CHAPTER 11

Guard モジュールの診断ツールの使用方法

この章では、Cisco Anomaly Guard Module（Guard モジュール）に関する統計情報や診断を表示する方法について説明します。この章には、次の項があります。

Guard モジュールの設定の表示

Guard モジュールの設定ファイルを表示することができます。このファイルには、インターフェイスの IP アドレス、デフォルト ゲートウェイ アドレス、設定されたゾーンなど、Guard モジュールの設定に関する情報が含まれています。

Guard モジュールの設定ファイルを表示するには、次のコマンドを入力します。

show running-config [**all** | **Guard module**| **interfaces** *interface-name* | self-protection | zones]]

表 11-1 に、**show running-config** コマンドのキーワードを示します。

表 11-1　show running-config コマンドのキーワード

パラメータ	説明
all	Guard モジュールのすべてのモジュール（Guard モジュール、ゾーン、インターフェイス、および自己保護）の設定ファイルを表示します。
Guard module	Guard モジュールの設定ファイルを表示します。
interfaces	Guard モジュールのインターフェイスの設定ファイルを表示します。インターフェイス名を入力します。
self-protection	Guard モジュールの自己保護の設定を表示します。
zones	すべてのゾーンの設定ファイルを表示します。

次の例を参考にしてください。

```
user@GUARD# show running-config guard
```

設定ファイルは、Guard モジュールを現在の設定値で設定するために実行されるコマンドで構成されています。Guard モジュールの設定ファイルをリモート FTP サーバにエクスポートして、バックアップ用にしたり、別の Guard モジュールにその Guard モジュールの設定パラメータを実装できるようにすることができます。詳細については、P.11-3 の「Guard モジュールのゾーンの表示」を参照してください。

Guard モジュールのゾーンの表示

Guard でゾーンの概要を表示して、アクティブなゾーンやゾーンの現在のステータスを確認できます。ゾーンのリストを表示するには、グローバル モードで **show** コマンドを使用します。表 11-2 で、さまざまなゾーン ステータスについて説明します。

表 11-2　ゾーンのステータス

ステータス	説明
Auto Protect mode	ゾーンは自動保護モードです。ユーザの介入なしに動的フィルタがアクティブになります。 ゾーンが自動保護モードにあり、ポリシーのしきい値を調整するために Guard モジュールがゾーンのトラフィック特性のラーニングを行っている場合、Guard モジュールはゾーン名の横に (+learning) を表示します。
Interactive Protect mode	ゾーンはインタラクティブ保護モードです。動的フィルタは手動でアクティブになります。
Threshold Tuning phase	ゾーンはしきい値調整フェーズです。Guard は、ゾーンのトラフィックを分析して、ポリシー構築フェーズ中に構築されたポリシーのしきい値を定義します。
Policy Construction phase	ゾーンはポリシー構築フェーズです。ゾーンのポリシーが作成されます。
Standby	ゾーンはアクティブではありません。

例

```
user@GUARD# show
```

ゾーンのカウンタの表示

ゾーン カウンタの表示およびゾーン トラフィックの分析には、次のコマンドを使用できます。

- **show rates :** Malicious カウンタと Legitimate カウンタの平均トラフィック レートを表示します。
- **show rates details :** すべての Guard モジュールのカウンタの平均トラフィック レートを表示します。
- **show rates history :** Malicious カウンタおよび Legitimate カウンタの平均トラフィック レートを、過去 24 時間にわたり 1 分ごとに表示します。
- **show counters**：Guard モジュールの Malicious カウンタと Legitimate カウンタを表示します。
- **show counters details**：すべての Guard モジュールのカウンタを表示します。
- **show counters history**：過去の Malicious カウンタおよび Legitimate カウンタの値を 1 分ごとに表示します。

レートの単位は bps および pps です。

（注）　ゾーンのレートは、ゾーン保護をイネーブルにしている場合、またはラーニング プロセスをアクティブにしている場合にのみ使用可能です。

Guard は、トラフィックの合計を測定し、平均のトラフィック レートを計算します。値が **cleared** のレートは、ゾーンが保護されていなかった時間を示します。

カウンタの単位はパケットおよびキロビットです。カウンタは、ゾーン保護をアクティブにしたときにゼロにリセットされます。

表 11-3 に、Guard モジュールのカウンタを示します。

表 11-3　Guard モジュールのカウンタ

カウンタ	説明
Malicious	ゾーンを宛先とする悪意のあるトラフィック。悪意のあるトラフィックは、ドロップされたカウンタとスプーフィングされたカウンタ（ゾンビ パケットも含む）の合計です。
Legitimate	Guard モジュールによってゾーンに転送された正当なトラフィック。
Received	Guard モジュールが受信し、処理したパケット。受信カウンタは、正当なカウンタと悪意のあるカウンタの合計です。
Forwarded	Guard モジュールによってゾーンに転送された正当なトラフィック。
Dropped	Guard モジュールの保護メカニズム（動的フィルタ、フレックスコンテンツ フィルタ、およびレート リミッタ モジュール）が攻撃の一部として識別し、ドロップしたパケット。
Replied	スプーフィング防止およびゾンビ防止メカニズムの一部として、信頼できるトラフィックと悪意のあるトラフィックのどちらに属するかを確認するために開始クライアントに対して応答が送信されたパケット。
Spoofed	Guard モジュールによってスプーフィングされたパケットと判断され、ゾーンに転送されなかったパケット。スプーフィングされたパケットは、応答が送信されたパケット（詳細については上の「Replied カウンタ」を参照）のうち、それに対する応答が受信されなかったものです。ゾンビ パケットは、スプーフィング パケット カウンタにも含まれています。
Invalid zone	Guard モジュールで保護されたどのゾーンも宛先としない、宛先変更されたトラフィック。この情報は、グローバル モードまたは設定モードでコマンドを入力した場合にのみ使用可能です。

次の例を参考にしてください。

```
admin@GUARD-conf-zone-scannet# show rates
```

ゾーンのステータスの表示

特定のゾーンの概要を表示して、そのゾーンの全般的な状況と現在のステータスを知ることができます。ゾーンの概要を表示するには、ゾーン設定モードで **show** コマンドを使用します。概要には、次の情報が含まれます。

- **ゾーンのステータス**：動作状態を示します。動作状態は、保護モード、保護およびラーニングのモード、しきい値調整モード、ポリシー構築モード、または非アクティブのいずれかです。
- **ゾーンの基本設定**：動作モード（自動またはインタラクティブ）、しきい値とタイマー、IP アドレスなど、ゾーンの基本的な設定を示します。詳細については、P.6-9 の「ゾーンのアトリビュートの設定」を参照してください。
- ゾーンのフィルタ：フレックスコンテンツ　フィルタの設定も含めて、アクティブな動的フィルタおよびユーザ フィルタの設定数を示します。ゾーンがインタラクティブ保護モードの場合、概要には推奨事項の数が表示されます。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」および P.7-24 の「ユーザ フィルタの設定」を参照してください。
- **ゾーンのトラフィック　レート**：ゾーンの正当なトラフィックと悪意あるトラフィックのレートを表示します。詳細については、P.11-4 の「ゾーンのカウンタの表示」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show
```

Guard モジュールのログの表示

Guard モジュールは、システムのアクティビティおよびイベントを自動的にログに記録します。Guard モジュールのログを表示して、Guard モジュールのアクティビティを確認および追跡できます。

表 11-4 に、イベント ログのレベルを示します。

表 11-4　イベント ログのレベル

イベントのレベル	数値コード	説明
Emergencies	0	システムが使用不能
Alerts	1	ただちに対処が必要
Critical	2	深刻な状態
Errors	3	エラー状態
Warnings	4	警告状態
Notifications	5	通常、ただし注意が必要
Informational	6	情報メッセージ
Debugging	7	デバッグ メッセージ

ログ ファイルには、すべてのログ レベル（emergencies、alerts、critical、errors、warnings、notification、informational、debugging）が表示されます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

イベント ログは、ローカルで表示することも、リモート サーバから表示することもできます。

- イベントのリアルタイム ロギング：P.11-8 の「オンライン イベント ログの表示」を参照してください。
- ログ ファイル：P.11-11 の「ログ ファイルの表示」を参照してください。

オンライン イベント ログの表示

Guard モジュールのモニタリング メカニズムをアクティブにして、リアルタイムのイベント ログを表示できます。この設定により、Guard モジュールのイベントのオンライン ロギングを表示できます。次のコマンドを入力します。

event monitor

次の例を参考にしてください。

