CHAPTER 13

Guard モジュールの診断ツールの使用

この章では、Cisco Anomaly Guard Module（Guard モジュール）に統計情報と診断を表示する方法について説明します。

（注）

1 Gbps で動作する Guard モジュールと、3 Gbps で動作する Guard モジュールでは、動作と設定に違いがあります。この章では、1 Gbps 動作と 3 Gbps 動作の違いについて説明します。特に記載がない限り、この章の情報は両方のモードの動作に適用されます。詳細については、P.1-9 の「1 Gbps と 3 Gbps の帯域幅オプションについて」を参照してください。

この章は、次の項で構成されています。

インストールされたソフトウェア バージョン番号とライセンス契約の表示

ソフトウェア ライセンス契約および使用する Guard モジュールにロードされたソフトウェア イメージのバージョン番号を表示できます。バージョン番号を表示することにより、次のどちらの帯域幅オプションを Guard モジュールが使用しているかを確認できます。

- 1 Gbps 動作：Guard モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 1 Gbps で、すべてのデータ トラフィックは 1 つのインターフェイス ポートのみを使用して移動します。
- 3 Gbps 動作：Guard モジュールとスーパーバイザ エンジン間のトラフィックの最大帯域幅は 3 Gbps で、すべてのデータ トラフィックは 3 つのインターフェイス ポートすべてを使用して移動します。インストールされたソフトウェア イメージで 3 Gbps 動作が許可される場合は、バージョン番号に XG 指定子（たとえば、Cisco Anomaly Guard Module Image version 6.0(0.39)-XG）が含まれています。

（注）　3 Gbps 動作の場合は、Guard モジュールを動作させるために、関連付けられたソフトウェア ライセンス キーをインストールしておく必要があります（P.13-2 の「ソフトウェア ライセンス キー情報の表示」を参照）。

ソフトウェア バージョン番号およびライセンス契約情報を表示するには、次のコマンドを使用します。

show version

ソフトウェア ライセンス キー情報の表示

Guard モジュールで 3 Gbps 動作に対応したソフトウェア イメージの XG バージョンを使用している場合は、XG ソフトウェア イメージのアクティブ化に必要なライセンス キーに関連した情報を表示できます。ライセンス キー情報を表示して、次の情報を確認します。

- ライセンス キーがロードされている。
- ライセンス キーの有効期限が切れていない。ライセンス キーがデモ バージョンの場合は、デモ ライセンス キーの有効期限の日付が表示されます。インストールされているライセンス キーが永続的に有効な場合は、有効期限日付として permanent という語が表示されます。

（注）　1 Gbps 動作に対応するソフトウェア イメージには、ライセンス キーは不要です。Guard モジュールに現在ロードされているソフトウェア イメージを確認するには、**show version** コマンドを使用します（P.13-2 の「インストールされたソフトウェア バージョン番号とライセンス契約の表示」を参照）。

ソフトウェア ライセンス キー情報を表示するには、次のコマンドを使用します。

show license-key

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、および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、次のコマンドを使用します。

show running-config [**all** | **guard** | **interfaces** [*interface_name*[*.vlan_name*]] | **self-protection** | **zones**]

表 13-1 に、**show running-config** コマンドの引数とキーワードを示します。

表 13-1　show running-config コマンドの引数とキーワード

パラメータ	説明
all	（オプション）Guard モジュールのすべての機能（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	（オプション）Guard モジュールの設定ファイルを表示します。
interfaces	（オプション）Guard モジュールのすべてのインターフェイス設定ファイルを表示します。
interface_name	（オプション）特定のインターフェイスの名前。 1 Gbps 動作の場合に有効な名前は次のとおりです。 • eth1 • giga 2 3 Gbps 動作の場合に有効な名前は次のとおりです。 • giga 1 • giga 2 • giga 3
.vlan_name	（オプション）特定の VLAN の名前。小数点（.）を入力し、続いて既存 VLAN の名前を（スペースなしで）入力します。
self-protection	（オプション）Guard モジュールの自己保護の設定を表示します。
zones	（オプション）すべてのゾーンの設定ファイルを表示します。

