（ステータスが停止、成功、または失敗のタスク）に関するメッセージをすべて削除するには、[総数（total）] でメッセージをフィルタリングして、[すべての完了タスクの削除（Remove all completed tasks）] をクリックします。
- すべての正常に完了したタスクに関するメッセージをすべて削除するには、[成功（success）] でメッセージをフィルタリングして、[すべての成功タスクの削除（Remove all successful tasks）] をクリックします。

- すべての失敗したタスクに関するメッセージをすべて削除するには、[失敗（failure）] でメッセージをフィルタリングして、[すべての失敗タスクの削除（Remove all failed tasks）] をクリックします。

ヘルスモニターアラートのメモリ使用率しきい値

メモリ使用率ヘルスモジュールは、アプライアンス上のメモリ使用率をモジュールに設定された制限と比較し、使用率がそのレベルを超えるとアラートを出します。このモジュールは、管理対象デバイスおよび Firewall Management Center 自体のデータをモニターします。

メモリー使用率の2つの設定可能なしきい値である「クリティカル」と「警告」は、使用されるメモリのパーセンテージとして設定できます。これらのしきい値を超えると、指定された重大度レベルでヘルスアラームが生成されます。ただし、ヘルスアラームシステムはこれらのしきい値を正確に計算しません。

高メモリデバイスでは、低メモリフットプリントデバイスよりも、特定のプロセスがシステムメモリ全体の大きな割合を使用することが予想されます。この設計では、物理メモリをできるだけ多く使用し、補助的なプロセス用に小さい値のメモリを解放します。

たとえば、32 GB のメモリを搭載したデバイスと 4 GB のメモリを搭載したデバイスを比較します。補助的なプロセスのために解放される 5 % のメモリは、32 GB のメモリを搭載したデバイスでは 1.6 GB、4 GB のメモリを搭載したデバイスでは 200 MB であり、前者の方がはるかに大きな値になります。

特定のプロセスによるシステムメモリの使用率が高いことを考慮して、Firewall Management Centerは、合計物理メモリと合計スワップメモリの両方を含めて合計メモリを計算します。そのため、ユーザーが設定するしきい値入力に対して適用されるメモリしきい値により、イベントの「値」列が、超過しきい値を特定するために入力された値と一致しないようなヘルスイベントが発生する可能性があります。

バージョン 7.4.1 以降、メモリ使用率正常性モジュールは、使用可能な空きメモリ、使用可能なスワップメモリ、およびバッファキャッシュを考慮してメモリ使用率を計算します。メモリ使用率正常性アラートの早すぎる生成を回避するために、警告およびクリティカルアラームのしきい値である 88% と 90% を超えないようにすることをお勧めします。

次の表は、搭載するシステムメモリに応じた、ユーザー入力のしきい値と適用されるしきい値の例を示しています。

（注） この表の値は一例です。この情報を使用して、ここに示されている搭載 RAM と一致しないデバイスのしきい値を推定することができます。また、より正確なしきい値の計算についてCisco TAC に問い合わせることもできます。

表 *1:* 搭載する *RAM* に基づくメモリ使用率しきい値

ユーザー入力しきい値	搭載するメモリ（RAM）ごとの適用しきい値			
	4 GB	**6 GB**	**32 GB**	**48 GB**
10%	10%	34 %	72%	81 %
20 %	20 %	41%	75%	83 %
30%	30%	48 %	78%	85 %
40%	40%	56 %	81 %	88 %
50%	50 %	63 %	84 %	90%
60 %	60 %	70%	88 %	92%
70%	70%	78%	91 %	94%
80%	80%	85 %	94%	96%
90 %	90 %	93%	97%	98%
100 %	100 %	100 %	100 %	100 %

注意 Firewall Management Center がクリティカルシステムメモリ状態に達すると、システムは、メモリ使用量の多いプロセスを終了したり、高いメモリ使用率が続く場合には Firewall Management Center を再起動する可能性があります。

障害モニタリング

Firewall Threat Defense の障害マネージャは、デバイスのさまざまな種類の障害をモニターし、障害が発生した際にデバイスを回復します。現在は、FlexConfig コマンドを使用して障害モニターを設定し、ブロックの枯渇をモニターして、ブロックの枯渇からデバイスを回復することができます。デバイスで FlexConfig ポリシーを作成して適用する方法については、『Cisco Secure Firewall Management Center デバイス構成ガイド』の「FlexConfig Policies」の章を参照してください。

HA では、デバイスでのブロックの枯渇が確認されると、アクティブデバイスが障害状態に移行し、他のスタンバイが引き継ぎます。このスイッチオーバーにより、ダウンタイムとパケットのドロップが減少します。障害が発生したピアはログを送信するので、show tech を使用してブロックの枯渇の原因を診断およびデバッグします。

ブロックの枯渇のモニタリングを有効または無効にするには、次のコマンドを使用して FlexConfig オブジェクトを作成します。

```
fault-monitor block-depletion recovery-action {none | reload}
fault-monitor block-depletion monitor-interval <monitor-interval>
```

デバイスの回復オプションを設定するには、リロードするかしないかをFlexConfigオブジェクトで定義します。デバイスでブロックプールの枯渇が検出された場合、デバイスのリロードが唯一の回復方法であるため、デフォルトの回復アクションはreloadです。noneオプションを使用してデバイスのリロードを回避する場合は、Cisco TAC チームの指示に従い、慎重に行う必要があります。通常は、誤検出のブロック検出がある場合、またはデバイスで自動リロードを行う前に TAC チームが追加データを収集する必要がある場合に、none が使用されます。

障害モニターが設定されている場合、プールの空きブロックが使い果たされ、システム定義の30分のモニター間隔にわたってゼロのままである場合に、指定されたブロックプールは枯渇していると見なされ、回復アクションが実行されます。このオプションは、誤検出が確認された場合にモニター間隔の期間を変更するために TAC によって使用されます。

例

```
fault-monitor block-depletion monitor-interval 30
```

設定をクリアするには、次のコマンドを使用して FlexConfig オブジェクトを定義します。

```
clear configure fault-monitor block-depeletion
```

ディスク使用率とイベントドレインの正常性モニターアラート

Disk Usage正常性モジュールは、管理対象デバイスのハードドライブとマルウェア ストレージ パック上のディスク使用率をモジュールに設定された制限と比較し、その使用率がモジュールに設定されたパーセンテージを超えた時点でアラートを出します。また、モジュールしきい値に基づいて、システムが監視対象のディスク使用カテゴリ内のファイルを過剰に削除する場合、または、これらのカテゴリを除くディスク使用率が過剰なレベルに達した場合にもアラートを出します。

このトピックでは、Disk Usage正常性モジュールによって生成される未処理イベントのドレイン正常性アラートの症状とトラブルシューティングのガイドラインについて説明します。

ディスクマネージャのプロセスは、デバイスのディスク使用率を管理します。ディスクマネージャによってモニターされる各タイプのファイルには、サイロが割り当てられます。システムで使用可能なディスク容量に基づいて、ディスクマネージャは各サイロの最高水準点（High Water Mark、HWM）と最低水準点（Low Water Mark 、LWM）を計算します。

システムの各部分のディスク使用率の詳細情報（サイロ、LWM、HWM など）を表示するには、**show disk-manager** コマンドを使用します。

例

次に、ディスクマネージャ情報の例を示します。

```
> show disk-manager
Silo                                Used        Minimum     Maximum
Temporary Files                     0 KB        499.197 MB  1.950 GB
Action Queue Results                0 KB        499.197 MB  1.950 GB
User Identity Events                0 KB        499.197 MB  1.950 GB
UI Caches                           4 KB        1.462 GB    2.925 GB
Backups                             0 KB        3.900 GB    9.750 GB
Updates                             0 KB        5.850 GB    14.625 GB
Other Detection Engine              0 KB        2.925 GB    5.850 GB
Performance Statistics              33 KB       998.395 MB  11.700 GB
Other Events                        0 KB        1.950 GB    3.900 GB
IP Reputation & URL Filtering       0 KB        2.437 GB    4.875 GB
Archives & Cores & File Logs        0 KB        3.900 GB    19.500 GB
Unified Low Priority Events         1.329 MB    4.875 GB    24.375 GB
RNA Events                          0 KB        3.900 GB    15.600 GB
File Capture                        0 KB        9.750 GB    19.500 GB
Unified High Priority Events        0 KB        14.625 GB   34.125 GB
IPS Events                          0 KB        11.700 GB   29.250 GB
```

正常性アラートの形式

Firewall Management Center の正常性モニタープロセスが実行されると（5 分ごとに 1 回、または手動実行がトリガーされると）、ディスク使用状況モジュールは diskmanager.log ファイルを調べ、該当する条件が満たされると、正常性アラートがトリガーされます。

正常性アラートの構造は、「Drain of unprocessed events from <*SILO NAME*>」です。

たとえば、「Drain of unprocessed events from Low Priority Events」のようになります。

重要 イベントサイロのみが Drain of unprocessed events from <SILO NAME> 正常性アラートを生成します。このアラートの重大度レベルは常に **[重大（Critical）]** です。