```
user@GUARD# event monitor
```

画面はイベントで常にアップデートされます。

（注）　モニタリング メカニズムを非アクティブにするには、**no event monitor** コマンドを使用してください。

オンライン イベント ログのエクスポート

Guard モジュールのオンライン イベント ログをエクスポートして、ログ ファイルに記録される Guard モジュールの動作を表示できます。Guard モジュールのイベントは Guard モジュールのログ ファイルにオンラインで記録されるため、リモート ホストからそのイベントを表示できます。Guard モジュールのログ ファイルは、syslog メカニズムを使用してエクスポートされます。Guard モジュールのログ ファイルは、複数の Syslog サーバにエクスポートできます。1 つのサーバがオフラインになったときに別のサーバでメッセージを受信できるように、追加のサーバを指定できます。

Guard モジュールのオンライン ログ エクスポート機能は、リモート syslog サーバを使用する場合にだけ適用できます。リモート syslog サーバが使用できない場合は、**copy log** コマンドを使用して、Guard モジュールのログ情報をファイルにエクスポートしてください。

次に、イベント ログの例を示します。

```
Sep 11 16:34:40 10.4.4.4 cm: scannet, 5 threshold-tuning-start: Zone
activation completed successfully.
```

syslog メッセージの構文は、次のとおりです。

event-date event-time Guard-IP-address protection-module zone-name event-severity-level event-type event-description

オンライン イベント ログをエクスポートするには、次の手順を実行します。

ステップ 1　（オプション）ロギング パラメータを設定します。次のコマンドを入力します。

```
logging {facility | trap}
```

表 11-5 で、**logging** コマンドのキーワードについて説明します。

表 11-5　logging コマンドのキーワード

パラメータ	説明
facility	エクスポート syslog ファシリティ。リモート syslog サーバは、ロギング ファシリティを使用してイベントをフィルタリングします。たとえば、ロギング ファシリティを使用すると、リモート ユーザは Guard モジュールのイベントを 1 つのファイルで受信し、他のネットワーク デバイスからのイベントには別のファイルを使用することができます。 使用できるファシリティは、local0 ～ local7 です。デフォルトは local4 です。
trap	リモート syslog に送信する syslog トラップの重大度。重大度のトラップ レベルには、それより高い重大度のレベルが含まれます。たとえば、トラップ レベルを **warning** に設定すると、error、critical、alerts、および emergencies も送信されます。指定できるトラップ レベルは、高い方から順に emergencies、alerts、critical、errors、warnings、notification、informational、debugging です。デフォルトは notification です。

（注）　動的フィルタの追加および削除に関するイベントを受信するには、トラップ レベルを informational に変更してください。

ステップ 2　リモート syslog サーバの IP アドレスを設定します。次のコマンドを入力します。

logging host *remote-syslog-server-ip*

または

export log *remote-syslog-server-ip*

remote-syslog-server-ip 引数には、リモート syslog サーバの IP アドレスを指定します。

ロギング メッセージを受信する syslog サーバのリストを作成するには、このコマンドを複数回入力してください。

次の例は、重大度のレベル *notification* からのトラップをファシリティ *local3* を使用して、IP アドレスが *10.0.0.191* である syslog サーバへ送信するように Guard モジュールを設定する方法を示しています。

```
user@GUARD-conf# logging facility local3
user@GUARD-conf# logging trap notifications
user@GUARD-conf# logging host 10.0.0.191
```

オンライン イベント ログのエクスポート設定を表示するには、**show logging** コマンドまたは **show log export-ip** コマンドを使用します。

ログ ファイルの表示

診断または監視のために Guard モジュールのログを表示できます。Guard モジュールのログ ファイルには、emergencies、alerts、critical、errors、warnings、および notification という重大度を持つゾーン イベントが含まれます。

Guard モジュールのログを表示するには、次のコマンドを入力します。

show log

次の例を参考にしてください。

```
user@GUARD# show log
```

ゾーンのログを表示して、指定したゾーンだけに関連するイベントを確認できます。

ゾーンのログを表示するには、**show log** [*sub-zone-name*] コマンドをゾーン設定モードで使用します。*sub-zone-name* 引数には、ゾーンから作成されたサブゾーンの名前を指定します。詳細については、P.6-42 の「サブゾーンについて」を参照してください。

ログ ファイルのエクスポート

監視または診断のために、Guard モジュールのログ ファイルを FTP サーバにエクスポートできます。グローバル モードで、次のいずれかのコマンドを入力します。

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-6 で、**copy log ftp** コマンドの引数とキーワードについて説明します。

表 11-6　copy log ftp コマンドの引数

パラメータ	説明
zone-name	（オプション）ゾーン名。ゾーンのログ ファイルをエクスポートします。デフォルトでは、Guard モジュールのログ ファイルがエクスポートされます。
ftp	ログを FTP サーバにエクスポートします。
sftp	ログを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy log ftp 10.0.0.191 log.txt <user> <password>
```

ログ ファイルのクリア

Guard モジュールまたはゾーンのログ ファイルが大きい場合、あるいは、テストを行う予定があり、そのテスト セッションからの情報だけをログ ファイルに反映する場合は、ログ ファイルをクリアできます。

Guard モジュールまたはゾーンのログ ファイルのエントリをすべてクリアするには、設定モードまたはゾーン設定モードで次のコマンドを入力します。

clear [zone *zone-name***] log**

zone-name 引数には、ゾーン名を指定します。デフォルトでは、Guard モジュールのログ ファイルがクリアされます。**clear log** コマンドをゾーン設定モードで発行する場合、**zone** *zone-name* キーワードと引数は使用できません。ゾーン設定モードで **clear log** コマンドを使用すると、現在のゾーン ログの全エントリが消去されます。

次の例を参考にしてください。

```
user@GUARD-conf# clear log
```

ネットワーク トラフィックの監視および攻撃のシグニチャの抽出

ネットワークのトラフィック パターンを記録し、監視できます。ネットワークの動作を阻害しないタップを使用して、直接ネットワークからトラフィックを記録するように Guard モジュールを設定し、記録されたトラフィックからデータベースを作成することができます。記録されたトラフィック データベースに問い合せることにより、過去のイベントの分析や、攻撃のシグニチャの生成が可能になります。あるいは、現在のネットワークのトラフィック パターンを、トラフィックが通常状態のときに Guard モジュールによって記録された以前のトラフィック パターンと比較することが可能になります。

特定の基準を満たすトラフィックだけが Guard モジュールによって記録されるようにフィルタを設定することができます。または、すべてのトラフィック データを記録して、Guard モジュールが表示するトラフィックをフィルタリングすることもできます。