次の例は、Guard モジュールの設定ファイルを表示する方法を示しています。

```
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入力す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.13-4 の「Guard モジュールのゾーン動作ステータスの表示」を参照してください。

Guard モジュールのゾーン動作ステータスの表示

グローバル モードで次のコマンドを入力することにより、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。

show

表 13-2 に、指定可能なゾーンの動作状態を示します。

表 13-2　ゾーンのステータス

ステータス	説明
Auto protect mode	ゾーン保護がイネーブルで、動的フィルタはユーザの操作なしでアクティブになります。 Guard モジュールで、ゾーン保護がイネーブルで、Guard モジュールがポリシーのしきい値調整のためにゾーンのトラフィック特性をラーニングしている場合、ゾーン名の隣には「(+learning)」と表示されます。
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 モジュールは、ゾーンのトラフィックを分析して、ラーニング プロセスの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。

次の例は、Guard モジュールのゾーンの概要を表示する方法を示しています。

```
user@GUARD# show
```

カウンタを使用したトラフィックの分析

Guard モジュールおよびゾーン カウンタを表示することで、Guard モジュールが処理している現在のトラフィック上の情報を表示したり、ゾーン トラフィックを分析したり、監視タスクを実行することができます。

この項では、次のトピックについて取り上げます。

カウンタおよびトラフィック レートの平均の表示

ゾーン カウンタを表示するには、次のコマンドのいずれかを入力します。

- **show** [**zone** *zone-name*] **rates** : 正当なカウンタと悪意のあるカウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **rates details** : すべての Guard モジュール カウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **rates history** : 過去 24 時間における 1 分ごとの悪意のあるカウンタと正当なカウンタの平均トラフィック レートを表示します。
- **show** [**zone** *zone-name*] **counters** : Guard モジュールの悪意のあるカウンタと正当なカウンタを表示します。
- **show** [**zone** *zone-name*]**counters details** : すべての Guard モジュール カウンタを表示します。
- **show** [**zone** *zone-name*] **counters history** : 過去 1 時間の悪意のあるカウンタおよび正当なカウンタの値を 1 分ごとに表示します。

Guard モジュール カウンタを表示するには、グローバル モードまたは設定モードでこのコマンドを使用します。

ゾーン カウンタを表示するには、次のコマンド モードのいずれかでコマンドを使用します。

- ゾーン設定モード : すでに特定のゾーン設定モードになっているため、**zone** *zone-name* キーワードおよび引数を使用しないでください。
- グローバル モードまたは設定モード : **zone** キーワードおよび *zone-name* 引数を入力してゾーン名を指定します。

レート単位は、ビット / 秒（bps）およびパケット / 秒（pps）で表されます。

（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だけ使用できます。

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設定されます。

表 13-3 に、Guard モジュールのカウンタを示します。

表 13-3　Guard モジュール 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 モジュールの保護機能（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）によって攻撃の一部と判断され、ドロップされたパケット。
Replied	スプーフィング防止およびゾンビ防止機能の一部として、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（詳細についてはこの表の Replied カウンタ エントリを参照）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	保護がイネーブルになっているいずれのゾーンにも宛先変更されなかったトラフィック。この情報は、Guard モジュールのカウンタに限り使用可能です（**zone** キーワードを使用せずにグローバル モードまたは設定モードでコマンドを入力した場合）。

次の例は、Guard モジュールの平均トラフィック レートを表示する方法を示しています。

```
admin@GUARD# show rates
```

Guard モジュールおよびゾーンのカウンタのクリア

テストを行う予定で、カウンタにテスト セッションからの情報だけを含める場合は、Guard モジュールまたはゾーン カウンタをクリアできます。Guard モジュールはカウンタおよび平均トラフィック レートをクリアします。

Guard モジュールのカウンタをクリアするには、グローバル モードまたは設定モードで次のコマンドを使用します。

clear counters

次の例は、Guard モジュールのカウンタをクリアする方法を示しています。

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

ゾーン カウンタをクリアするには、次のコマンドのいずれかを入力します。

- **clear counters**（ゾーン設定モードで使用）
- **clear zone** *zone-name* **counters**（グローバル モードまたは設定モードで使用）*zone-name* 引数には、ゾーンの名前を指定します。

次の例は、ゾーン カウンタをクリアする方法を示しています。

