



システムの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最初の手順](#) (1 ページ)
- [システム メッセージ](#) (2 ページ)
- [基本的なシステム情報の表示](#) (5 ページ)
- [システム メッセージの管理](#) (6 ページ)
- [トラブルシューティング用のヘルス モニタ レポート](#) (12 ページ)
- [一般的なトラブルシューティング](#) (15 ページ)
- [Firepower Threat Defense デバイスの高度なトラブルシューティング](#) (15 ページ)
- [機能固有のトラブルシューティング](#) (20 ページ)

トラブルシューティングの最初の手順

- 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 レポート](#) (12 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 に連絡する必要がある場合に、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。[FMC 展開に関するトップレベルのドキュメントのリストページ](#)を参照してください。

システムメッセージ

Firepower 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、Firepower 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)] ボタンの右隣にある[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、システムの状態によって以下のように表示されます。

-  : 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。
-  : 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。
-  : 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、Firepower システム 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、非表示アイコン (✖) 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。Firepower 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)] () とともに表示されるメッセージ数に含まれます。
- [失敗 (Failure)] () 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)

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、ヘルスマonitoringについてに記載されているように、ヘルスマジュールによって生成されます。Firepower システムでは、次のヘルスステータス値がこのタブでレポートされます。

- [警告 (Warning)] () 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。
- [重大 (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 (Error)] ( 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、[ヘルスマonitoring (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

Firepower システムでは、完了するまで時間がかかる可能性がある特定のタスク (構成のバックアップやインストールの更新など) を実行できます。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。Firepower 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せん。
- [実行中 (Running)] (🌀 の表示が回転中) : 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動作を設定します (これらを表示するかどうかを選択します)。
- システム データベースの追加のタスクのステータス メッセージを表示します (削除されていないもので利用可能なものがある場合)。
- 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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
該当なし	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)

[バージョン情報 (About)] ページには、Firepower 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から [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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	FMC 7000 & 8000 シリーズ	グローバルだけ	Admin

手順

[System] > [Configuration] を選択します。

システムメッセージの管理

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	<p>[展開 (Deployment)] : 管理者/[設定をデバイスに展開する (Deploy Configuration to Devices)] 権限を持つカスタム ユーザ ロール</p> <p>[ヘルス (Health)] : 管理者/[ヘルス (Health)] 権限を持つカスタム ユーザ ロール</p> <p>他人によって開始されたタスク : 管理者/[他のユーザのタスクを確認する (View Other Users' Tasks)] 権限があるカスタム ユーザ ロール</p> <p>自分が開始したタスク : 任意</p>

手順

ステップ 1 [システム ステータス (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 次の選択肢があります。

- [展開 (Deployments)] タブをクリックして、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。

- [ヘルス (Health)] タブをクリックして、Firepower 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。ヘルス メッセージの表示 (9 ページ) を参照してください。
- [タスク (Tasks)] タブをクリックして、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 (10 ページ) またはタスク メッセージの管理 (11 ページ) を参照してください。
- Message Center の右上隅にある歯車アイコン (⚙) をクリックして、ポップアップ通知の動作を設定します。通知動作の設定 (12 ページ) を参照してください。

展開メッセージの表示

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	[設定をデバイスに展開する (Deploy Configuration to Devices)] 権限を持つ管理者/ユーザ ロール

手順

ステップ 1 [システム ステータス (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 [展開 (Deployments)] タブをクリックします。

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、[合計 (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、[1分5秒 (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、[履歴を表示 (Show 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 [トランスクリプト (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립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 Firepower Management Center (FMC) 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。FTD がセキュリティレベルを使用することはありません。

```

===== 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.

```

関連トピック

[設定変更の展開](#)

ヘルスメッセージの表示

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	[ヘルス (Health)] の権限を持つ管理者/ユーザ ロール

手順

ステップ 1 [システム ステータス (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 [ヘルス (Health)] タブをクリックします。

ステップ 3 次の選択肢があります。

- 現在のすべてのヘルス ステータスを表示するには、[合計 (total)] をクリックします。
- 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ヘルス 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)] ページの完全なヘルス ステータスを表示するには、タブの下部にある [ヘルス モニタ (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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する (View Other Users' Tasks)] 権限があるカスタムユーザ ロール 自分が開始したタスク：任意

手順

ステップ 1 [システム ステータス (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)] タブをクリックします。

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、[合計 (total)] 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

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	他人によって開始されたタスク：管理者/[他のユーザのタスクを確認する (View Other Users' Tasks)] 権限があるカスタムユーザ ロール 自分が開始したタスク：任意

手順

ステップ 1 [システム ステータス (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)] タブをクリックします。

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アイコン (✖) 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。

通知動作の設定

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)