アラート以外のその他の症状には、次のものがあります。

- Firewall Management Center ユーザーインターフェイスの速度低下
- イベントの喪失

一般的なトラブルシューティング シナリオ

Drain of unprocessed events of <SILO NAME> 正常性アラートは、イベント処理パスのボトルネックが原因で発生します。

これらのディスク使用率アラートに関して、次の 3 つのボトルネックが存在する可能性があります。

- 過剰なロギング：Firewall Threat Defense の EventHandler プロセスがオーバーサブスクライブされています（Snort の書き込みよりも読み取りが遅い）。
- Sftunnel ボトルネック：イベント用インターフェイスが不安定またはオーバーサブスクライブ状態です。

- SFDataCorrerator のボトルネック：Firewall Management Center と管理対象デバイス間のデータ伝送チャネルがオーバーサブスクライブ状態です。

過剰なロギング

このタイプの正常性アラートの最も一般的な原因の 1 つは、過剰な入力です。**show disk-manager** コマンドから収集された最低水準点（LWM）と最高水準点（HWM）の差は、該当サイロが LWM（新たにドレインされた状態）から HWM 値に移行するまでに使用できる容量を示しています。未処理のイベントのドレインがある場合は、ロギング設定を確認してください。

- ダブルロギングを確認する：Firewall Management Center でコリレータ *perfstats* を調査すると、ダブルロギングのシナリオを特定できます。

```
admin@FMC:~$ sudo perfstats -Cq < /var/sf/rna/correlator-stats/now
```

- ACP のロギング設定を確認する：アクセス コントロール ポリシー（ACP）のロギング設定を確認します。ロギング設定に接続の「開始」と「終了」の両方が含まれている場合は、イベントの数を減らすために、終了のみをログに記録するように設定を変更します。

  接続のロギングのベストプラクティスに記載されているベストプラクティスに従っていることを確認します。

通信のボトルネック：Sftunnel

Sftunnel は、Firewall Management Center と管理対象デバイス間の暗号化通信を担当します。イベントはトンネルを介して Firewall Management Center に送信されます。管理対象デバイスと Firewall Management Center 間の通信チャネル（sftunnel）の接続性の問題や不安定性は、次の原因が考えられます。

- Sftunnel がダウンしているか、不安定（フラッピングしている）。

  Firewall Management Center と管理対象デバイスが、TCP ポート 8305 の管理インターフェイス間で到達可能であることを確認します。

  sftunnel プロセスは安定している必要があり、予期せず再起動することがあってはいけません。これを検証するには、**/var/log/message** ファイルを確認し、文字列 ***sftunneld*** を含むメッセージを検索します。

- Sftunnel がオーバーサブスクライブされている。

  正常性モニターからのトレンドデータを確認し、Firewall Management Center の管理インターフェイスのオーバーサブスクリプションの兆候を探します。この徴候には、管理トラフィックのスパイクや一定したオーバーサブスクリプションなどがあります。

  イベントのセカンダリ管理インターフェイスとして使用します。このインターフェイスを使用するには、Firewall Threat Defense CLI で **configure network management-interface** コマンドを使用して、IP アドレスなどのパラメータを設定する必要があります。

通信のボトルネック：SFDataCorrerator

SFDataCorrerator は、Firewall Management Center と管理対象デバイス間のデータ伝送を管理します。 Firewall Management Center では、システムによって作成されたバイナリファイルを分析して、イベント、接続データ、およびネットワークマップを生成します。最初のステップでは、**diskmanager.log** ファイルを調べて、次のような重要な情報を収集します。

- ドレインの頻度。
- 未処理イベントを含むファイルがドレインされた数。
- 未処理イベントによるドレインの発生。

ディスクマネージャプロセスが実行されるたびに、各サイロのエントリが独自のログファイルに生成されます。エントリは、**[/ngfw]/var/log/diskmanager.log** 下に存在します。diskmanager.log（CSV形式）から収集された情報は、原因の検索を絞り込むために使用できます。

その他のトラブルシューティング手順：

- コマンド **stats_unified.pl** は、Firewall Management Center に送信する必要があるデータが管理対象デバイスにあるかどうかを判断するのに役立ちます。この状態は、管理対象デバイスと Firewall Management Center で接続の問題が生じた場合に発生する可能性があります。管理対象デバイスは、ログデータをハードドライブに保存します。

  ```
  admin@FMC:~$ sudo stats_unified.pl
  ```

- **manage_proc.pl** コマンドは、Firewall Management Center 側のコリレータを再設定できます。

  ```
  root@FMC:~# manage_procs.pl
  ```

Cisco TAC へのお問い合わせの前に

Cisco TAC に連絡する前に、次の項目を収集することを強く推奨します。

- 表示される正常性アラートのスクリーンショット。
- Firewall Management Center から生成されたトラブルシュートファイル。
- 影響を受ける管理対象デバイスから生成されたトラブルシュートファイル。
- 問題が最初に検出された日時。
- ポリシーに最近加えられた変更に関する情報（該当する場合）。
- 通信のボトルネック：SFDataCorrerator （16 ページ） で説明されている stats_unified.pl コマンドの出力。

デバイス設定履歴ファイルのディスク使用量

[ディスク使用量（Disk Usage）] 正常性モジュールは、Firewall Management Center 上のデバイス設定履歴ファイルのサイズをモニターし、サイズが許容制限を超えると正常性アラートを送

信します。デバイス設定履歴ファイルの保存に関する最大許容ディスクサイズは20GBです。Firewall Management Centerの高可用性展開では、この正常性アラートは、高可用性同期が一時停止されている場合にのみスタンバイ Firewall Management Center に表示されます。

デバイス設定履歴ファイルのサイズが許容制限を超えると、Firewall Management Centerのアップグレード中にアップグレードの準備に失敗する可能性があります。Firewall Management Centerの高可用性展開では、デバイス設定履歴ファイルのサイズ制限を超えると、高可用性同期速度が低下する可能性があります。

デバイス設定履歴ファイルサイズの正常性アラートを解消するには、**[展開（Deploy）]** > **[展開履歴（Deployment History）]** > **[展開設定（Deployment Setting）]** > **[設定バージョンの設定（Configuration Version Setting）]** を選択し、[保持するバージョンの数（Number of Versions to Retain）] を減らします。バージョンの数を減らすと、選択したバージョンサイズと一致するように最も古い設定バージョンが削除されます。[設定バージョンの推定サイズ（Estimated Configuration Version Size）] は、保持することを選択したバージョンの数に基づいて、Firewall Management Center 上の設定履歴ファイルのおおよそのサイズを提供します。推定値を使用してバージョンの数を変更し、設定バージョンのサイズを許容制限未満に減らします。

詳細については、『Cisco Secure Firewall Management Center デバイス設定ガイド』の「設定バージョン番号の設定」を参照してください。

ディスク容量のクリア

ディスク容量が少ないと、管理センターおよび管理対象の脅威防御デバイスのパフォーマンスが低下する可能性があります。ディスク容量が少なくなると、パフォーマンスが低下することや、アップグレードの妨げになる可能性があり、容量を回復しようとして重要なファイルを誤って削除するリスクが増大します。管理センターまたは脅威防御デバイスから次の一時ファイルを削除して、ディスク容量を解放できます。

- **バックアップファイル**：保存されたバックアップ設定ファイルです。詳細については、「管理センターまたは管理対象デバイスのバックアップ」を参照してください。
- **コンテンツのアップデート**：SRU、VDB、およびGeoDB更新ファイルが含まれます。詳細については、「システムアップデートについて」を参照してください。
- **トラブルシューティング ファイル**：これらはトラブルシューティングの目的で生成されるログ ファイルです。詳細については、「トラブルシューティング用のヘルス モニター レポート」を参照してください。

ディスク容量がクリアされると、システムは最新のファイルを保持し、古いファイルをすべて削除します。

⚠

注意 ディスク容量のクリアにより、選択されたファイルは完全に削除されます。

手順

ステップ 1 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]**を選択します。

ステップ 2 左側のナビゲーションウィンドウで、ディスク容量をクリアするデバイスをクリックします。管理センターのディスク容量をクリアする場合は、**[ファイアウォール管理センター（Firewall Management Center）]**をクリックします。

ステップ 3 **[ディスク使用量（Disk Usage）]** ウィジェットで、**[ディスク領域のクリア（Clear disk space）]** をクリックします。

ステップ 4 チェックボックスをオンにして、削除する一時ファイルのタイプを選択します。

ステップ 5 **[ディスク容量のクリア（Clear disk space）]**。

ステップ 6 **[クリア（Clear）]** をクリックします。

メッセージ センターでディスク クリーンアップ タスクの進行状況を確認します。タスクが完了すると、**[ディスク使用状況（Disk Usage）]** ウィジェットに更新されたストレージデータが表示されます。

トラブルシューティング用のヘルス モニター レポート

アプライアンスで問題が発生したときに、問題の診断に役立つように、サポートからトラブルシューティング ファイルを提供するように依頼されることがあります。システムは、特定の機能分野を対象とした情報を含むトラブルシューティング ファイルと、高度なトラブルシューティング ファイル（このファイルはサポートと連携して取得します）を生成することができます。次の表に示すオプションのいずれかを選択して、特定の機能のトラブルシューティング ファイルの内容をカスタマイズできます。

一部のオプションは報告対象のデータの点で重複していますが、トラブルシューティング ファイルには、オプションの選択に関係なく冗長コピーは含まれません。

表 *2:* 選択可能なトラブルシュート オプション

オプション	報告内容
Snort のパフォーマンスと設定（Snort Performance and Configuration）	アプライアンス上の Snort に関連するデータと構成設定
ハードウェア パフォーマンスとログ（Hardware Performance and Logs）	アプライアンス ハードウェアのパフォーマンスに関連するデータとログ
システムの設定、ポリシー、ログ（System Configuration, Policy, and Logs）	アプライアンスの現在のシステム設定に関連する構成設定、データ、およびログ