トラフィックは、Guard モジュールによって gzip 圧縮されたパケット キャプチャ（PCAP）形式で保存され、記録されたデータについて記述する Extensible Markup Language（XML）形式のファイルが付属します。

記録されたトラフィックの重要な用途は、記録された攻撃パケットのペイロードに共通のパターンまたはシグニチャが見られるかどうかを判断するというものです。Guard モジュールでは、記録されたトラフィックを分析し、シグニチャを抽出することができます。シグニチャを使用すると、そのシグニチャと一致するパケット ペイロードを含むすべてのトラフィックをブロックするようにフレックスコンテンツ フィルタを設定できます。

Guard モジュールは、次の 2 つの方法でトラフィックを記録できます。

- **自動**：Guard モジュールは常時パケットダンプ キャプチャ ファイルにトラフィック データを記録します。

  新しいパケットダンプ キャプチャ ファイルによって、以前のファイルは置き換えられます。以前のパケットダンプ キャプチャ ファイルを保存するには、FTP サーバまたは SFTP サーバにそれらのファイルをエクスポートする必要があります。
- **手動**：Guard モジュールは、パケットダンプ キャプチャ ファイルにトラフィックを記録するようにアクティブ化されたときに記録します。

以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。記録されたトラフィックを保存するには、パケットダンプ キャプチャ ファイルを FTP サーバまたは SFTP サーバにエクスポートしてから、Guard モジュールをアクティブ化して再度トラフィックを記録します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、手動で同時に最大 4 つのゾーンについてトラフィックを記録できます。

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

この項では、次のトピックについて取り上げます。

- Guard モジュールの設定によるトラフィックの自動記録
- Guard モジュールのアクティブ化によるトラフィックの手動記録
- Guard モジュールによるトラフィックの手動記録の停止
- 手動パケットダンプ設定の表示
- パケットダンプ キャプチャ ファイルの自動エクスポート
- パケットダンプ キャプチャ ファイルの手動エクスポート
- パケットダンプ キャプチャ ファイルのインポート
- パケットダンプ キャプチャ ファイルの表示
- パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成
- パケットダンプ キャプチャ ファイルのコピー
- パケットダンプ キャプチャ ファイルの削除

Guard モジュールの設定によるトラフィックの自動記録

Guard モジュールをアクティブにして、自動的にネットワーク トラフィックを記録することができます。このようにして、ネットワークの問題や攻撃が発生したときに分析または比較に使用可能なトラフィックの記録を入手できます。パケットダンプ キャプチャ フィルタを使用すると、指定した基準を満たすトラフィックだけが記録されるように Guard モジュールを設定できます。また、すべてのトラフィックを記録し、その記録済みのトラフィックを表示するときにパケットダンプ キャプチャ フィルタを適用することもできます。

Guard モジュールはトラフィックをキャプチャ バッファに記録します。キャプチャ バッファ サイズが 50 MB に達するか 10 分経過すると、Guard モジュールはバッファを圧縮形式でローカル ファイルに保存します。バッファは消去され、トラフィックの記録が続行されます。

Guard モジュールは、複数の自動パケットダンプ キャプチャ ファイルを保存します。記録されたトラフィックは、処理方法に基づいて分割されます。したがって、複数の自動パケットダンプ キャプチャ ファイルを 1 つの時間枠から取得できます。自動パケットダンプ キャプチャ ファイルの名前は、Guard モジュールによるトラフィックの記録時間とトラフィックの処理方法を示します。

表 11-7 で、自動パケットダンプ キャプチャ ファイル名のセクションについて説明します。

表 11-7　自動パケットダンプ キャプチャ ファイル名のセクション

セクション	説明
機能	パケットダンプ キャプチャ時に実行された Guard モジュールの機能。機能は次のいずれかになります。 • **protect**：ゾーン保護の間、Guard モジュールがトラフィックを記録。 • **learn**：ゾーンのラーニング プロセスの間、または保護およびラーニング プロセスの間、Guard モジュールがトラフィックを記録。
キャプチャ開始時刻	Guard モジュールがトラフィックの記録を開始した時刻。

表 11-7　自動パケットダンプ キャプチャ ファイル名のセクション（続き）

セクション	説明
キャプチャ終了時刻	（オプション）Guard モジュールがトラフィックの記録を完了した時刻。Guard モジュールが現在トラフィックをファイルに記録している場合、終了時刻は表示されません。
処理	Guard モジュールがトラフィックを処理した方法。アクションは次のいずれかになります。 • **forwarded**：Guard モジュールが正当なトラフィックと見なしてゾーンに転送したトラフィック • **dropped**：Guard モジュールが悪意のあるトラフィックと見なしてドロップしたトラフィック • **replied**：パケットが正当なトラフィックの一部であるか攻撃の一部であるかを確認するために、Guard モジュールがスプーフィング防止メカニズムまたはゾンビ防止メカニズムによる処理の一環として、開始側のクライアントに応答を送信したトラフィック

Guard モジュールは、ラーニング プロセスからパケットダンプ キャプチャ ファイルを 1 つ保存します。ゾーン保護の間、Guard モジュールは次のパケットダンプ キャプチャ ファイルを保存します。

- 直前 10 分間のトラフィックのパケットダンプ キャプチャ ファイル 1 つ
- 現在のトラフィックのパケットダンプ キャプチャ ファイル 1 つ

ゾーン保護をアクティブにするか、または自動的にネットワーク トラフィックが記録されるように Guard モジュールをアクティブにすると、保護プロセスで記録された以前のパケットダンプ キャプチャ ファイルはすべて Guard モジュールによって消去され、新しいファイルが作成されます。

自動的にネットワーク トラフィックを記録するように Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　ゾーン トラフィックを自動的に記録するように Guard モジュールを設定します。ゾーン設定モードで次のコマンドを入力します。

```
packet-dump auto-capture
```

ステップ 2　（オプション）パケットダンプ　キャプチャ　データベースを作成するには、FTP サーバまたは SFTP サーバにパケットダンプ キャプチャ ファイルをエクスポートします。P.11-22 の「パケットダンプ キャプチャ ファイルの自動エクスポート」を参照してください。