(注) この設定は、すべてのポップアップ通知に影響を及ぼし、ログインセッション間で保持されません。

手順

- ステップ 1** [システムステータス (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** メッセージセンターの右上にある歯車アイコン (⚙️) をクリックします。
- ステップ 3** ポップアップ通知の表示を有効または無効にするには、[通知を表示 (Show notifications)] スライダをクリックします。
- ステップ 4** スライダを非表示にするには、歯車アイコン (⚙️) を再度クリックします。
- ステップ 5** [システムステータス (System Status)] アイコンを再度クリックして、メッセージセンターを閉じます。

トラブルシューティング用のヘルス モニタ 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 1: 選択可能なトラブルシューティングオプション

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

オプション	報告内容
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
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	トラブルシューティング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 ファイルの作成

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

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。

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティングファイルの生成およびダウンロードが可能です。



注意 低メモリ デバイス用のトラブルシューティング ファイルを生成すると、自動アプリケーションバイパス (AAB) が有効になっている場合は AAB をトリガーすることができます。少なくとも、AAB をトリガーすると Snort プロセスを再開すると、一時的にトラフィック検査が中断されます。この中断中にトラフィックがドロップされるか、それ以上インスペクションが行われずに受け渡されるかは、ターゲットデバイスがトラフィックを処理する方法に応じて異なります。詳細は [Snort® の再起動によるトラフィックの動作](#) を参照してください。そのような場合、AAB のトリガーによって、デバイスが一時的に動作不能な状態になることがあります。動作不能な状態が続く場合は Cisco Technical Assistance Center (TAC) に連絡してください。展開に適したソリューションをご提案します。影響を受けやすいデバイスは、Firepower 7010、7020、および 7030、ASA5508-X、5516-X、5515-X、および 5525-X、NGIPSv などです。

手順

- ステップ 1 [アプライアンス ヘルス モニタの表示](#) の手順を実行します。
- ステップ 2 [トラブルシューティング ファイルの生成 (Generate Troubleshooting Files)] をクリックします。
- ステップ 3 [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。詳細については、[タスク メッセージの表示 \(10 ページ\)](#) を参照してください。
- ステップ 4 [OK] 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 \(10 ページ\)](#) 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

スマート ライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	任意 (Any)	任意 (Any)	Admin/Maint/Any Security Analyst

マルチドメイン展開では、子孫ドメイン内のデバイスに対するトラブルシューティングファイルの生成およびダウンロードが可能です。グローバルドメインの場合のみ、Firepower Management Center からファイルをダウンロードできます。

手順

- ステップ 1 アプライアンスのヘルスマニタを表示します ([アプライアンスヘルスマニタの表示](#)を参照)。
- ステップ 2 [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 3 [ファイルのダウンロード (File Download)] タブで、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。

一般的なトラブルシューティング

システムでのディスクレイフル以外のシャットダウンまたは再起動は、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）によって発生します。これらによって最終的にデータが破損することがあります。

FirepowerThreatDefenseデバイスの高度なトラブルシューティング

Firepower 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の有用性は、プロトコルおよびポート情報を含め、送信元と宛先アドレスを指定することで、実際のトラフィックをシミュレートできることにあります。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、次を参照してください。 [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 \(14 ページ\)](#)

Web インターフェイスからの FTD CLI の使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	任意 (Any)	FTD	任意 (Any)	Admin/Maint/Any Security Analyst

Firepower Management Center Web インターフェイスから、選択した FTD コマンドライン インターフェイス (CLI) コマンドを実行できます。これらのコマンドは、ping、traceroute、show (show サブコマンドの history と banner を除く) です。

マルチドメイン環境では、子孫ドメインの管理対象デバイスの Firepower Management Center Web インターフェイスを使用して、FTD CLI コマンドを入力できます。



(注) Firepower Management Center ハイアベイラビリティを使用した展開では、この機能はアクティブ Firepower Management Center でのみ使用できます。

FTD CLI の詳細については、*Firepower Threat Defense* のコマンドリファレンス [英語] を参照してください。

手順

- ステップ 1 アプライアンスのヘルスモニタを表示します (アプライアンスヘルスモニタの表示を参照)。
- ステップ 2 [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 3 [脅威防御 CLI (Threat Defense CLI)] タブをクリックします。
- ステップ 4 [コマンド (Command)] ドロップダウンリストで、コマンドを選択します。
- ステップ 5 オプションで、[パラメータ (Parameters)] テキストボックスにコマンドパラメータを入力します。
- ステップ 6 [実行 (Execute)] をクリックして、コマンド出力を表示します。

パケットトレーサの概要

パケットトレーサを使用して、送信元と宛先のアドレスおよびプロトコルの特性に基づいてパケットをモデル化することによって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を実行してアクセスルール、NAT、ルーティング、アクセスポリシー、レート制限ポリシーをテストし、パケットを許可するか拒否するかを確認します。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。このようにパケットをテストすることによって、ポリシーの結果を確認し、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。処理は、セッション単位またはパケット単位に基づいてトランザクションとして行われます。次世代ファイアウォール（NGFW）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、パケットのトレースとトレースによるキャプチャにより、パケット単位でトレースデータがログに記録されます。