オプション	報告内容
検知機能の構成、ポリシー、ログ（Detection Configuration, Policy, and Logs）	アプライアンス上の検知機能に関連する構成設定、データ、およびログ
インターフェイスとネットワーク関連データ（Interface and Network Related Data）	アプライアンスのインラインセットとネットワーク設定に関連する構成設定、データ、およびログ
検知、認識、VDB データ、およびログ（Discovery, Awareness, VDB Data, and Logs）	アプライアンス上の現在の検出設定と認識設定に関連する構成設定、データ、およびログ
データおよびログのアップグレード（Upgrade Data and Logs）	アプライアンスの以前のアップグレードに関連するデータおよびログ
All Database Data	トラブルシュート レポートに含まれるすべてのデータベース関連データ
All Log Data	アプライアンス データベースによって収集されたすべてのログ
ネットワーク マップ情報	現在のネットワーク トポロジ データ

特定のシステム機能のトラブルシューティング ファイルの生成

カスタマイズしたトラブルシューティング ファイルを生成およびダウンロードして、そのファイルをサポートに送信できます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティ アナリスト ユーザー（読み取り専用）である必要があります。

手順

ステップ 1 デバイス正常性モニターの表示の手順を実行します。

ステップ 2 [システム（System）]（⚙）>**[正常性（Health）]**>**[モニタ（Monitor）]** を選択し、左側のパネルでデバイスをクリックして、**[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]**、**[トラブルシューティング ファイルの生成（Generate Troubleshooting Files）]** の順にクリックします。

（注）

- Firewall Management Center Web インターフェイスから生成されたトラブルシューティング ファイルは Firewall Management Center に保存されます。各アプライアンスの最新のトラブルシューティング ファイルのみが保存されます。
- CLI から生成されたトラブルシューティング ファイルはローカルに保存され、上書きされることはありません。

ステップ 3 タスクメッセージの表示 （9 ページ） で説明されているように、**[全データ（All Data）]** を選択して生成可能なすべてのトラブルシューティングデータを生成することも、個別のボックスをオンにすることもできます。

ステップ 4 [生成（Generate）] をクリックします。

ステップ 5 Message Center でタスクのメッセージを表示します。タスクメッセージの表示 （9 ページ） を参照してください。

ステップ 6 生成されたトラブルシューティング ファイルに対応するタスクを探します。

ステップ 7 アプライアンスがトラブルシューティング ファイルを生成して、タスク ステータスが [完了（Completed）] に変わったら、[クリックして生成されたファイルを取得（Click to retrieve generated files）] をクリックします。

ステップ 8 ブラウザのプロンプトに従ってファイルをダウンロードします。(トラブルシューティング ファイルは、1 つの `.tar.gz` ファイルでダウンロードされます)。

ステップ 9 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

高度なトラブルシューティング ファイルのダウンロード

トラブルシューティング ファイルをダウンロードできます。

始める前に

このタスクを実行するには、管理者ユーザー、メンテナンスユーザー、またはセキュリティアナリスト ユーザー（読み取り専用）である必要があります。

手順

ステップ 1 アプライアンスの正常性モニターを表示します。、デバイス正常性モニターの表示を参照してください。

ステップ 2 [システム（System）] （⚙） > **[正常性（Health）]** > **[モニター（Monitor）]** の順に選択し、左側のパネルでデバイスをクリックして、[システムおよびトラブルシューティングの詳細を表示（View System & Troubleshoot Details）]、[高度なトラブルシューティング（Advanced Troubleshooting）] の順にクリックします。

ステップ 3 [ファイルのダウンロード（File Download）] で、サポートから提供されたファイル名を入力します。

ステップ 4 [ダウンロード（Download）] をクリックします。

ステップ 5 ブラウザのプロンプトに従ってファイルをダウンロードします。

（注）
管理対象デバイスでは、システムはファイル名の前にデバイス名を付加してファイル名を変更します。

ステップ 6 サポートの指示に従って、トラブルシューティング ファイルを Cisco に送信してください。

Secure Firewall Management Center でのトラブルシューティング Syslog の表示

Firewall Threat Defense デバイスでトラブルシューティング syslog をログに記録し、Firewall Management Center に送信できます。データをロギングすることで、ネットワークの問題またはデバイス設定の問題を特定して分離できます。ロギングを有効にすると、Firewall Threat Defense デバイスから Firewall Management Center に VPN Syslog が送信され、分析されて保管されます。

ターゲットデバイスの Firewall Threat Defense プラットフォーム設定ポリシーの [Cisco Secure Firewall Management Center へのロギング（Logging to Secure Firewall Management Center）] オプションを編集することで、ロギングとメッセージのシビラティ（重大度）を管理できます。ロギングの有効化、syslog サーバーの設定、およびシステムログの表示の詳細については、Cisco Secure Firewall Management Center デバイス構成ガイド の「*Threat Defense* デバイスの *Syslog* ロギングの設定」を参照してください。

すべてのトラブルシューティングログ

Firewall Threat Defense デバイスを設定して、すべての診断 syslog を Management Center に記録し、それらを [統合イベント（Unified Events）] テーブルの他のイベント（とともに [トラブルシュートイベント（Troubleshoot Events）] として表示します（**[分析（Analysis）] > [統合イベント（Unified Events）]**）。[統合イベント（Unified Events）] テーブルを使用して、トラブルシューティングログをリアルタイムで確認し、トラブルシューティングの実行中にそれらを最近のデバイス設定の変更と関連付けることができます。同じテーブルの他のイベントタイプでログをフィルタリングおよび分析して、Firewall Threat Defense デバイスのインサイトを取得し、トラブルシューティングを実行できます。

[トラブルシュートイベント（Troubleshoot Events）] の表示の詳細については、統合イベントの使用 を参照してください。

[重大（Critical）]、[アラート（Alerts）]、[緊急（Emergencies）] のすべてのトラブルシューティング syslog を Firewall Management Centerに送信することを選択できます。

VPN トラブルシューティングログ

VPN トラブルシューティング Syslog のみを分析用に Firewall Management Center に送信するように Firewall Threat Defense デバイスを設定します。VPN Syslog は、デフォルトのシビラティ（重大度）レベルである [エラー（Errors）] またはより高いシビラティレベルとともに表示されます（変更されていない限り）。VPN ログのロギングレベルを [エラー（Errors）] に設定することをお勧めします。VPN ロギングレベルを 4 以下の重大度（[警告（Warnings）]、[通知（Notification）]、[情報（Infromational）]、または [デバッグ（Debugging）]）に設定すると、Firewall Management Center が過負荷になる可能性があります。

（注） サイト間 VPN またはリモートアクセス VPN を設定してデバイスを設定すると、デフォルトで自動的に VPN syslog が Firewall Management Center に送信されます。

トラブルシューティング Syslog の表示

Firewall Threat Defense デバイスは、デバイス設定の問題や VPN の問題の原因に関する追加情報を収集するのに役立つイベント情報をキャプチャします。デフォルトでは、行は [時間（Time）] 列でソートされています。

始める前に

- Firewall Threat Defense プラットフォーム設定で **[Secure Firewall Management Center へのロギング（Logging to Secure Firewall Management Center）]** Cisco Security Cloud Control のファイアウォールオプションを設定することにより、ロギングを有効にします。詳細については、Cisco Secure Firewall Management Center デバイス構成ガイドの「*Enable Logging and Configure Basic Settings*」を参照してください。
- このタスクを実行するには、リーフドメインの管理者ユーザーである必要があります。

手順

ステップ 1 **[デバイス（Devices）]** > **[トラブルシューティング（Troubleshoot）]** > **[トラブルシューティングログ（Troubleshooting Logs）]** を選択します。

ステップ 2 次の選択肢があります。

- 検索：現在のメッセージ情報をフィルタリングするには、[検索の編集（Edit Search）] をクリックします。
- 表示：選択したメッセージに関連付けられた VPN の詳細をビューに表示するには、[表示（View）] をクリックします。
- すべて表示：すべてのメッセージの VPN の詳細をビューに表示するには、[すべて表示（View All）] をクリックします。
- 削除：選択したメッセージをデータベースから削除するには [削除（Delete）] をクリックするか、またはすべてのメッセージを削除するには [すべて削除（Delete All）] をクリックします。

次のタスク

すべてのトラブルシューティング syslog を Management Center に送信する場合、ログに記録された**トラブルシューティング イベント**をリアルタイムで、他のセキュア ファイアウォール イ

ベント タイプとともに表示するには、**[分析（Analysis）]** > **[統合イベント（Unified Events）]** をクリックします。

Cisco RADKit 統合による高度なトラブルシューティング エクスペリエンス

Cisco Remote Automation Development Kit（RADKit）は、シスコのサポート エンジニアがシステムの問題を診断およびトラブルシューティングするためにネットワーク デバイスに安全にアクセスできるように設計された、ネットワーク全体のオーケストレータです。RADKitをリモートサーバにインストールし、そのサービスを Firewall Management Center およびその管理対象 Firewall Threat Defense デバイスと統合することで、問題の診断に必要なデータを自動的に利用できるようにすることができます。