以前のパケットダンプ キャプチャ ファイルは新しいファイルに置き換えられます。パケットダンプ キャプチャ データベースを作成するには、パケットダンプ キャプチャ ファイルをエクスポートする必要があります。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# packet-dump auto-capture
```

Guard モジュールでゾーンのトラフィック データを自動的にキャプチャしないようにするには、**no packet-dump auto-capture** コマンドを使用します。

現在のパケットダンプ設定を表示するには、**show packet-dump** コマンドを使用します。

Guard モジュールのアクティブ化によるトラフィックの手動記録

Guard モジュールをアクティブにして、トラフィックの記録を開始できます。このようにして、特定期間のトラフィックを記録したり、あるいは Guard モジュールがトラフィックの記録に使用する基準を変更することができます。

指定されたパケット数を記録するか、ラーニング プロセスまたはゾーン保護が終了すると、Guard モジュールはトラフィックの記録を停止し、手動パケットダンプ キャプチャをファイルに保存します。

1 つのゾーンに対し、手動パケットダンプ キャプチャは一度に 1 つずつしかアクティブにできませんが、手動パケットダンプ キャプチャと自動パケットダンプ キャプチャを同時にアクティブにすることはできます。Guard モジュールは、同時に 10 ゾーンまで手動パケットダンプ キャプチャを記録できます。

手動パケットダンプ キャプチャをアクティブにするには、ゾーン設定モードで次のコマンドを入力します。

packet-dump capture [**view**] *capture-name pdump-rate pdump-count* {**all | dropped | forwarded | replied**} [***tcpdump-expression***]

（注）　トラフィックをキャプチャする間は、CLI セッションが停止します。キャプチャの実行中に作業を続行するには、Guard モジュールとの追加のセッションを確立してください。

表 11-8 で、**packet-dump** コマンドの引数とキーワードについて説明します。

表 11-8　packet-dump コマンドの引数とキーワード

パラメータ	説明
view	（オプション）Guard モジュールが記録しているトラフィックをリアルタイムに表示します。
capture-name	パケットダンプ キャプチャ ファイルの名前。1 ～ 63 文字の英数字文字列を入力します。文字列にアンダースコア（_）を含めることはできますが、スペースを含めることはできません。

表 11-8　packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
pdump-rate	サンプル レート（pps）。1 ～ 10000 の値を入力します。 （注）　Guard モジュールは、すべての同時手動キャプチャに対する最大の累積パケットダンプ キャプチャ レートとして、10000 パケット / 秒をサポートします。 高いサンプル レート値を設定したパケットダンプ キャプチャは、多くのリソースを消費します。パフォーマンスに悪影響を与える可能性があるので、高いレート値を設定するときは注意してください。
pdump-count	記録対象のパケット数。Guard モジュールは、指定されたパケット数の記録を終了すると、手動パケットダンプ キャプチャ バッファをファイルに保存します。1 ～ 5000 の整数を入力します。
all	すべてのトラフィックをキャプチャします。
dropped	Guard モジュールがドロップしたトラフィックだけをキャプチャします。
forwarded	Guard モジュールがゾーンに転送した正当なトラフィックだけをキャプチャします。
replied	検証の試行で Guard モジュールのスプーフィング防止メカニズムおよびゾンビ防止メカニズムが送信元に返送したトラフィックだけをキャプチャします。
tcpdump-expression	（オプション）記録対象のトラフィックを指定するために適用するフィルタ。Guard モジュールはフィルタの式に適合するトラフィックだけをキャプチャします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# packet-dump capture view 10 1000 all
```

Guard モジュールによるトラフィックの手動記録の停止

Guard モジュールは、手動パケットダンプ キャプチャをアクティブにしたときに指定したパケット数を記録すると、キャプチャを停止します。しかし、指定したパケット数が Guard モジュールによって記録される前に、手動パケットダンプ キャプチャを停止することができます。

Guard モジュールによるトラフィックの手動記録を停止するには、次のいずれかのアクションを実行します。

- 開かれている CLI セッションで Ctrl+C を押す。
- 新しい CLI セッションを開き、関連するゾーン設定モードで次のコマンドを入力する。

  no packet-dump capture *capture-name*

  capture-name 引数には、停止するキャプチャの名前を指定します。

Guard モジュールは、パケットダンプ キャプチャ ファイルを保存します。

手動パケットダンプ設定の表示

Guard モジュールによって手動パケットダンプ キャプチャ ファイル用に割り当てられたディスク スペースの現在の容量を表示するには、設定モードまたはグローバル モードで **show packet-dump** コマンドを使用します。Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 1 ブロックのディスク スペースを割り当てています。

次の例を参考にしてください。

```
user@GUARD-conf# show packet-dump
```

表 11-9 で、**show packet-dump** コマンド出力のフィールドについて説明します。

表 11-9　手動の show packet-dump コマンド出力のフィールドの説明

フィールド	説明
Allocated disk-space	Guard モジュールによって、すべてのゾーンの手動パケットダンプ キャプチャ用に割り当てられたディスクスペースの合計量を指定します（MB 単位）。
Occupied disk-space	割り当てられたディスク スペースのうち、すべてのゾーンからの手動パケット ダンプ ファイルによって消費されたパーセンテージを示します。

パケットダンプ キャプチャ ファイルの自動エクスポート

パケットダンプ キャプチャ ファイルを自動的に FTP サーバまたは SFTP サーバにエクスポートするように Guard モジュールを設定できます。自動エクスポート機能をイネーブルにすると、Guard モジュールはパケットダンプ バッファの内容をローカル ファイルに保存するたびに、パケットダンプ キャプチャ ファイルをエクスポートします。パケットダンプ キャプチャ ファイルは gzip 圧縮された PCAP 形式でエクスポートされ、記録されたデータについて記述する XML 形式のファイルが付属します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。

パケットダンプ キャプチャ ファイルを自動的にエクスポートするには、設定モードで次のいずれかのコマンドを入力します。

- **export packet-dump ftp** *server full-file-name* [*login* [*password*]]
- **export packet-dump sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-10 で、**export packet-dump** コマンドの引数について説明します。

表 11-10　export packet-dump コマンドの引数

パラメータ	説明
ftp	パケットダンプ キャプチャ ファイルを FTP サーバにエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	Guard モジュールによるパケットダンプ キャプチャ ファイルの保存先の完全パス名。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例は、IP アドレスが *10.0.0.191* の FTP サーバにパケットダンプ キャプチャ ファイルを自動的にエクスポートする方法を示しています。

```
user@GUARD# export packet-dump ftp 10.0.0.191 /root/captures/ <user> <password>
```

パケットダンプ キャプチャ ファイルの手動エクスポート

パケットダンプ キャプチャ ファイルを FTP サーバに手動でエクスポートできます。パケットダンプ キャプチャ ファイルを 1 つエクスポートすることも、特定のゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートすることもできます。Guard モジュールによって、パケットダンプ キャプチャ ファイルは gzip 圧縮された PCAP 形式でエクスポートされ、記録されたデータについて記述する XML ファイルが付属します。XML スキーマについては、このバージョンに付属の Capture.xsd ファイルを参照してください。

パケットダンプ キャプチャ ファイルを FTP サーバに手動でエクスポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **ftp** *server full-file-name* [*login* [*password*]]
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] **sftp** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-11 で、**copy zone packet-dump** コマンドの引数とキーワードについて説明します。

表 11-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
zone-name	既存のゾーンの名前。
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルをすべてエクスポートします。詳細については、P.11-27 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。
ftp	パケットダンプ キャプチャ ファイルを FTP サーバにエクスポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバにエクスポートします。
server	サーバの IP アドレス。
remote-path	Guard モジュールによるパケットダンプ キャプチャ ファイルの保存先の完全パス名。

表 11-11　copy zone packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy zone scannet packet-dump captures ftp 10.0.0.191 <user> <password>
```

パケットダンプ キャプチャ ファイルのインポート

パケットダンプ キャプチャ ファイルを FTP サーバから Guard モジュールにインポートできます。このようにして、過去のイベントを分析したり、現在のネットワークのトラフィック パターンを、Guard モジュールによってトラフィックが通常状態のときに記録された以前のトラフィック パターンと比較することができます。Guard モジュールは、XML 形式と PCAP 形式のパケットダンプ キャプチャ ファイルをどちらもインポートします。

パケットダンプ キャプチャ ファイルをインポートするには、グローバル モードで次のいずれかのコマンドを入力します。

- **copy ftp zone** *zone-name* **packet-dump captures** *server full-file-name* [*login* [*password*]]
- **copy sftp zone** *zone-name* **packet-dump captures** *server full-file-name login*

（注）　**copy reports** コマンドを入力する前に、Guard モジュールが SFTP 通信に使用する SSH 鍵を設定する必要があります。詳細については、P.4-33 の「SFTP 接続の鍵の設定」を参照してください。

表 11-12 で、**copy zone packet-dump** コマンドの引数について説明します。

表 11-12　copy zone packet-dump コマンドの引数

パラメータ	説明
zone-name	パケットダンプ キャプチャ ファイルをインポートする既存のゾーンの名前。
ftp	パケットダンプ キャプチャ ファイルを FTP サーバからインポートします。
sftp	パケットダンプ キャプチャ ファイルを SFTP サーバからインポートします。
server	サーバの IP アドレス。
full-file-name	インポート対象のファイルの完全なパスとファイル名。ファイル拡張子は除きます。パスを指定しない場合、サーバはユーザのホーム ディレクトリからファイルをコピーします。 （注）　ファイル拡張子を指定しないでください。指定すると、インポート プロセスは失敗します。
login	サーバのログイン名。 *login* 引数は、FTP サーバを定義するときは省略可能です。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）リモート FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy ftp zone scannet packet-dump captures 10.0.0.191
capture-1 <user> <password>
```