パケットトレーサの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	適用対象外	Firepower Threat Defense	任意 (Any)	Admin/Maint

手順

- ステップ 1 Firepower Management Center で、**[Devices] > [Device Management]** 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 トラブルシューティングアイコンをクリックします。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- ステップ 4 [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 5 [パケットトレーサ (Packet Tracer)] タブをクリックします。
- ステップ 6 トレースの [パケットタイプ (Packet type)] を選択し、以下の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。
 - [IP] : プロトコル番号 (0 ~ 255) を入力します。
- ステップ 7 パケット トレースの入力 [インターフェイス (Interface)] を選択します。
- ステップ 8 パケット トレースの [送信元 (Source)] タイプを選択し、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。
- ステップ 9 パケット トレースの [送信元ポート (Source Port)] を選択します。
- ステップ 10 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。
- ステップ 11 パケット トレースの [宛先ポート (Destination Port)] を選択します。
- ステップ 12 オプションで、セキュリティグループタグ (SGT) 値がレイヤ 2 CMD ヘッダー (TrustSec) に組み込まれているパケットをトレースする場合、有効な [SGT 番号 (SGT number)] を入力します。

- ステップ 13** 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。
- ステップ 14** 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。
- Firepower 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。
- Firepower 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。
- ステップ 15** パケット ログの [出力形式 (Output Format)] を選択します。
- ステップ 16** [開始 (Start)] をクリックします。

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。Firepower 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 [ドロップ (DROP)]/[許可 (ALLOW)]/[条件付きドロップ (Would DROP)] のいずれかの判定結果を出します。

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。

ファイルサイズを設定すると、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 `capture_name.pcap` 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、[Firepower Threat Defense のコマンドリファレンス \[英語\]](#) を参照してください。

キャプチャトレースの使用

スマートライセンス	従来のライセンス	サポートされるデバイス	サポートされるドメイン	アクセス (Access)
任意 (Any)	適用対象外	Firepower Threat Defense	任意 (Any)	Admin/Maint

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。シスコでは、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。

pcap または *ASCII* ファイル形式で保存されたトラフィックデータをダウンロードできます。

手順

- ステップ 1 Firepower Management Center で、**[Devices] > [Device Management]** 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 トラブルシューティングアイコンをクリックします。
[ヘルス モニタ (Health Monitor)] ページが表示されます。
- ステップ 4 [高度なトラブルシューティング (Advanced Troubleshooting)] をクリックします。
- ステップ 5 [w/トレースのキャプチャ (Capture w/Trace)] タブを選択します。
- ステップ 6 **[キャプチャの追加 (Add Capture)]** をクリックします。
- ステップ 7 トレースのキャプチャの [名前 (Name)] を入力します。
- ステップ 8 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 9 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 10 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。
- 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)] を選択します。
- e) (オプション) [トレース カウント (Trace Count)] チェックボックスをオンにします。デフォルト値は 50 です。1 ~ 1000 の範囲で値を入力できます。

ステップ 11 [保存 (Save)] をクリックします。

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 2: 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
LDAP 外部認証	LDAP 認証接続のトラブルシューティング
7000 および 8000 シリーズ デバイスのハイ アベイラビリティ状態共有	トラブルシューティングのためのデバイスのハイ アベイラビリティの状態共有統計情報
ユーザ ルール条件	ユーザ制御のトラブルシューティング
ユーザ アイデンティティ ソース	ユーザ エージェント アイデンティティ ソースのトラブルシューティング ISE/ISE-PIC アイデンティティ ソースのトラブルシューティング TS エージェント アイデンティティ ソースのトラブルシューティング キャプティブ ポータルのアイデンティティ ソースのトラブルシューティング リモートアクセス VPN アイデンティティ ソースのトラブルシューティング
URL フィルタリング	URL フィルタリングのトラブルシューティング
レルムとユーザデータのダウンロード	レルムとユーザのダウンロードのトラブルシューティング
ネットワーク検出	ネットワーク検出戦略のトラブルシューティング

機能	関連するトラブルシューティング情報
カスタム セキュリティ グループ タグ (SGT) のルール条件	カスタム SGT 条件のトラブルシューティング
SSL ルール	TLS/SSL ルールのトラブルシューティング
Cisco Threat Intelligence Director (TID)	Cisco Threat Intelligence Director (TID) のトラブルシューティング
Firepower Threat Defense syslog	Syslog の設定概要
侵入パフォーマンス統計	侵入パフォーマンス統計情報のロギング設定
7000 および 8000 シリーズ NGIPSv 次を搭載した ASA FirePOWER サービス	generate-troubleshoot (コマンドラインインターフェイス (CLI) のコマンド)
Cisco Security Packet Analyzer との統合	Packet Analyzer クエリのトラブルシューティング