```
user@GUARD-conf-zone-scannet# clear counters
```

ゾーンのステータスの表示

ゾーンの概要とそのステータスを表示するには、ゾーン設定モードで次のコマンドを使用します。

show

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：保護モード（自動またはインタラクティブ）、しきい値、タイマー、および 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.6-7 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、ユーザ フィルタの設定、およびアクティブな動的フィルタの数を含みます。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.7-4 の「フレックスコンテンツ フィルタの設定」および P.7-16 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.13-5 の「カウンタを使用したトラフィックの分析」を参照してください。

次の例は、ゾーン ステータスを表示する方法を示しています。

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

ゾーンのプロキシ使用率の表示

Guard モジュールでは、各ゾーンのプロキシの使用率が監視されます。Guard モジュールは、TCP 強化認証および Domain Name System（DNS; ドメイン ネーム システム）認証の処理中に、プロキシ IP アドレスを使用します。プロキシあたりの TCP ポートの数に限りがあるために、Guard モジュールがこのような処理を実行する機能は制限されます。使用可能なプロキシ ポートがない場合、Guard モジュールでは新しい認証接続を開始できず、接続がドロップされる結果になります。この問題を防ぐには、ゾーンで使用中のプロキシ ポートのパーセンテージを監視します。

ゾーンのプロキシ使用率の情報を表示するには、次のいずれかのコマンドを使用します。

- **show zone** *zone-name* **proxy-usage**（グローバル モードで使用）*zone-name* 引数は、プロキシの使用率を監視するゾーンの名前です。
- **show proxy-usage**（ゾーン設定モードで使用）

アクティブなゾーンで最大のプロキシ使用率だけを表示するには、グローバル モードまたは設定モードで次のコマンドを入力します。

show resources

詳細については、「システム リソースの監視」の項を参照してください。

Guard モジュールでは、使用中のプロキシ ポートのパーセンテージが Guard モジュールのポート単位（1 Gbps 動作の場合はポート 1 つ、3 Gbps 動作の場合はポート 3 つ）で表示されます。

あるゾーンで使用されているプロキシ ポートのパーセンテージを小さくするには、次のいずれかのアクションを実行します（推奨度の高い順に示します）。

- プロキシ IP アドレスの数を増やす：この方法を推奨します。詳細については、P.3-13 の「プロキシ IP アドレスの設定」を参照してください。
- ゾーン ポリシーのしきい値を再設定する：ポリシーのしきい値を引き上げて、強化保護レベルを必要とする送信元 IP アドレスを減らします。詳細については、P.8-16 の「ポリシーのしきい値の設定」を参照してください。
- ゾーンを TCP_NO_PROXY ゾーンにする：GUARD_TCP_NO_PROXY ゾーン テンプレートを使用して、ゾーンを再作成および再設定します。このゾーン テンプレートは強化保護レベルを使用していません。詳細については、P.6-4 の「新しいゾーンの作成」を参照してください。

次の例は、scannet ゾーンのプロキシ使用率を表示する方法を示しています。

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

5.0% (3225/64511)
```

Guard モジュールのログの管理

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エクスポートおよび表示して、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 13-4 に、イベント ログのレベルを示します。

表 13-4　イベント ログのレベル

イベント 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。

この項では、次のトピックについて取り上げます。

- ロギング パラメータの設定
- オンライン イベント ログの管理
- ログ ファイルの管理

ロギング パラメータの設定

Guard モジュールのログ ファイルの動作を制御するには、ロギング パラメータを設定します。

ロギング パラメータを設定するには、設定モードで次のコマンドを使用します。

logging {**device-log size** *logging-size-init* | **facility** {**local0** | **local1** | **local2** | **local3** | **local4** | **local5** | **local6** | **local7**} | **host** *remote-syslog-server-ip* | **trap** {**alerts** | **critical** | **debugging** | **emergencies** | **errors** | **informational** | **notifications** | **warnings**} | **zone-log size** *logging-size-init*}