RADKit と Firewall Management Center を統合すると、次のことが可能になります。

- Firewall Management Center および Firewall Threat Defense デバイスにリモートでアクセスします。
- 設定の不一致やハードウェアの問題を診断するために、Firewall Management Center および Firewall Threat Defense デバイスへの制御されたアクセス権を持つエンジニアを割り当てます。
- 自動化機能を活用して、診断データを収集して問題を分析します。
- 以前のセッションに移動し、すべての操作ログを表示し、アーカイブ ファイルとしてダウンロードします。

RADKit サービスの登録

RADKit サービスを SSO に登録します。これにより、RADKit クライアントとの接続が確立されます。

始める前に

HTTP プロキシを使用する場合は、サービスを正常に登録するため RADKit サービスを有効にする前に、管理センターでプロキシを設定します。

手順

ステップ 1 **[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[リモート診断（Remote Diagnostics）]**を選択します。

ステップ 2 RADKit クラウドにサービスを登録するには、**[RADKit サービスの有効化（Enable the RADKit service）]** トグルボタンをクリックし、**[SSO での登録（Enroll with SSO）]**をクリックします。

ステップ 3 電子メール アドレス（ドメイン名を含む）を入力し、**[送信（Submit）]**をクリックします。

（注）
同じ電子メール ID を使用して短期間に複数回登録することはできません。登録するたびに、電子メール ID アカウントに対して新しい証明書が生成されます。同じユーザー アカウントに対して複数の証明書を作成するのは効率的ではありません。したがって、RADKit クラウドでは、ユーザーごとに発行される証明書の数を 6 ヵ月間で 12 の新しいサービス ID に制限します。

ステップ 4 SSO プロセスを完了します。

ステップ 5 **[Cisco RADKit アクセス（Cisco RADKit Access）]** ページで、**[承認（Accept）]**をクリックします。
登録後、ページに成功メッセージとトークン ID が表示されます。

ステップ 6 （オプション）サービスを無効にするには、**[RADKit サービスの無効化（Disable the RADKit service）]** トグルボタンをクリックします。

注意
サービスを無効化すると、関連するすべてのデータと既存の許可が失われます。

RADKit サービス承認の管理

TAC エンジニアがトラブルシューティングのためにデバイスにリモート アクセスできるようにすることで、承認を管理できます。また、リモートユーザーに、特定の期間だけ、すべてのデバイスのインベントリにアクセスさせることも、選択したデバイスだけにアクセスさせることもできます。

（注） 承認の追加と表示は、グローバル ドメインからのみ行うことができます。

始める前に

RADKit サービスに登録します。登録の手順については、RADKit サービスの登録 （23 ページ） を参照してください。

手順

ステップ 1 **[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[リモート診断（Remote Diagnostics）]**を選択します。

[リモート診断（Remote Diagnostics）] ページに、現在の承認が表示されます。RADKit サービスに登録していることを確認します。

ステップ 2 新しい承認を作成するには、**[新しい承認の作成（Create New Authorization）]** タブをクリックします。

ステップ 3 **[承認のセットアップ（Setup Authorization）]**で、サポート エンジニアの電子メールアドレスを入力します。電子メール アドレスの最大長は40文字です。

（注）
- サポートエンジニアの電子メールアドレスは、承認レコードに対して一意です。したがって、承認の作成後にこの値を変更することはできません。
- 同じ電子メール アドレスに対して承認アカウントを作成することはできません。

ステップ 4 [次へ（Next）] をクリックします。

ステップ 5 **[デバイスの選択（Device Selection）]** で、サポート エンジニアがアクセスできるデバイスと Firewall Management Center を指定します。関連するオプションを選択します。

- **[すべてのデバイスへのアクセスを許可（Grant access to all devices）]**：このラジオ ボタンをクリックし、**[すべてのデバイスへのアクセスに同意する（I agree to provide access to all devices）] チェックボックスをオンにして、** すべてのデバイスと Firewall Management Centerにアクセスを許可することに同意します。
- **[特定のデバイスへのアクセスを許可（Grant access to specific devices）]**：このラジオ ボタンをクリックし、**[デバイスの選択（Select Devices）]** ドロップダウン リストから、サポート エンジニアがアクセスできるデバイスの IP アドレスと Firewall Management Center を選択します。**[すべてのデバイスへのアクセスに同意する（I agree to provide access to the selected devices）]** チェック ボックスがオンになっていることを確認してください。

  （注）
  バージョン7.7以降を実行しているデバイスのみがサポートされており、選択可能になっています。

ステップ 6 [次へ（Next）] をクリックします。

ステップ 7 **[アクセスのスケジュール（Schedule the Access）]** で、サポート エンジニアがデバイスにアクセスできるタイムラインを指定します。

- **[今（Now）]**：このラジオボタンをクリックし、**[期間（Duration）]** フィールドでアクセスを許可する期間を指定します。期間のプリセットを設定するには、**[時間のプリセット（Time presets）]** リンク（1 時間、6 時間、12 時間、1 日、または 1 週間）をクリックします。
- デバイスへの永続的なアクセスを許可するには、**[取り消すまでアクセスを許可（Grant access until revoke ）]**：このラジオ ボタンをクリックします。

  （注）
  アクセスを取り消すには、**[現在の承認（Current Authorizations）]** グリッドで、**[アクション（Actions）]** 列の下にあるそれぞれの取り消しアイコンをクリックします。

ステップ 8 **[サマリー（Summary）]**で、承認アカウントに対して行った選択内容をプレビューします。選択した内容を変更するには、[編集（Edit）]アイコンをクリックし、対応する変更を行います。

（注）
サポート エンジニアの電子メール アドレスは、承認レコードに対して一意です。そのため、電子メール アドレスを変更することはできません。

ステップ 9 [作成（Create）] をクリックします。

後続のウィンドウに、RADKit クライアントで使用されるユーザーの電子メール アドレスと RADKit サービス ID を含む新しい承認の確認メッセージが表示されます。

ステップ 10 （オプション）別の承認を作成するには、**[別の承認の作成（Create Another Authorization）]** をクリックします。

ステップ 11 ウィンドウを終了するには、**[閉じる（Close）]** をクリックします。

次のタスク

[リモート診断（Remote Diagnostics）] ウィンドウに、現在の承認のリストが表示されます。次の操作を実行できます。

- 設定の編集
- 承認を取り消します。
- デバイスと Firewall Management Center の sudo アクセスを有効にする。

デバイスの sudo アクセスの有効化

sudo デバイス アクセスを提供すると、通常のユーザーにデバイスへの管理権限を付与できます。ユーザー ロールに関係なく、デバイスの sudo アクセスを有効にすると、デバイスのすべてのユーザーがこの権限を利用できます。

始める前に

Firewall Management Centerに必要なデバイスが追加されていることを確認します。

手順

ステップ 1 **[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[リモート診断（Remote Diagnostics）]**を選択します。

ステップ 2 デバイスへの sudo アクセスを有効にするには、**[デバイスのsudoアクセス（Device Sudo Access）]** タブをクリックします。

Firewall Management Center および Firewall Management Center に展開されたデバイスが一覧表示されます。

ステップ 3 デバイスの sudo アクセスを有効にするには、**[Sudo ステータス（Sudo Status）]** の下の対応するトグルボタンをクリックします。

ステップ 4 （オプション）一括アクションで、デバイスの横にあるチェックボックスをオンにし、**[有効化（Enable）]**をクリックします。

ステップ 5 （オプション）sudo アクセスを無効にするには、**[Sudo ステータス（Sudo Status）]**の下にあるそれぞれのトグルボタンをクリックします。

セッション ログのダウンロード

[前のセッション（Previous Sessions）] タブには、Firewall Threat Defense デバイスおよび Firewall Management Centerで RADKit クライアントによって実行された操作のログ ファイルのリストが表示されます。これらのセッション ログはアーカイブとしてダウンロードできます。RADKit セッションのログは、 Firewall Management Center ログ ローテーション メカニズムに追加され、他の Firewall Management Center ログファイルと同様にデフォルトのログ ローテーション メカニズムの対象になります。

手順

ステップ 1 **[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[リモート診断（Remote Diagnostics）]** を選択し、**[前のセッション（Previous Sessions）]** タブをクリックします。

ステップ 2 **[過去のセッション ログ（Past Session Logs）]** 検索バーに検索文字列を入力して、特定のセッションログを検索します。

ステップ 3 **[すべてのログのダウンロード（Download All Logs）]**を使用して、ログをアーカイブとしてダウンロードします。

（注）
ログは **[現在の許可（Current Authorization）]** ページからもダウンロードできます。

一般的なトラブルシューティング

内部電源障害（ハードウェア障害、電源サージなど）や外部電源の障害（コードが外れている）によって、グレースフルでないシャットダウンまたは再起動が発生することがあります。これによってデータが破損することがあります。

接続ベースのトラブルシューティング

接続ベースのトラブルシューティングまたはデバッグにおいて、モジュール間で一貫したデバッグが提供され、特定の接続について適切なログを収集します。また、レベルベースのデバッグを最大7レベルまでサポートし、モジュール間で一貫したログ収集メカニズムを使用できます。接続ベースのデバッグでは、次の機能がサポートされています。

- Firewall Threat Defense の問題をトラブルシューティングする一般的な接続ベースのデバッグサブシステム
- モジュール間のデバッグメッセージで均一的な形式
- リブート後の永続的なデバッグメッセージ
- 既存の接続に基づくモジュール間のエンドツーエンドのデバッグ
- 進行中の接続のデバッグ