パケットダンプ キャプチャ ファイルの表示

パケットダンプ キャプチャ ファイルのリスト、または 1 つのパケットダンプ キャプチャ ファイルの内容を表示できます。デフォルトでは、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルすべてのリストを表示します。

パケットダンプ キャプチャ ファイルを表示するには、ゾーン設定モードで次のコマンドを入力します。

show packet-dump captures [***capture-name*** [***tcpdump-expression***]]

表 11-13 に、**show packet-dump captures** コマンドの引数を示します。

表 11-13　show packet-dump captures コマンドの引数

パラメータ	説明
capture-name	（オプション）既存のパケットダンプ キャプチャ ファイルの名前。パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはゾーンのパケットダンプ キャプチャ ファイルすべてのリストを表示します。コマンド出力のフィールド説明については、表 11-14 を参照してください。 パケットダンプ キャプチャ ファイルの名前を指定しない場合、Guard モジュールはファイルを TCPDump 形式で表示します。
tcpdump-expression	（オプション）パケットダンプ キャプチャ ファイルを表示するときに Guard モジュールが使用するフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけを表示します。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# show packet-dump captures
```

表 11-14 で、**show packet-dump captures** コマンド出力のフィールドについて説明します。

表 11-14　show packet-dump captures コマンド出力のフィールドの説明

フィールド	説明
Capture -name	パケットダンプ キャプチャ ファイルの名前。自動パケットダンプ キャプチャ ファイル名については、表 11-7 を参照してください。
Size (MB)	パケットダンプ キャプチャ ファイルのサイズ（MB）。
Filter	Guard モジュールがトラフィックの記録時に使用したユーザ定義のフィルタ。このフィルタは TCPDump 形式です。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

パケットダンプ キャプチャ ファイルからの攻撃シグニチャの生成

攻撃シグニチャは、攻撃パケットのペイロードに見られる共通パターンを記述するものです。Guard モジュールをアクティブにして異常なトラフィックのシグニチャを生成し、この情報を使用してタイプが同じ将来の攻撃をすばやく識別することができます。この機能を使用すると、アンチウィルス ソフトウェアのメーカーやメーリング リストなどからシグニチャが発行される前であっても、新しい DDoS 攻撃やインターネット ワームを検出することができます。

Guard モジュールは、フレックスコンテンツ フィルタのパターン式の構文を使用して攻撃のシグニチャを生成します。このシグニチャをフレックスコンテンツ フィルタのパターンで使用して、異常なトラフィックをフィルタリングして排除できます。詳細については、P.7-7 の「フレックスコンテンツ フィルタの設定」を参照してください。

参照用として、トラフィックが通常状態（平時）のときに Guard モジュールによって記録された追加のパケットダンプ キャプチャ ファイルを指定できます。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Guard モジュールは異常なトラフィックからシグニチャを生成し、トラフィックが通常状態のと

きに記録されたトラフィックの中に、シグニチャが存在している時間の割合を特定します。正常のトラフィック状態で記録されたトラフィックに攻撃シグニチャが高い確率で出現しても、攻撃パターンを意味するとは限りません。

攻撃のシグニチャを生成するには、次の手順を実行します。

ステップ 1　Guard　モジュールをアクティブにして、攻撃進行中のトラフィックを記録します。**packet-dump capture** コマンドを使用します（P.11-18 の「Guard モジュールのアクティブ化によるトラフィックの手動記録」を参照）。

ステップ 2　攻撃進行中に Guard モジュールが記録したパケットダンプ キャプチャ ファイルを識別します。**show packet-dump captures** コマンドを使用して、パケットダンプ キャプチャ ファイルのリストを表示します。詳細については、P.11-27 の「パケットダンプ キャプチャ ファイルの表示」を参照してください。

ステップ 3　Guard モジュールをアクティブにして、攻撃されたトラフィックのシグニチャを生成します。ゾーン設定モードで次のコマンドを入力します。

```
show packet-dump signatures capture-name [reference-capture-name]
```

表 11-15 に、**show packet-dump signatures** コマンドの引数を示します。

表 11-15　show packet-dump signatures コマンドの引数

パラメータ	説明
capture-name	シグニチャの生成元である既存のパケットダンプ キャプチャ ファイルの名前。
reference-capture-name	（オプション）トラフィックが通常状態のときに Guard モジュールによって記録された既存のパケットダンプ キャプチャ ファイルの名前。参照用のパケットダンプ キャプチャ ファイルを指定した場合、Guard モジュールは参照用のパケットダンプ キャプチャ ファイルの中に、シグニチャが存在している時間の割合を表示します。

表 11-16 で、**show packet-dump signatures** コマンド出力のフィールドについて説明します。

表 11-16　show packet-dump signatures コマンド出力のフィールドの説明

フィールド	説明
Start Offset	パケット ペイロードの先頭から、パターン マッチングを開始する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *start-offset* 引数にコピーします。
End Offset	パケット ペイロードの先頭から、パターン マッチングを終了する位置までのオフセット（バイト単位）。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーする場合、このオフセットをフレックスコンテンツ フィルタの *end-offset* 引数にコピーします。
Pattern	Guard モジュールが生成したシグニチャ。Guard モジュールは、フレックスコンテンツ フィルタのパターン式の構文を使用してシグニチャを生成します。詳細については、P.7-16 の「パターン式の構文について」を参照してください。 このパターンをフレックスコンテンツ フィルタのパターン式にコピーできます。
Percentage	シグニチャが *reference-capture-name* ファイルに存在する時間の割合。

次の例は、手動パケットダンプ キャプチャ ファイルからシグニチャを生成する方法を示しています。

```
user@GUARD-conf-zone-scannet# show packet-dump signatures PDumpCapture
```

パケットダンプ キャプチャ ファイルのコピー

1 つのパケットダンプ キャプチャ ファイル、または 1 つのファイルの一部を、新しい名前でコピーできます。

Guard モジュールは、既存の自動パケットダンプ キャプチャ ファイルを新しいファイルで上書きします。自動パケットダンプ キャプチャ ファイルをコピーする場合、Guard モジュールはそのファイルを手動パケットダンプ キャプチャ ファイルとして保存し、新しいファイルで上書きしません。つまり、ディスク スペースを解放するには、そのファイルを手動で削除する必要があります。

手動パケットダンプ キャプチャ ファイルをコピーする場合も、Guard モジュールは元のファイルのコピーを保存します。ディスク スペースを解放する必要がある場合は、そのコピーを手動で削除します。

詳細については、P.11-32 の「パケットダンプ キャプチャ ファイルの削除」を参照してください。

パケットダンプ キャプチャ ファイルをコピーするには、設定モードで次のコマンドを入力します。

copy zone *zone-name* **packet-dump captures** ***capture-name*** [***tcpdump-expression***] ***new-name***

表 11-17 に、**copy packet-dump captures** コマンドの引数を示します。

表 11-17　copy packet-dump captures コマンドの引数

パラメータ	説明
zone-name	コピー対象のパケットダンプ キャプチャ ファイルがある既存のゾーンの名前。
capture-name	既存のパケットダンプ キャプチャ ファイルの名前。
tcpdump-expression	（オプション）パケットダンプ キャプチャ ファイルをコピーするときに Guard モジュールが使用するフィルタ。Guard モジュールは、フィルタ基準に一致する一部のパケットダンプ キャプチャ ファイルだけをコピーします。この式の規則は、フレックスコンテンツ フィルタの TCPDump 式の規則と同じです。詳細については、P.7-13 の「TCPDump 式の構文について」を参照してください。

表 11-17　copy packet-dump captures コマンドの引数（続き）

パラメータ	説明
new-name	新しいパケットダンプ キャプチャ ファイルの名前。この名前は 1 ～ 63 文字の英数字の文字列です。アンダースコアを含めることができますが、スペースを含めることはできません。

次の例を参考にしてください。