表 13-5 に、**logging** コマンドの引数とキーワードを示します。

表 13-5　logging コマンドの引数とキーワード

パラメータ	説明
device-log size *logging-size-init*	Guard モジュールのすべてのログ ファイル用に割り当てるスペースを指定します。スペースの最大容量は 50 MB で、これがデフォルトの設定です。
facility	エクスポート syslog ファシリティを指定します。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 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を別のファイルで受信できます。 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。
host *remote-syslog-server-ip*	ログ ファイルのエクスポート時に使用するリモート syslog サーバの IP アドレスを指定します。IP アドレスとサブネット マスクをドット区切り 10 進表記で入力します（たとえば IP アドレスが 192.168.100.1、サブネット マスクが 255.255.255.0）。詳細については、「ログ ファイルのネットワーク サーバへのコピー」を参照してください。
trap	リモート syslog に送信する syslog トラップの重大度を指定します。低い重大度を指定した場合、それ以上の重大度がイベント ログに含まれます。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、重大度が高い方から順に次のようになります。 • **emergencies** • **alerts** • **critical** • **errors** • **warnings** • **notification** • **informational** • **debugging** デフォルトは **notification** です。詳細については、表 13-4 を参照してください。 （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** に設定してください。
zone-log size *logging-size-init*	ゾーンのすべてのログ ファイル用に割り当てるスペースを指定します。スペースの最大容量は 10 MB で、これがデフォルトの設定です。

ロギング パラメータの現在の設定を表示するには、グローバル モードまたは設定モードで、次のいずれかのコマンドを使用します。

- **show logging**
- **show running-config**

次の例は、ゾーンのログ用に 6 MB のスペースを割り当てる方法を示しています。

```
user@GUARD-conf# logging zone-log size 6
```

オンライン イベント ログの管理

この項では、Guard モジュールのイベントのリアルタイム ロギングを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- オンライン イベント ログの表示
- オンライン イベント ログのエクスポート

オンライン イベント ログの表示

Guard モジュールの監視機能をアクティブにして、リアルタイム イベント ログを表示すると、Guard モジュール イベントのオンライン ロギングを表示できます。オンライン イベント ログを表示するには、次のコマンドを使用します。

event monitor

次の例は、モニタリングをアクティブにする方法を示しています。

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

画面は新しいイベントを表示するために、定期的にアップデートされます。

（注）　モニタリング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、ログファイルに登録された Guard モジュールの動作を表示できます。また、Guard モジュールのログ ファイルに登録されている Guard モジュールのイベントをリモート ホストから表示できます。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 ファイルを複数の syslog サーバにエクスポートし、追加サーバを指定できるため、1 つのサーバがオフラインになっても、他のサーバがメッセージを受信できます。

Guard モジュールのオンライン ログのエクスポートは、リモート syslog サーバだけに適用できます。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.
```

システム ログ メッセージの構文は、次のとおりです。

event-date event-time Guard-IP-address protection-level 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）設定モードで次のコマンドを入力して、ロギング パラメータを設定します。

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

詳細については、「ロギング パラメータの設定」の項を参照してください。

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

logging host *remote-syslog-server-ip*

詳細については、「ロギング パラメータの設定」の項を参照してください。

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、**logging host** コマンドを複数回入力してください。

次の例は、重大度レベルが notification より高いトラップを送信するように Guard モジュールを設定する方法を示しています。Guard モジュールは、ファシリティ local3 を使用して、IP アドレス 10.0.0.191 の syslog サーバにトラップを送信します。

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

Guard モジュールがオンライン イベント ログのエクスポートに使用する設定を表示するには、**show logging** コマンドを使用します。

ログ ファイルの管理

この項では、Guard モジュールのログ ファイルを管理する方法について説明します。この項では、次のトピックについて取り上げます。

- ログ ファイルの表示
- ログ ファイルのネットワーク サーバへのコピー
- ログ ファイルのクリア

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、グローバル モードで次のコマンドを使用します。

show log

次の例は、Guard モジュールのログを表示する方法を示しています。