接続のトラブルシューティングの詳細については、接続のトラブルシューティング （28 ページ）を参照してください。

接続のトラブルシューティング

手順

ステップ 1 **debug packet-condition** コマンドを使用して接続を識別するためのフィルタを設定します。

例：

```
Debug packet-condition match tcp 192.168.100.177 255.255.255.255 192.168.102.177
255.255.255.255
```

ステップ 2 対象モジュールおよび対応するレベルのデバッグを有効にします。**debug packet** コマンドを入力します。

例：

```
Debug packet acl 5
```

ステップ 3 次のコマンドを使用して、パケットのデバッグを開始します。

```
debug packet-start
```

ステップ 4 データベースからデバッグ メッセージを取得し、次のコマンドを使用してデバッグ メッセージを分析します。

```
show packet-debugs
```

ステップ 5 次のコマンドを使用して、パケットのデバッグを停止します。

```
debug packet-stop
```

Secure Firewall Threat Defense デバイスの高度なトラブルシューティング

Secure Firewall Threat Defense デバイスでは、パケットトレーサ機能とパケットキャプチャ機能を使って詳細なトラブルシューティング分析が可能です。パケットトレーサを使うと、ファイアウォール管理者はセキュリティアプライアンスに仮想パケットを注入し、入力から出力までのフローを追跡できます。このとき、パケットはフローおよびルーティング ルックアップ、ACL、プロトコルインスペクション、NAT、侵入検知に照らして評価されます。このユーティリティは、送信元および宛先のアドレスとプロトコルおよびポート情報を指定することにより、実際のトラフィックをシミュレートできるため、効果的です。パケットキャプチャにはトレースオプションがあり、このオプションを使用すれば、パケットがドロップされたか成功したかの判断を知ることができます。

トラブルシューティング ファイルの詳細については、高度なトラブルシューティング ファイルのダウンロード （20 ページ）を参照してください。

パケット キャプチャの概要

トレースオプションを有効にしたパケットキャプチャ機能では、入力インターフェイスでキャプチャされた実際のパケットをシステム内でトレースできます。トレース情報は後で表示されます。キャプチャしたパケットは、実際のデータパストラフィックであるため、出力インターフェイスでドロップされません。Firewall Threat Defense デバイスのパケットキャプチャは、データパケットのトラブルシューティングおよび分析をサポートします。

パケットをキャプチャすると、Snort がパケットで有効になっているトレースフラグを検出します。Snort は、パケットが通過するトレーサエレメントを書き込みます。パケットキャプチャの結果、Snort は次のいずれかの判定結果を出します。

表 *3 : Snort* の判定

判定	説明
成功（Pass）	分析されたパケットを許可します。
ブロック （Block）	転送されないパケット。
置換（Replace）	変更されたパケット。
許可フロー（AllowFlow）	インスペクションなしで転送されるフロー。
ブロックフロー（BlockFlow）	フローがブロックされました。

判定	説明
無視	フローがブロックされました。パッシブインターフェイスでフローがブロックされているセッションでのみ発生します。
再試行	フローが停止し、enamelwareまたはURLカテゴリ/レピュテーションクエリを待機しています。タイムアウトが発生した場合、処理は続行され、結果は不明になります。enamelwareの場合、ファイルは許可されます。URLカテゴリ/レピュテーションの場合、ACルールルックアップは未分類の不明なレピュテーションで続行されます。

Snortの判定に基づいて、パケットはドロップまたは許可されます。たとえば、Snortの判定が**[ブロックフロー（BlockFlow）]**である場合、パケットはドロップされ、セッション内の後続のパケットはSnortに到達する前にドロップされます。Snortの判定が[ブロック（Block）]または**[ブロックフロー（BlockFlow）]**の場合、[ドロップ理由（Drop Reason）]は次のいずれかになります。

表 *4:* ドロップ理由

ブロックまたはフローブロックの実行元	原因
Snort	Snortがパケットを処理できません。たとえば、パケットが破損しているか、無効な形式であるため、Snortがパケットを復号化できません。
前処理されたアプリケーションID	アプリケーションIDモジュール/前処理されたアプリケーションIDは、それ自体はパケットをブロックしません。ただし、これは、アプリケーションID検出が原因で他のモジュール（ファイアウォールなど）がブロッキングルールに一致することを示している可能性があります。
前処理されたSSL	SSLポリシーにトラフィックと一致するブロック/リセットルールがあります。
ファイアウォール	ファイアウォールポリシーにトラフィックと一致するブロック/リセットルールがあります。
前処理されたキャプティブポータル	トラフィックと一致する、IDポリシーを使用するブロック/リセットルールがあります。

ブロックまたはフローブロックの実行元	原因
前処理されたセーフサーチ	トラフィックと一致する、ファイアウォールポリシーのセーフサーチ機能を使用するブロック/リセットルールがあります。
前処理された SI	AC ポリシーの [セキュリティインテリジェンス（Security Intelligence）] タブに、トラフィックをブロックするブロック/リセットルールがあります（DNS または URL SI ルールなど）。
前処理された filterer	AC ポリシーの [filterer] タブに、トラフィックと一致するブロック/リセットルールがあります。
前処理されたストリーム	侵入ルールのブロッキング/リセットストリーム接続があります（TCP 正規化エラー時のブロッキングなど）。
前処理されたセッション	このセッションは他のモジュールによってすでにブロックされているため、前処理されたセッションが同じセッションの以降のパケットをブロックしています。
前処理されたフラグメンテーション	データの以前のフラグメントがブロックされているため、ブロックしています。
前処理された snort 応答	たとえば、特定の HTTP トラフィックで応答ページを送信する、react snort ルールがあります。
前処理された snort 応答	条件に一致するパケットに、カスタム応答を送信する snort ルールがあります。
前処理されたレピュテーション	パケットがレピュテーションルール（特定の IP アドレスのブロッキングなど）に一致しています。
前処理された x-Link2State	SMTP で検出されたバッファオーバーフローの脆弱性によるブロッキング。
前処理された back orifice	back orifice データの検出によるブロッキング。
前処理された SMB	SMB トラフィックをブロックする snort ルールがあります。
前処理されたファイルプロセス	ファイルをブロックするファイルポリシーがあります（enamelware ブロッキングなど）。

ブロックまたはフローブロックの実行元	原因
前処理された IPS	IPS を使用する snort ルールがあります（レートフィルタリングなど）。

パケット キャプチャ機能を使用すると、システム メモリに保存されているパケットをキャプチャしてダウンロードできます。ただし、メモリの制約により、バッファ サイズは 32 MB に制限されます。大量のパケット キャプチャを処理できるシステムはすぐに最大バッファ サイズを超過するため、パケットキャプチャの制限を増やす必要があります。これを行うには、セカンダリ メモリを使用します（ファイルを作成してキャプチャ データを書き込む）。サポートされている最大ファイル サイズは 10 GB です。

file-size を設定すると、キャプチャされたデータがファイルに保存され、キャプチャ名 **recapture** に基づいてファイル名が割り当てられます。

ファイル サイズ オプションは、32 MB 以上のサイズ制限のパケットをキャプチャする必要がある場合に使用されます。

詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

キャプチャ トレースの使用

パケットキャプチャは、定義された基準に基づいてデバイスの指定されたインターフェイスを通過するネットワークトラフィックのライブスナップショットを提供するユーティリティです。このプロセスは、一時停止していない限り、または割り当てられたメモリが使い果たされていない限り、パケットのキャプチャを続行します。

パケット キャプチャ データには、パケットの処理中にシステムが行う決定とアクションに関する Snort とプリプロセッサからの情報が含まれています。一度に複数のパケット キャプチャを実行できます。キャプチャの変更、削除、クリア、保存を実行するようにシステムを設定できます。

（注） パケットデータのキャプチャには、パケットのコピーが必要です。この操作によって、パケットの処理中に遅延が生じる可能性があります。また、パケットのスループットが低下する可能性もあります。特定のデータトラフィックをキャプチャするためにパケットフィルタを使用することをお勧めします。

始める前に

Secure Firewall Threat Defense デバイスでパケットキャプチャツールを使用するには、管理者またはメンテナンスユーザーである必要があります。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]** > **[パケットキャプチャ（Packet Capture）]** を選択します。

ステップ 2 デバイスを選択します。

ステップ 3 **[キャプチャの追加（Add Capture）]** をクリックします。

ステップ 4 トレースのキャプチャの [名前（Name）] を入力します。

ステップ 5 トレースのキャプチャの [インターフェイス（Interface）] を選択します。

ステップ 6 以下の [一致基準（Match Criteria）] の詳細を指定します。

a) [プロトコル（Protocol）] を選択します。
b) [送信元ホスト（Source Host）] の IP アドレスを入力します。
c) [宛先ホスト（Destination Host）] の IP アドレスを入力します。
d) （オプション）[SGT 番号（SGT number）] チェックボックスをオンにし、セキュリティ グループ タグ（SGT）を入力します。

ステップ 7 以下の [バッファ（Buffer）] の詳細を指定します。

a) （オプション）最大 [パケット サイズ（Packet Size）] を入力します。
b) （オプション）最小 [バッファ サイズ（Buffer Size）] を入力します。
c) 中断せずにトラフィックをキャプチャしたい場合は、[連続キャプチャ（Continuous Capture）] を選択し、最大バッファ サイズに到達したらキャプチャを停止したい場合は、[いっぱいになったら停止（Stop when full）] を選択します。