```
user@GUARD-conf# copy zone scannet capture-1 "tcp and dst port 80 and
not src port 1000" capture-2
```

パケットダンプ キャプチャ ファイルの削除

デフォルトでは、Guard モジュールは、すべてのゾーンの手動パケットダンプ キャプチャ ファイル用に 20 MB のディスク スペースを割り当てています。すべてのゾーンで最大 80 MB の手動および自動によるパケットダンプ キャプチャ ファイルを保存できます。将来のパケットダンプ キャプチャ ファイルのためにディスク スペースを解放するには、古いパケットダンプ キャプチャ ファイルを削除します。

手動パケットダンプ キャプチャ ファイルは、ゾーンごとに 1 つだけ保存でき、10 個を超えるパケットダンプ キャプチャ ファイルを Guard モジュールに置くことはできません。新しい手動パケットダンプ キャプチャ ファイルのためのスペースを解放するには、古いファイルを削除する必要があります。

自動パケットダンプ キャプチャ ファイルまたは手動パケットダンプ キャプチャ ファイルを削除するには、次のいずれかのコマンドを入力します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}—In configuration mode
- **clear packet-dump captures** {***** | *name*}—In zone configuration mode

表 11-18 に、**clear packet-dump** コマンドの引数を示します。

表 11-18　clear packet-dump コマンドの引数

パラメータ	説明
zone-name	既存のゾーンの名前。
*	すべてのパケットダンプ キャプチャ ファイルを消去します。
name	消去対象のパケットダンプ キャプチャ ファイルの名前。

次の例は、すべての手動パケットダンプ キャプチャ ファイルを消去する方法を示しています。

```
user@GUARD-conf# clear packet-dump captures *
```

一般的な診断データの表示

Guard モジュールの一般的な診断データを表示できます。

一般的な診断データを表示するには、次のコマンドを入力します。

show diagnostic-info

診断データは、次の情報で構成されます。

- **Line Card Number**：Guard の識別子ストリング。
- **Number of Pentium-class Processors**：Guard モジュールのプロセッサの番号。Guard モジュールはプロセッサ 1 をサポートします。
- **BIOS Vendor**：Guard の BIOS のベンダー。
- **BIOS Version**：Guard の BIOS バージョン。
- **Total available memory**：Guard で使用可能なメモリの合計量。
- **Size of compact flash**：Guard のコンパクト フラッシュのサイズ。
- **Slot Num**：モジュールをシャーシに装着するためのスロットの番号（1 ～ 9）。
- **CFE version**：CFE のバージョン番号。

（注）　CFE のバージョンを変更するには、新しいフラッシュ バージョンをインストールする必要があります。CFE の新しいバージョンを焼き付けるには、**flash-burn** コマンドを使用してください。詳細については、P.12-8 の「Guard モジュールのバージョンのアップグレード」を参照してください。

- **Recognition Average Sample Loss**：認識モジュールの、計算されたパケット サンプル損失。
- **Forward failures (no resources)**：システム リソースが不足しているために転送されなかったパケット数。

（注）　**Recognition Average Sample Loss** または **Forward failures** の値が大きいと、Guard モジュールはトラフィックで過負荷の状態になることを示します。複数の Guard モジュールを負荷分散型構成にインストールすることをお勧めします。

メモリ消費量の表示

Guard モジュールのメモリ消費量を表示できます。Guard モジュールは、メモリ使用量を KB 単位で表示します。さらに、Guard モジュールは、認識保護モジュールが使用しているメモリのパーセンテージも表示します。認識保護モジュールのメモリ使用率は、アクティブなゾーンの数、および各ゾーンが監視するサービスの数に影響されます。

（注）　認識保護モジュールのメモリ使用率が 90% を超えた場合は、アクティブなゾーンの数を減らすことを強くお勧めします。

次のコマンドを入力します。

show memory

次の例を参考にしてください。

```
user@GUARD# show memory
              total    used    free    shared   buffers   cached
  In KBytes:  2065188  146260  1918928    0     2360      69232

  Recognition Used Memory: 0.3%
```

（注）　Guard モジュールの空きメモリの合計量は、**free** メモリと **cached** メモリの合計です。

CPU 使用率の表示

現在の CPU 使用率（パーセンテージ）を表示できます。Guard モジュールは、ユーザ モード、システム モード、ナイス値が負のタスク、およびアイドル状態の CPU 時間のパーセンテージを表示します。ナイス値が負のタスクは、システム時間およびユーザ時間にもカウントされるため、CPU 使用率の合計が 100% を超えることがあります。

次のコマンドを入力します。

show cpu

次の例を参考にしてください。

```
user@GUARD# show cpu
Host CPU:  0.0% user,  0.1% system,  0.0% nice, 99.0% idle
```

ARP キャッシュの操作

ARP キャッシュを表示または操作して、アドレス マッピング エントリを消去または手動で定義できます。次のいずれかのコマンドを入力します。

arp [**-evn**] [**-H** *type*] [**-i** *if*] **-a** [*hostname*]

arp [**-v**] [**-i** *if*] **-d** *hostname* [**pub**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**temp**]

arp [**-v**] [**-H** *type*] [**-i** *if*] **-s** *hostname hw_addr* [**netmask** *nm*] **pub**

arp [**-v**] [**-H** *type*] [**-i** *if*] **-Ds** *hostname* ifa [**netmask** *nm*] **pub**

arp [**-vnD**] [**-H** *type*] [**-i** *if*] **-f** [*filename*]

表 11-19 で、**arp** コマンドの引数とキーワードについて説明します。

表 11-19　arp コマンドの引数とキーワード

パラメータ	説明
-v、--verbose	出力を詳細に表示します。
-n、--numeric	数値アドレスを表示します。
-H *type*、**--hw-type** *type*、**-t** *type*	Guard モジュールがチェックするエントリのクラスを指定します。このパラメータのデフォルト値は、ether（IEEE 802.3 10Mbps イーサネットに対応するハードウェア コード 0x01）です。
-a [*hostname*]、**--display** [*hostname*]	指定したホストのエントリを代替（BSD）形式で表示します。デフォルトでは、すべてのエントリが表示されます。
-d *hostname*、**--delete** *hostname*	指定したホストのエントリを削除します。
-D、**--use-device**	インターフェイス ifa のハードウェア アドレスを使用します。
-e	エントリをデフォルトの形式で表示します。

表 11-19　arp コマンドの引数とキーワード（続き）

パラメータ	説明
-i *If*、**--device** *If*	インターフェイスを指定します。ARP キャッシュをダンプすると、指定したインターフェイスに一致するエントリだけが出力されます。永続的または一時的な ARP エントリを設定する場合、このインターフェイスがそのエントリに関連付けられます。このオプションを使用しない場合、Guard モジュールはルーティング テーブルに基づいてインターフェイスを推測します。pub エントリの場合、これは Guard モジュールが ARP 要求に応えるインターフェイスで、IP データグラムのルーティング先のインターフェイスとは異なっている必要があります。
-s *hostname hw_addr*、**--set** *hostname*	ハードウェア アドレスを *hw_addr* クラスに設定して、ホスト *hostname* の ARP アドレス マッピング エントリを作成します。ほとんどのクラスでは、通常の表現を使用できます。
-f *filename*、**--file** *filename*	ARP アドレス マッピング エントリを作成します。情報は、ファイル *filename* から取得されます。ファイル形式は、ホスト名とハードウェア アドレスが空白で区切られた ASCII テキスト行です。pub、temp、および netmask フラグを使用することもできます。ホスト名を入力するどの場所にも、ドット区切り 10 進表記で IP アドレスを入力できます。

注意　Guard モジュールの ARP キャッシュを設定するには、Guard モジュール システムとネットワークの知識が必要です。

次の例を参考にしてください。