```
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.10-9 の「サブゾーンについて」を参照してください。

ログ ファイルのネットワーク サーバへのコピー

グローバル モードで次のいずれかのコマンドを入力することにより、監視または診断を行うために、Guard モジュールのログ ファイルをネットワーク サーバにコピーできます。

- **copy** [**zone** *zone-name*] **log ftp** *server full-file-name* [*login* [*password*]]
- **copy** [**zone** *zone-name*] **log** {**sftp** | **scp**} *server full-file-name login*

表 13-6 に、**copy log** コマンドの引数とキーワードを示します。

表 13-6　copy log ftp コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	（オプション）ゾーン名を指定します。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。
log	ログ ファイルをエクスポートします。
ftp	ログを FTP ネットワーク サーバにエクスポートします。
sftp	ログを SFTP ネットワーク サーバにエクスポートします。
scp	ログを SCP ネットワーク サーバにエクスポートします。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
full-file-name	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）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、Guard モジュールによってパスワードを要求されます。

（注）　**logging host** コマンドを使用すると、イベント ログを自動的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。詳細については、P.13-11 の「オンライン イベント ログのエクスポート」を参照してください。

Secure File Transfer Protocol（SFTP; セキュア ファイル転送プロトコル）および Secure Copy Protocol（SCP）は安全な通信を行うために Secure Shell（SSH; セキュア シェル）を使用します。したがって、**sftp** または **scp** オプションを指定して **copy** コマンドを入力したときに、Guard モジュールで使用される鍵が設定されていないと、Guard モジュールからパスワードの入力を求められます。Guard モジュールが安全な通信のために使用する鍵を設定する方法の詳細については、P.4-25 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