（注）
[連続キャプチャ（Continues Capture）] がオンになっている場合、割り当てられたメモリがいっぱいになると、メモリ内の最も古いキャプチャ済みパケットが、新しくキャプチャされたパケットで上書きされます。

d) 各パケットの詳細をキャプチャする場合は、[トレース（Trace）] チェックボックスをオンにします。
e) [トレース数（Trace Count）] フィールドに値を入力します。デフォルト値は 128 です。1 ～ 1000 の範囲で値を入力できます。

ステップ 8 [保存（Save）] をクリックします。

パケットキャプチャ画面に、パケットキャプチャの詳細とそのステータスが表示されます。パケットキャプチャページを自動更新するには、[自動更新の有効化（Enable Auto Refresh）] チェックボックスをオンにして、自動更新間隔を秒単位で入力します。

パケットキャプチャでは、次の操作を実行できます。

- [編集（Edit）]（✎）：キャプチャ基準を変更できます。

- [削除（Delete）]（  ）：パケットキャプチャとキャプチャされたパケットを削除できます。
- **クリア**（  ）：1 つのパケットキャプチャから、キャプチャされたすべてのパケットを消去できます。既存のすべてのパケットキャプチャから、キャプチャされたパケットを消去するには、[すべてのパケットをクリア（Clear All Packets）] をクリックします。
- [一時停止（Pause）]（  ）：パケットのキャプチャを一時的に停止できます。
- **保存**（  ）：キャプチャされたパケットのコピーを ASCII または PCAP 形式でローカルマシンに保存できます。必要な形式オプションを選択し、[保存（Save）] をクリックします。保存されたパケットキャプチャがローカルマシンにダウンロードされます。
- キャプチャされているパケットの詳細を表示するには、必要なキャプチャ行をクリックします。

パケット トレーサの概要

パケットトレーサツールを使用すると、送信元および宛先のアドレスとプロトコルの特性によってパケットをモデル化することにより、ポリシー設定をテストできます。トレースでは、ポリシールックアップが実行され、設定済みのアクセスルール、NAT、ルーティング、アクセスポリシー、レート制限ポリシーに基づいてパケットが許可されるか拒否されるかが確認されます。パケットフローは、インターフェイス、送信元アドレス、宛先アドレス、ポート、プロトコルに基づいてシミュレートされます。この方式でパケットをテストすることによって、ポリシーの有効性を確認し、必要に応じて、許可または拒否するトラフィックのタイプが処理されるかどうかをテストできます。

設定の確認に加えて、トレーサを使用して、アクセスを許可すべきパケットが拒否されるなどの予期せぬ動作をデバッグできます。パケットを完全にシミュレートするために、パケットトレーサはデータパス（低速パスモジュールと高速パスモジュール）をトレースします。当初は、処理が、セッション単位またはパケット単位のトランザクションとして行われていました。ファイアウォールがセッション単位またはパケット単位でパケットを処理する際は、パケットトレーサツールと「トレースによるキャプチャ」機能により、パケット単位でトレースデータがログに記録されます。

PCAP ファイル

PCAP ファイルを使用してパケットトレーサを開始できます。これにより、完全なフローが実現されます。現時点では、単一の TCP/UDP ベースのフローおよび最大 100 パケットでの PCAP のみがサポートされています。パケットトレーサツールは、PCAP ファイルを読み取り、クライアントとサーバーのリプレイエンティティの状態を初期化します。ツールは、後続の処理と表示のために PCAP 内の各パケットのトレース出力を収集して保存することで、同期方式でパケットのリプレイを開始します。

PCAP リプレイ

パケットリプレイは、PCAP ファイル内のパケットのシーケンスによって実行されます。リプレイアクティビティへの干渉があると、リプレイアクティビティが中断され、リプレイが終了します。指定された入力インターフェイスおよび出力インターフェイスにおける PCAP のすべ

てのパケットについてトレース出力が生成されるため、フロー評価の完全なコンテキストが提供されます。

PCAP リプレイは、リプレイ中にパケットを動的に変更する一部の機能（IPsec、VPN、、HTTP 復号など）ではサポートされません。

NAT が設定された Firewall Threat Defense デバイスの場合、PCAP パケットはリプレイ中に変換されたアドレスを反映するため、そのアドレスはドロップされずに処理されます。ただし、PCAP リプレイは、「IPv4 から IPv6」または「IPv6 から IPv4」の NAT タイプをサポートしていません。

パケットトレーサでアイデンティティおよび TLS 復号関連のトレース情報をキャプチャするには、デバイスで Snort 3 が検出エンジンとして設定されていることを確認する必要があります。

より現実的なパケット リプレイ シミュレーションのために、このツールでは、パケットの実際のタイミングを模倣できます。PCAP ファイルに記録されたタイムスタンプに従ってパケットがリプレイされます。タイムスタンプオプションを有効にするには、**packet-tracer** コマンドで **honor-timestamp** キーワードを使用します。

（注） Firewall Threat Defense デバイスでのリプレイされたパケットの処理時間がパケット間の遅延よりも大きい場合、PCAP のタイムスタンプを受け入れる精度が制限されます。

show packet tracer コマンドで **export-pcapng** キーワードを使用すると、Firewall Threat Defense デバイスで生成されるパケットトレースデータを PCAP ファイルの一部として保存できます。保存された pcapng ファイルは、他の外部パケットビューアツール（Wireshark など）を使用して表示できます。

パケット トレーサの使用

Secure Firewall Threat Defense デバイスでパケットトレーサを使用するには、管理者またはメンテナンスユーザーである必要があります。

手順

ステップ 1 Firewall Management Center で、**[デバイス（Devices）]** > **[トラブルシュート（Troubleshoot）]** > **[パケットトレーサ（Packet Tracer）]** を選択します。

ステップ 2 [デバイスの選択（Select Device）] ドロップダウンリストから、トレースを実行するデバイスを選択します。

ステップ 3 **[プロトコルの使用（Use Protocol）]** を選択して設定を手動で行うか、**[PCAP ファイルのアップロードまたは編集（Upload or Edit a PCAP file）]** を選択してパケット キャプチャ（PCAP）ファイルをアップロードします。

ステップ 4 PCAP ファイルをアップロードする場合は、次の手順を実行します。

a) **[PCAP ファイルのアップロードまたは編集（Upload or Edit a PCAP file）]** ドロップダウンをクリックし、**[PCAP ファイルのアップロード（Upload a PCAP file）]** オプションを選択します。最近アップロードしたファイルを使用するには、リストからファイルをクリックします。

（注）
.pcap および .pcapng ファイル形式のみがサポートされています。このファイルには、同じイーサネット接続、または同じ単一 VLAN でカプセル化された TCP、または UDP 接続からの最大100個のパケットを含めることができます。マルチフローPCAPファイルはサポートされていません。単一のフローPCAPファイルのみをアップロードします。

b) PCAP ファイルのアップロードを選択した場合は、PCAP ファイルをダイアログ ボックスにドラッグアンドドロップするか、クリックして PCAP ファイルを参照します。ファイルを選択すると、アップロードプロセスが自動的に開始されます。

（注）
構成をアップロードした後では、**[プロトコル（Protocol）]**、**[送信元タイプ（Source Type）]**、および **[宛先タイプ（Destination Type）]** フィールドがグレー表示され、編集できなくなります。これらのフィールドを変更するには、新しい PCAP ファイルをアップロードする必要があります。送信元と宛先の IP アドレス、送信元と宛先のポート、VLAN ID、宛先の MAC アドレス（透過モードのファイアウォール用）、および PCAP ファイル名を編集できます。si

c) 手順7に進みます。

ステップ 5 手動構成を行う場合は、次の手順を実行します。

a) [入力インターフェイス（Ingress Interface）] ドロップダウンリストから、パケットトレース用の入力インターフェイスを選択します。

（注）
[VTI] を選択しないでください。パケットトレーサでは、入力インターフェイスとしての VTI はサポートされていません。

b) トレースパラメータを定義するには、**[プロトコル（Protocol）]** ドロップダウンメニューからトレースのパケットタイプを選択し、プロトコル特性を指定します。

- [ICMP]：ICMP タイプ、ICMP コード（0 ～ 255）、およびオプションで ICMP 識別子を入力します。
- [TCP/UDP/SCTP]：送信元および宛先のポート番号を入力します。
- [GRE/IPIP]：プロトコル番号（0 ～ 255）を入力します。
- **[ESP]**：送信元の SPI 値（0 ～ 4294967295）を入力します。
- [RAWIP]：プロトコル番号（0 ～ 255）を入力します。

c) パケットトレースの [送信元タイプ（Source Type）] を選択し、送信元 IP アドレスを入力します。

送信元と宛先のタイプとして、IPv4、IPv6、完全修飾ドメイン名（FQDN）を選択できます。Cisco TrustSec を使用する場合、IPv4 または IPv6 アドレスと FQDN を指定できます。

d) パケット トレースの [送信元ポート（Source Port）] を選択します。
e) パケット トレースの **[宛先（Destination）]** タイプを選択し、宛先 IP アドレスを入力します。

宛先タイプのオプションは、選択した送信元タイプによって異なります。

f) パケット トレースの [宛先ポート（Destination Port）] を選択します。
g) パケットトレーサで親インターフェイスに入力する（後でサブインターフェイスにリダイレクトされる）場合は、[VLAN ID] を入力します。