```
user@GUARD# arp -e

Address         HWtype  HWaddress           Flags Mask  Iface
10.10.1.254     ether   00:02:B3:C0:61:67   C           eth1
10.10.8.11      ether   00:02:B3:45:B9:F1   C           eth1
10.10.8.253     ether   00:D0:B7:46:72:37   C           eth1
10.10.10.54     ether   00:03:47:A6:44:CA   C           eth1
```

netstat の使用

ホスト ネットワーク接続、ルーティング テーブル、インターフェイス統計情報、マスカレード接続、およびマルチキャスト メンバシップを表示して、ネットワークの問題をデバッグできます。次のいずれかのコマンドを入力します。

netstat [*address_family_options*] [**--tcp**|**-t**] [**--udp**|**-u**] [**--raw**|**-w**] [**--listening**|**-l**] [**--all**|**-a**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--symbolic**|**-N**] [**--extend**|**-e**[**--extend**|**-e**]][**--timers**|**-o**] [**--program**|**-p**] [**--verbose**|**-v**] [**--continuous**|**-c**] [*delay*]

netstat {**--route**|**-r**} [*address_family_options*] [**--extend**|**-e**[**--extend**|**-e**]] [**--verbose**|**-v**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--interfaces**|**-i**} [*iface*] [**--all**|**-a**] [**--extend**|**-e**[**--extend**|**-e**]] [**--verbose**|**-v**] [**--program**|**-p**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--groups**|**-g**} [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--masquerade**|**-M**} [**--extend**|**-e**] [**--numeric**|**-n**] [**--numeric-hosts**][**--numeric-ports**][**--numeric-ports**] [**--continuous**|**-c**] [*delay*]

netstat {**--statistics**|**-s**} [**--tcp**|**-t**] [**--udp**|**-u**] [**--raw**|**-w**] [*delay*]

netstat {**--version**|**-V**}

netstat {**--help**|**-h**}

（注）　アドレス ファミリを指定しない場合、Guard モジュールは設定されているすべてのアドレス ファミリのアクティブなソケットを表示します。

表 11-20 で、**netstat** コマンドの引数とキーワードについて説明します。

表 11-20　netstat コマンドの引数とキーワード

パラメータ	説明
address_family_options	[--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]][--unix|-x][--inet|--ip] [--ax25] [--ipx] [--netrom] [--ddp]
--route、-r	Guard モジュールのルーティング テーブルを表示します。
--groups、-g	IPv4 および IPv6 のマルチキャスト グループ メンバシップ情報を表示します。
--interface、-i *iface*	すべてのネットワーク インターフェイスまたはインターフェイス *iface* のテーブルを表示します。
--masquerade、-M	マスカレード接続のリストを表示します。
--statistics、-s	各プロトコルのサマリー統計情報を表示します。
-v、--verbose	出力を詳細に表示します。
-n、--numeric	数値アドレスを表示します。
--numeric-hosts	数値ホスト アドレスを表示します。これは、ポート名およびユーザ名の解決に影響を及ぼしません。
--numeric-ports	数値ポート番号を表示します。これは、ホスト名およびユーザ名の解決に影響を及ぼしません。
--numeric-users	数値ユーザ ID を表示します。これは、ホスト名およびポート名の解決に影響を及ぼしません。
--protocol、-A *family*	接続を表示するアドレス低レベル プロトコル（ファミリ）を指定するカンマ区切りリスト。アドレス ファミリ inet には、raw、udp、および tcp プロトコル ソケットが含まれます。
-c、--continuous	選択した情報を 1 秒ごとに継続的に表示します。
-e、--extend	追加情報を表示します。最も詳しい情報を表示するには、このオプションを 2 回使用します。
-o、--timers	ネットワーキング タイマーに関連する情報を表示します。
-p、--program	各ソケットが属するプログラムの PID および名前を表示します。

表 11-20　netstat コマンドの引数とキーワード（続き）

パラメータ	説明
-l、--listening	リスニング ソケットだけを表示します。デフォルトでは、リスニング ソケットは省略されます。
-a、--all	リスニング ソケットと非リスニング ソケットの両方を表示します。
-F	FIB からのルーティング情報を表示します。
-C	ルート キャッシュからのルーティング情報を表示します。
delay	*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

1 つのコマンドに最大 13 の引数とキーワードを入力できます。

次の例を参考にしてください。

```
user@GUARD# netstat -v
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address   Foreign Address         State
tcp        0      0 localhost:1111  localhost:32777    ESTABLISHED
tcp        0      0 localhost:8200  localhost:32772    ESTABLISHED
.
.
.
tcp        0      0 localhost:33464 localhost:8200     TIME_WAIT
tcp        1      0 localhost:1113  localhost:33194    CLOSE_WAIT
.
.
.
Active UNIX domain sockets (w/o servers)
unix  2      [ ]         STREAM     CONNECTED     928
unix  3      [ ]         STREAM     CONNECTED     890  /tmp/.zserv
.
.
.
user@GUARD#
```

traceroute の使用

パケットがネットワーク ホストに到達するまでのルートを出力して、ネットワークの問題をデバッグできます。次のコマンドを入力します。

traceroute *ip-address* [**-F**] [**-f** *first_ttl*] [**-g** *gateway*] [**-i** *iface*] [**-m** *max_ttl*] [**-p** *port*] [**-q** *nqueries*] [**-s** *src_addr*] [**-t** *tos*] [**-w** *waittime*] [*packetlen*]

（注）　**traceroute** コマンドでは IP アドレスだけが表示され、名前は表示されません。

表 11-21 で、**traceroute** コマンドの引数とキーワードについて説明します。

表 11-21　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	どの IP アドレスへのルートをトレースするか。
-f *first_ttl*	最初の発信プローブ パケットで使用される最初の Time-To-Live（TTL; 存続可能時間）を設定します。
-F	*don't fragment* ビットを設定します。
-g *gateway*	ルース ソース ルート ゲートウェイを指定します（最大 8 個）。
-i *iface*	発信プローブ パケットの送信元 IP アドレスを取得するネットワーク インターフェイスを指定します。これは通常、マルチホーム ホストで役立ちます。
-m *max_ttl*	発信プローブ パケットで使用される最大存続可能時間（最大ホップ数）を設定します。デフォルトは 30 ホップです。
-p *port*	プローブで使用されるベース UDP ポート番号を設定します。デフォルトは 33434 です。
packetlen	プローブのパケットの長さを設定します。
-s *src_addr*	IP アドレス *src_addr* を発信プローブ パケットで送信元 IP アドレスとして設定します。

表 11-21　traceroute コマンドの引数とキーワード（続き）

パラメータ	説明
-t *tos*	プローブ パケットのサービス タイプを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	プローブに対する応答を待つ時間（秒）を設定します。デフォルトは 5 秒です。

次の例を参考にしてください。