次の例は、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する方法を示しています。

```
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、またはテストを行う予定で、ログ ファイルにテスト セッションからの情報だけが含まれるようにする場合は、ログ ファイルをクリアすることができます。

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、ゾーン設定モードで次のコマンドを使用します。

clear log

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、設定モードで次のコマンドを使用します。

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

省略可能な **zone** *zone-name* のキーワードおよび引数で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。

次の例は、Guard モジュール ログをクリアする方法を示しています。

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

ネットワーク トラフィックの監視と攻撃シグニチャの抽出

ネットワークの動作を阻害しないタップを使用して、ネットワークから直接トラフィックを記録するように Guard モジュールを設定できます。記録されたトラフィックからデータベースを作成できます。記録されたトラフィックのデータベースのクエリーによって、過去のイベントの分析、攻撃シグニチャの生成、ネットワークの現在のトラフィック パターンと Guard モジュールで以前に正常のトラフィック状態で記録されたトラフィック パターンとの比較などを行うことができます。

フィルタを設定すると、特定の基準を満たすトラフィックだけを Guard モジュールで記録することや、すべてのトラフィック データを記録して、Guard モジュールに表示するトラフィックをフィルタリングするように指定できます。

Guard モジュールは、トラフィックを Packet Capturing Application Program（PCAP）形式で記録します。これは gzip（GNU zip）プログラムで圧縮および符号化され、記録されたデータを説明する Extensible Markup Language（XML）形式のファイルが添付されます。

Guard モジュールは、記録されたトラフィックを分析し、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できます。Guard モジュールには、記録されたトラフィックからシグニチャを抽出する機能が備わっています。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 モジュールでは、次の方法でトラフィックを記録できます。

- 自動：トラフィック データは持続的にパケットダンプ キャプチャ ファイルに記録されます。

  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。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、ネットワーク 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：ユーザがセッションの記録をアクティブにすると、トラフィックがパケットダンプ キャプチャ ファイルに記録されます。

  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、Guard モジュールでトラフィックの記録を再開する前に、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。

  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。すべてのゾーンの手動および自動パケットダンプ キャプチャ ファイル用には最大 80 MB のディスク領域を確保できます。将来のパケットダンプ キャプチャ ファイル用にディスク スペースを開放するため、古いファイルを削除する必要があります。

この項では、次のトピックについて取り上げます。

- 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 モジュールが自動的にネットワーク トラフィックを記録する機能をアクティブにして、ネットワーク問題のトラブルシューティングや攻撃トラフィックの分析を行うことができます。パケットダンプ キャプチャ フィルタを使用して、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 モジュールでは、ゾーン保護中またはラーニング中のトラフィックがキャプチャ バッファに記録されます。キャプチャ バッファのサイズが 20 MB に到達するか、または 10 分が経過すると、Guard モジュールはバッファされた情報を圧縮形式のローカル ファイルに保存し、バッファをクリアしてから、トラフィックの記録を継続します。

（注）　Guard モジュールでは、自動パケットダンプ キャプチャ機能を最大 4 つのゾーンで同時に実行できます。自動パケットダンプ キャプチャ機能がイネーブルになっている第 5 のゾーンに対してラーニングまたはゾーン保護をアクティブにすると、ゾーンはアクティブになりますが、パケットダンプ キャプチャ機能は実行されません。そのゾーンについてのキャプチャが実行されないことを示す syslog が発行されます。

Guard モジュールでは、キャプチャの期間内に、次のパケット処理方法に応じて、3 種類までのキャプチャ ファイルを作成できます。

- Forwarded（転送）：Guard モジュールからゾーンに転送された正当なトラフィックの送信元 IP アドレス。
- Dropped（ドロップ）：Guard モジュールによってドロップされた悪意のあるトラフィックの送信元 IP アドレス。
- Replied（返送）：検証処理中に Guard モジュールのスプーフィング防止機能およびゾンビ防止機能によって送信元に返送されたトラフィックの宛先 IP アドレス。

転送パケットダンプ キャプチャ ファイルだけが存在する場合、ゾーンはキャプチャの期間中に攻撃を受けなかったことになります。ドロップ キャプチャ ファイルまたは返送キャプチャ ファイルも作成された場合には、ゾーンに対する攻撃の可能性があります。Guard モジュールでは、3 種類あるパケットダンプ キャプチャ ファイルのいずれにも、IP サマライズが出力されます。IP サマライズとは、（トラフィックの量に応じて）最も頻繁に検出される IP アドレスのサマリーです。

返送パケットダンプ キャプチャ ファイルに提示される IP サマライズの情報を使用して、スプーフィング攻撃の送信元を特定できます。また、この情報はキャプチャ ファイルから抽出されて、ゾーン攻撃レポートの「Replied IP Summarization」の見出しの下に表示されます（P.12-7 の「Replied IP Summarizations」を参照）。

注意　返送 IP サマライズでより正確な結果が得られるようにするには、ゾーンに対する攻撃の期間中、パケットダンプ キャプチャ機能をイネーブルにしておく必要があります。攻撃中にパケットダンプ キャプチャ機能をディセーブルにした場合、返送 IP サマライズの情報が表示されないか、または正確でなくなる可能性があります。Guard モジュールでは、返送 IP サマライズの情報が攻撃レポートに表示されるのは、自動パケットダンプ キャプチャ機能がイネーブルになっている場合に限られます（手動でアクティブにされたパケットダンプ キャプチャの場合、返送 IP サマライズの情報は表示されません）。