インターフェイス タイプはすべてサブインターフェイスで設定するため、これはサブインターフェイスを使用しない場合だけのオプションです。

h) パケット トレースの [宛先 MAC アドレス（Destination MAC Address）] を指定します。

Secure Firewall Threat Defense デバイスをトランスペアレント ファイアウォール モードで実行していて、入力インターフェイスが VTEP であるとき、[VLAN ID] に値を入力する場合は、[宛先 MAC アドレス（Destination MAC Address）] は必須になります。一方、インターフェイスがブリッジ グループのメンバーであるとき、[VLAN ID] に値を入力する場合は [宛先 MAC アドレス（Destination MAC Address）] はオプションですが、[VLAN ID] に値を入力しない場合は必須になります。

Secure Firewall Threat Defense をルーテッド ファイアウォール モードで実行しているときに、入力インターフェイスがブリッジグループのメンバーである場合、[VLAN ID] と [宛先MACアドレス（Destination MAC Address）] はオプションになります。

i) （任意）パケットトレーサで、シミュレートされたパケットのセキュリティチェックを無視する場合は、[シミュレートされたパケットのすべてのセキュリティチェックをバイパスする（Bypass all security check for Simulated packet）] をクリックします。これにより、パケットトレーサは、これを設定しないとシステムを通過するときにドロップされるパケットのトレースを継続できるようになります。
j) （任意）デバイスから出力インターフェイスを介してパケットを送信できるようにするには、[シミュレートされたパケットがデバイスから送信できるようにする（Allow Simulated packet to transmit from device）] をクリックします。
k) （任意）パケットトレーサで、インジェクトされたパケットを IPsec/SSL VPN で復号されたパケットと見なすようにするには、[シミュレートされたパケットをIPsec/SSL VPN 復号として扱う（Treat simulated packet as IPsec/SSL VPN decrypt）] をクリックします。

ステップ 6 パケットトレーサで PCAP リプレイを使用するには、次の手順を実行します。

a) [PCAPファイルの選択（Select a PCAP File）] をクリックします。
b) 新しい PCAP ファイルをアップロードするには、[PCAPファイルのアップロード（Upload a PCAP file）] をクリックします。最近アップロードしたファイルを再利用するには、リストからファイルをクリックします。

（注）

.pcap および .pcapng ファイル形式のみがサポートされています。PCAP ファイルには、最大 100 パケットの TCP/UDP ベースのフローを 1 つだけ含めることができます。PCAP ファイル名（ファイル形式を含む）の最大文字数は 64 文字です。

c) [PCAPのアップロード（Upload PCAP）] ボックスで、PCAP ファイルをドラッグするか、ボックスをクリックしてファイルを参照およびアップロードすることができます。ファイルを選択すると、アップロードプロセスが自動的に開始されます。

ステップ 7 [トレース（Trace）] をクリックします。

ステップ 8 値を変更する場合は、トレースを続行する前に **[PCAP の保存（Save PCAP）]** をクリックして値を保存してください。

ステップ 9 **[イベントとログ（Events & Logs）]** > **[分析（Analysis）]** > **[監査ログ（Audit Logs）]** ウィンドウでトレースのステータスを追跡できます。次の動作を追跡できます。

- PCAP ファイルの保存
- PCAP ファイルのアップロード
- パケット トレースの詳細

[トレース結果（Trace Result）] には、PCAP パケットがシステムを通過した各フェーズの結果が表示されます。個々のパケットのトレース結果を表示するには、そのパケットをクリックします。次を実行できます。

- トレース結果をクリップボードにコピー（[コピー（copy）]）します。
- 表示される結果を展開したり折りたたんだり（展開または折りたたみ）します。
- トレース結果画面を最大化（[最大化（Maximize）]）します。

要した処理能力の測定に役立つ経過時間情報が、フェーズごとに表示されます。入力インターフェイスから出力インターフェイスへのパケットフロー全体にかかった合計時間も、結果セクションに表示されます。

[トレース履歴（Trace History）] ペインには、PCAP トレースごとに保存されたトレースの詳細が表示されます。最大 100 のパケットトレースを保存できます。保存されたトレースを選択して、パケット トレース アクティビティを再度実行できます。次を実行できます。

- 任意のトレースパラメータの使用してトレースを検索します。
- スライダ ボタンを使用して、履歴へのトレースの保存を無効にします。
- 特定のトレース結果を削除します。
- すべてのトレースをクリアします。

CPU プロファイラの概要

CPU プロファイラは、パケットが特定のタイムフレーム内で処理されている間に、Snort 3 の個別モジュールまたはインスペクタの CPU 使用率に関するデータを収集します。Snort 3 プロセスの合計 CPU 使用率に関連して、各モジュールが消費する CPU 時間の量に関する情報を提供します。CPU プロファイラを使用すると、設定をリロードしたり、Snort 3 を再起動したりする必要がないため、ダウンタイムが最小限に抑えられます。プロファイリングの結果には、最後のプロファイリングセッション中にすべてのモジュールが要した処理時間が表示されます。CPU プロファイリングの結果は、Threat Defense デバイスに JSON 形式で保存され、Management Center で同期されます。

⚠

注意 CPUプロファイリングにより、システムパフォーマンスが約3%低下する可能性があります。

CPU プロファイラの使用

始める前に

CPU プロファイリングを使用するには、Snort 3 を搭載したバージョン 7.6 以降のデバイスが必要です。

手順

ステップ 1 Management Center から、**[デバイス（Devices）] > [Snort 3 プロファイリング（Snort 3 Profiling）]** を選択します。

ステップ 2 [CPUプロファイリング（CPU Profiling）] タブをクリックします。

ステップ 3 [CPUプロファイリングのデバイスの選択（Select device for CPU Profiling）] ドロップダウンリストから、CPU プロファイリングのデバイスを選択します。

（注）
異なるデバイスで複数のプロファイリングセッションを同時に実行できます。

ステップ 4 CPU プロファイリングセッションを開始するには、[開始（Start）] をクリックします（セッションは 120 分後に自動的に停止します）。

[停止（Stop）] をクリックすると、いつでもプロファイリングセッションを停止できます。ただし、スケジュールされた 120 分間の前にキャンセルすると、正確な結果が得られない場合があります。

（注）
CPUプロファイリングセッションの進行中に、タスクが作成されます。詳細を表示するには、**[通知（Notifications）] > [タスク（Tasks）]** をクリックします。

最新のプロファイリング結果が [CPUプロファイリングの結果（CPU Profiling Results）] セクションに自動的に表示されます。このテーブルには、最後のプロファイリングセッション中に

すべての Snort 3 モジュールまたはインスペクタが要した処理時間の統計が含まれています。CPU プロファイラの出力は、次の表形式で表示できます。

- [モジュール（Module）]：モジュールまたはインスペクタの名前。
- [CPU時間の合計（%）（% Total of CPU Time）]：Snort 3 がトラフィックを処理するために要した時間全体に対する、モジュールが要した時間の割合（%）。この値が他のモジュールの値よりも大幅に高い場合は、そのモジュールが Snort 3 のパフォーマンス低下に大きく影響していることを意味します。
- [時間（マイクロ秒）（Time(μs)）]：各モジュールが要した合計時間（マイクロ秒単位）。
- [平均/チェック（Avg/Check）]：モジュールが呼び出されるたびにモジュールが要した平均時間。
- [%発信者（% Caller）]：メインモジュールに対する、サブモジュール（設定されている場合）が要した時間。この値はデバッグ用途に使用されます。

ステップ 5 （任意）[スナップショットのダウンロード（Download Snapshot）]をクリックして、プロファイリング結果をダウンロードします。ダウンロードされるファイルは CSV 形式であり、プロファイリング結果のページにあるすべてのフィールドが含まれています。

ステップ 6 （任意）[Snort時間の%でフィルタ処理（Filter by % of Snort time）] トグルボタンをクリックして、実行にプロファイリング時間の *n*% を超えて要したモジュールをフィルタ処理によって除外します。

ステップ 7 （任意）[検索（Search）]フィールドを使用して、[CPUプロファイリングの結果（CPU Profiling Results）] テーブルのフィールドを検索します。

（注）
[モジュール（Module）]を除き、他のどの列ヘッダーも、クリックしてデータをソートできます。

ステップ 8 （任意）[プロファイリング履歴（Profiling History）] セクション（左側にある折りたたみ可能なパネル）をクリックして展開し、選択したデバイスの以前のプロファイリングセッションを表す一連のカードを表示します。履歴からカードをクリックすると、[CPUプロファイリングの結果（CPU Profiling Results）] セクションに詳細が表示されます。

（注） CPU プロファイリングの実行中に展開を開始すると、プロファイリング セッションは展開に対応するために自動的に終了します。ただしアクセス コントロール ポリシー ルールおよびセキュリティ インテリジェンスに対する変更による展開を除きます。デバイスの CPU プロファイリングを再度実行する必要があります。

ルールプロファイラの概要

Snort 3 ルールプロファイラは、一連の Snort 3 侵入ルールの処理にかかった時間に関するデータを収集し、潜在的な問題を強調表示して、パフォーマンスが不十分なルールを表示します。Snort 3 エンジン内では、ルールプロファイラが Snort 3 侵入検出メカニズムを使用してトラフィックを検査します。ルールプロファイラは、チェックに最も長い時間を要した上位 100 の IPS ルールを表示します。ルールプロファイラのトリガーには、Snort 3 のリロードまたは再起動は必要ありません。ルールプロファイリングの結果は、Threat Defense デバイスに JSON 形式で保存され、Management Center で同期されます。