```
user@GUARD# traceroute 10.10.10.34
traceroute to 10.10.10.34 (10.10.10.34), 30 hops max, 38 byte packets
 1 10.10.10.34 (10.10.10.34) 0.577 ms  0.203 ms  0.149 ms
```

ping の使用

ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続性を確認できます。次のコマンドを入力します。

ping *ip-address* [**-c** *count*] [**-i** *interval*] [**-l** *preload*] [**-s** *packetsize*] [**-t** *ttl*]
[**-w** *deadline*] [**-F** *flowlabel*] [**-I** *interface*]
[-Q *tos*] [**-T** *timestamp option*] [**-W** *timeout*]

表 11-22 で、**ping** コマンドの引数とキーワードについて説明します。

表 11-22　ping コマンドの引数とキーワード

パラメータ	説明
ip-address	宛先 IP アドレス。
-c *count*	*count* 個の ECHO_REQUEST パケットを送信します。deadline オプションが指定されている場合、ping はタイムアウトになるまでこの数の ECHO_REPLY パケットを待ちます。
-F *flow label*	エコー要求パケットに 20 ビットのフロー ラベルを割り当てて設定します（ping6 のみ）。値がゼロの場合は、ランダムなフロー ラベルが使用されます。
-i *interval*	パケットの送信間隔を *interval* 秒に設定します。デフォルトでは、1 秒に設定されます。
-I *interface*	送信元 IP アドレスを、指定したインターフェイス アドレスに設定します。
-l *preload*	応答を待たずに *preload* 個のパケットを送信します。
-Q *tos*	ICMP データグラムに Quality of Service（QoS）関連のビットを設定します。
-s *packetsize*	送信するデータ バイト数を指定します。デフォルトは 56 です。
-t ttl	IP の TTL を設定します。
-T *timestamp option*	特別な IP タイムスタンプ オプションを設定します。

表 11-22　ping コマンドの引数とキーワード（続き）

パラメータ	説明
-w *deadline*	送受信されたパケット数に関係なく ping が終了するまでのタイムアウト（秒）を指定します。
-W *timeout*	応答を待つ時間（秒）。

1 つのコマンドに最大 10 の引数とキーワードを入力できます。

次の例を参考にしてください。

```
user@GUARD# ping 10.10.10.30 -n 1
```

デバッグ情報の取得

Guard モジュールに動作上の問題が発生した場合は、シスコのテクニカルサポートがお客様に Guard モジュールの内部デバッグ情報のコピーを送信するようお願いすることがあります。Guard モジュールのデバッグ コア ファイルには、Guard モジュールの誤動作についてトラブルシューティングを行うための情報が含まれています。このファイルの出力は暗号化されており、Cisco TAC の担当者のみが使用するよう意図されています。

デバッグ情報を FTP サーバに抽出するには、次の手順を実行します。

ステップ 1　Guard モジュール のログ ファイルを表示します。詳細については、P.11-11 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を収集する時刻を特定します。問題があることを示している最初のログ メッセージを識別します。

ステップ 3　デバッグ情報を FTP サーバに抽出します。次のコマンドを入力します。

```
copy debug-core time ftp server full-file-name [login [password]]
```

表 11-23 で、**copy debug-core** コマンドの引数について説明します。

表 11-23　copy debug-core コマンドの引数

パラメータ	説明
time	デバッグ情報が必要となった原因のイベントの時刻。時刻の文字列では、*MMDDhhmm*[[*CC*]*YY*][*.ss*] という形式を使用します。 • *MM*：月（数値）。 • *DD*：日。 • *hh*：時（24 時間表記）。 • *mm*：分。 • *CC*：（オプション）年の最初の 2 桁（たとえば **20**05）。 • *YY*：（オプション）年の最後の 2 桁（たとえば 20**05**）。 • *.ss*：（オプション）秒（小数点が必要）。
server	FTP サーバの IP アドレス。
full-file-name	バージョン ファイルの完全な名前。パスを指定しない場合、サーバはユーザのホーム ディレクトリにファイルを保存します。
login	（オプション）FTP サーバのログイン名。ログイン名を入力しない場合、FTP サーバは匿名ログインであると想定し、パスワードを要求しません。
password	（オプション）FTP サーバのパスワード。パスワードを入力しない場合、入力するよう Guard モジュールから要求されます。

次の例を参考にしてください。

```
user@GUARD# copy debug-core 11090645 ftp 10.0.0.191
/home/debug/debug-file <user> <password>
```

Guard モジュールの自己保護設定の表示

独立した IP アドレスを持つネットワーク要素としての Guard モジュールは、潜在的な DDoS 攻撃の危険にさらされています。デフォルトの設定では、このような攻撃に対する保護が提供されます。ユーザは、この自己防衛保護設定にアクセスし、変更することができます。

注意　Guard　モジュールの自己防衛保護のデフォルト設定は変更しないことを強くお勧めします。不要な設定の結果として、Guard モジュールの自己保護機能に大きな支障をきたす場合があります。

Guard モジュールの自己防衛保護設定を変更するには、自己保護設定モードに入る必要があります。

自己保護設定モードに入るには、設定モードで次のコマンドを入力します。

self-protection

Guard モジュールの自己防衛保護に使用できるコマンドのセットは、通常のゾーンで使用できるものと同じです。ゾーンの設定の詳細については、第 6 章「ゾーンの設定」、第 7 章「ゾーンのフィルタの設定」、第 8 章「ポリシー テンプレートとポリシーの設定」、および第 9 章「インタラクティブ保護モード」を参照してください。

Guard モジュールの自己保護設定ファイルを表示するには、**show running-config** コマンドを使用します。詳細については、「Guard モジュールの設定の表示」を参照してください。

フレックスコンテンツ フィルタのデフォルト設定

Guard モジュールのフレックスコンテンツ フィルタは、明示的な指定がない限り、デフォルトですべてのトラフィック フローをブロック（ドロップ）するように設定されています。表 11-24 に、Guard モジュールが適切に機能するために必要な通信を可能にするためのフレックスコンテンツ フィルタのデフォルト設定を示します。

表 11-24　フレックスコンテンツ フィルタのデフォルト設定

サービス	IP プロトコル	送信元ポート	宛先ポート	同期の許可
ftp-control	6	21	*	no
ftp-data	6	20	*	yes
tacacs	6	49	*	yes
ssh	6	22	*	no
ssh	6	*	22	yes
https	6	*	443	yes
icmp	1	*	*	—
snmp	17	*	161	—
ssl	6	*	3220	no
ssl	6	3220	*	yes

フレックスコンテンツ フィルタのデフォルト設定は、次の内容で構成されます。

- Guard モジュールによって開始される FTP サーバとの FTP 通信をイネーブル化し、送信元ポート 21 で着信 FTP 制御 SYN パケットをブロックする。
- TACACS+ サーバとの TACACS 通信をイネーブル化し、送信元ポート 49 からの着信 SYN パケットをブロックする。この設定により、認証、認可、アカウンティングのための TACACS+ サーバとの通信が可能になります。
- 着信および発信 SSH 通信をイネーブルにする。
- 着信 HTTPS 通信をイネーブルにする。
- ICMP 通信をイネーブルにする。
- SNMP 通信をイネーブルにする。
- SSL 通信をイネーブルにする。