ルールプロファイラの使用

始める前に

ルール プロファイリングを使用するには、Snort 3 を備えたバージョン 7.6 以降のデバイスが必要です。

手順

ステップ 1 Management Center から、**[デバイス（Devices）] > [Snort 3 プロファイリング（Snort 3 Profiling）]** を選択します。

ステップ 2 [ルールプロファイリング（Rule Profiling）] タブをクリックします。

ステップ 3 [ルールプロファイリングのデバイスの選択（Select device for Rule Profiling）] ドロップダウンリストから、ルールプロファイリングのデバイスを選択します。

（注）
異なるデバイスで複数のプロファイリングセッションを同時に実行できます。

ステップ 4 ルールプロファイリングセッションを開始するには、[開始（Start）] をクリックします（セッションは 120 分後に自動的に停止します）。

[停止（Stop）] をクリックすると、いつでもプロファイリングセッションを停止できます。ただし、スケジュールされた 120 分間の前にキャンセルすると、正確な結果が得られない場合があります。

（注）
ルール プロファイリング セッションの進行中に、タスクが作成されます。詳細を表示するには、**[通知（Notifications）] > [タスク（Tasks）]** をクリックします。

最新のプロファイリング結果が [ルールプロファイリングの結果（Rule Profiling Results）] セクションに自動的に表示されます。このテーブルには、処理に最も時間がかかったルールの統計が、合計時間（マイクロ秒（µs）単位）ごとに降順で表示されます。IPS ルールプロファイラの出力は、次の表形式で表示できます。

- [Snort時間の%（% of Snort Time）]：Snort 3 動作の合計時間に対する、ルールの処理に費やされた時間。

- [リビジョン（Rev）]：ルールのリビジョン番号。
- [チェック（Checks）]：IPS ルールが実行された回数。
- [一致（Matches）]：トラフィックで IPS ルールが完全に一致した回数。
- [アラート（Alerts）]：IPS ルールが IPS アラートをトリガーした回数。
- [時間（Time）]：Snort が IPS ルールのチェックに費やした時間（マイクロ秒単位）。
- [平均/チェック（Avg/Check）]：ルールの 1 回のチェックに Snort が費やした平均時間。
- [平均/一致（Avg/Match）]：1 回のチェック（結果として一致）に Snort が費やした平均時間。
- [平均/不一致（Avg/Non-Match）]：1 回のチェック（結果として不一致）に Snort が費やした平均時間。
- [タイムアウト（Timeouts）]：アクセス コントロール ポリシーの [遅延ベースのパフォーマンス設定（Latency-Based Performance Settings）] で設定された [ルール処理 - しきい値（Rule Handling - Threshold）] をルールが超えた回数。
- [一時停止（Suspends）]：連続したしきい値違反が原因でルールが一時停止された回数。

ステップ 5 （任意）[スナップショットのダウンロード（Download Snapshot）] をクリックして、プロファイリング結果をダウンロードします。ダウンロードされるファイルは CSV 形式であり、プロファイリング結果のページにあるすべてのフィールドが含まれています。

ステップ 6 （任意）[Snort時間の%でフィルタ処理（Filter by % of Snort time）] トグルボタンをクリックして、実行にプロファイリング時間の *n*% を超えて要したルールをフィルタ処理によって除外します。一般に、ルールが Snort の全体的な処理時間の 0.2% 以上を消費している場合、そのルールのパフォーマンスは不十分であると見なされます。

ステップ 7 （任意）[検索（Search）] フィールドを使用して、[ルールプロファイリングの結果（Rule Profiling Results）] テーブルのフィールドを検索します。

ステップ 8 （任意）[ルールプロファイリング履歴（Rule Profiling History）] セクション（左側にある折りたたみ可能なパネル）をクリックして展開し、選択したデバイスの以前のプロファイリング セッションを表す一連のカードを表示します。履歴からカードをクリックすると、[ルールプロファイリングの結果（Rule Profiling Results）] セクションに詳細が表示されます。

（注） ルール プロファイリングの実行中に展開を開始すると、アクセス コントロール ポリシー ルールおよびセキュリティ インテリジェンスに対する変更による展開を除き、展開に対応するためプロファイリング セッションが自動的に終了します。デバイスに対してルール プロファイリングを再度実行する必要があります。

Web インターフェイスから Firewall Threat Defense 診断 CLI を使用する方法

Firewall Management Center から選択した Firewall Threat Defense 診断 CLI コマンドを実行できます。コマンド **ping**（**ping system** を除く）、**traceroute**、および一部の **show** コマンドは、通常の CLI ではなく診断 CLI で実行されます。

show コマンドを実行したときに、「`Unable to execute the command properly. Please see logs for more details`」（コマンドを正しく実行できません。詳細については、ログを参照してください）というメッセージが表示される場合は、そのコマンドが診断 CLI で無効であることを意味します。たとえば、**show access-list** は機能しますが、**show access-control-policy** と入力すると、このメッセージが表示されます。非診断コマンドを使用するには、SSH を使用して Management Center の外部のデバイスにログインします。

Firewall Threat Defense CLI の詳細については、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

始める前に

- 診断 CLI を使用するには、管理者、メンテナンス、またはセキュリティアナリストである必要があります。
- 診断 CLI の目的は、デバイスのトラブルシューティングに役立ついくつかのコマンドをすばやく使用できるようにすることです。すべてのコマンドにアクセスするには、デバイスとの SSH セッションを直接開きます。
- Firewall Management Center 高可用性を使用する展開では、診断 CLI は、アクティブ Firewall Management Center でのみ使用できます。

手順

ステップ 1 **[デバイス（Devices）]** > **[脅威対策CLI（Threat Defense CLI）]**を選択します。

また、デバイスの正常性モニター（[システム（System）]（⚙） > **[正常性（Health）]** > **[モニタ（Monitor）]**）から CLI ツールにアクセスすることもできます。そこから、デバイスを選択し、[システムとトラブルシューティングの詳細を表示（View System and Troubleshoot Details）] リンクをクリックし、[高度なトラブルシューティング（Advanced Troubleshooting）] をクリックして、そのページで [Threat Defense CLI] をクリックします。

ステップ 2 [デバイス（Device）] ドロップダウンリストから、診断コマンドを実行するデバイスを選択します。

ステップ 3 [コマンド（Command）] ドロップダウンリストから、実行するコマンドを選択します。

ステップ 4 [パラメータ（Parameters）] フィールドにコマンドパラメータを入力します。

有効なパラメータについては、Cisco Secure Firewall Threat Defense コマンドリファレンスを参照してください。

たとえば、**show access-list** コマンドを実行するには、[コマンド（Command）] ドロップダウンリストから **show** を選択し、[パラメータ（Parameters）] フィールドに **access-list** と入力します。

（注）
[パラメータ（Parameters）] フィールドにコマンド全体を入力しないでください。関連するキーワードのみを入力してください。

ステップ 5 [実行（Execute）] をクリックして、コマンド出力を表示します。

「`Unable to execute the command properly. Please see logs for more details.`」（コマンドを正しく実行できません。詳細については、ログを参照してください）というメッセージが表示される場合は、パラメータをよく確認してください。構文エラーがある可能性があります。

このメッセージは、実行しようとしているコマンドが診断 CLI（**system support diagnostic-cli** コマンドを使用してデバイスからアクセスした）のコンテキスト内で有効なコマンドではないことを意味する場合もあります。これらのコマンドを使用するには、SSH を使用してデバイスにログインします。

機能固有のトラブルシューティング

機能固有のトラブルシューティングのヒントやテクニックについては、次の表を参照してください。

表 *5*: 機能固有のトラブルシューティング トピック

機能	関連するトラブルシューティング情報
アプリケーション制御	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Best Practices for Application Control*」
LDAP 外部認証	LDAP 認証接続のトラブルシューティング
ライセンシング	スマート ライセンスのトラブルシューティング 特定のライセンスの予約のトラブルシューティング
Firewall Management Center ハイ アベイラビリティ	Firewall Management Center のハイ アベイラビリティのトラブルシューティング
ユーザ ルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot User Control*」

機能	関連するトラブルシューティング情報
ユーザ アイデンティティ ソース	ISE/ISE-PIC、TS エージェント アイデンティティ ソース、キャプティブ ポータル アイデンティティ ソース、およびリモートアクセス VPN アイデンティティソースに関するトラブルシューティング情報については、Cisco Secure Firewall Management Center デバイス構成ガイドの対応する項を参照してください。 LDAP 認証接続のトラブルシューティング
URL フィルタリング	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot URL Filtering*」
レルムとユーザ データのダウンロード	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot Realms and User Downloads*」
ネットワーク検出	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshooting Your Network Discovery Strategy*」
カスタム セキュリティ グループ タグ（SGT）のルール条件	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Custom SGT Rule Conditions*」
SSL ルール	Cisco Secure Firewall Device Manager Configuration Guideの SSL ルールに関する章
Cisco Threat Intelligence Director（TID）	Cisco Secure Firewall Management Center デバイス構成ガイドの「*Troubleshoot Secure Firewall Threat Intelligence Director*」
Secure Firewall Threat Defense syslog	Cisco Secure Firewall Management Center デバイス構成ガイドの「*About Configuring Syslog*」
接続ベースのトラブルシューティング	接続ベースのトラブルシューティング （28 ページ）

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。