（注）　IP サマライズのプロセスは多大なリソースを要します。リソースが少なくなると、プロセスは一時停止され、Guard モジュールからログ メッセージが発行されて、ゾーンのログに表示されます。キャプチャ xml ファイルには、IP サマライズ情報が障害のためにキャプチャ ファイルに記録されなかったことを示すステータス アトリビュートが表示されます。

Guard モジュールでは自動パケットダンプ キャプチャ ファイルに命名規則が適用され、Guard モジュールでトラフィックが記録された日時やトラフィックの処理方法に関する情報が与えられます。表 13-7 に、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を示します。

表 13-7　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
機能およびゾーン名	パケットダンプ キャプチャの際に Guard モジュールで実行されていたゾーン機能とそのゾーン名。ゾーン機能は次のとおりです。 • **protect**：Guard モジュールはゾーン保護中にトラフィックを記録。 • **learn**：Guard モジュールはゾーンのラーニング プロセス中または保護およびラーニング プロセス中にトラフィックを記録。
キャプチャ開始時刻	Guard モジュールでトラフィックの記録が開始した時刻。
キャプチャ終了時刻	（オプション）Guard モジュールでトラフィックの記録が終了した時刻。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の処理に使用する方式。この方式は次のいずれかになります。 • **forwarded**：Guard モジュールはトラフィックを正当であると識別して、ゾーンに転送する。 • **dropped**：Guard モジュールはトラフィックを悪意があるトラフィックであると識別して、削除する。 • **replied**：Guard モジュールは、スプーフィング防止およびゾンビ防止機能の一部として、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を送信する。

Guard モジュールは、ラーニング プロセスでは 1 つのパケットダンプ キャプチャ ファイルを、ゾーン保護がイネーブルのときには次の 2 つのタイプのパケットダンプ 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
- 現在のトラフィック

ゾーン保護をアクティブにするか、Guard モジュールでネットワーク トラフィックが自動的に記録されるように設定すると、保護プロセス中に記録された以前のパケットダンプ キャプチャ ファイルがすべて消去され、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、パケットダンプ キャプチャ ファイルをネットワーク サーバにエクスポートします。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。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。

P.13-21 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。

次の例は、自動的にゾーン 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方法を示しています。

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

Guard モジュールによるゾーン トラフィック データの自動キャプチャを停止するには、**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 モジュールがゾーン トラフィックの記録やキャプチャ ファイルの作成を行う機能を手動でアクティブにできるので、特定の期間のトラフィックをキャプチャできます。Guard モジュールで記録されるトラフィックのタイプを、次の中から指定することもできます。

- Forwarded：Guard モジュールからゾーンに転送された正当なトラフィック。
- Dropped：Guard モジュールによってドロップされた悪意のあるトラフィック。
- Replied：検証処理中に Guard モジュールのスプーフィング防止機能およびゾンビ防止機能によって送信元に返送されたトラフィック。
- All：転送、ドロップ、および返送されたトラフィック。

Forwarded（転送）、Dropped（ドロップ）、および Replied（返送）のタイプのパケットダンプ キャプチャ ファイル中には、IP サマライズが出力されます。IP サマライズとは、（トラフィックの量に応じて）最も頻繁に検出される送信元 IP アドレスのサマリーです。すべてのトラフィック タイプが含まれるキャプチャ ファイルには、IP サマライズは出力されません。

（注）　IP サマライズのプロセスは多大なリソースを要します。リソースが少なくなると、プロセスは一時停止され、Guard モジュールからログ メッセージが発行されて、ゾーンのログに表示されます。キャプチャ xml ファイルには、IP サマライズ情報が障害のためにキャプチャ ファイルに記録されなかったことを示すステータス アトリビュートが表示されます。

Guard モジュールは指定した数のパケットが記録されるか、またはラーニング プロセスとゾーン保護のいずれかが終了した時点で、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使用します。

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 13-8 に、**packet-dump** コマンドの引数とキーワードを示します。

表 13-8　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 モジュールでリアルタイムに記録されているトラフィックを表示します。
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。
pdump-rate	サンプル レート。単位はパケット / 秒（pps）。1 ～ 10000 の値を入力します。 （注）　Guard モジュールでは、同時に発生するすべての手動キャプチャについて、最大で 10,000 パケット / 秒の累積パケットダンプ キャプチャ レートがサポートされます。 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ため、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の数。Guard モジュールが指定した数のパケットの記録を終了した時点で、手動パケットダンプ キャプチャ バッファがファイルに保存されます。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。 （注）　**all** キーワードを入力した場合、そのキャプチャ ファイルに対して IP サマライズのプロセスは実行されません。キャプチャ xml ファイルには、この設定の **packet-dump** コマンドでは IP サマライズがサポートされないことを示すステータス アトリビュートが表示されます。
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。

表 13-8　packet-dump コマンドの引数とキーワード（続き）

パラメータ	説明
forwarded	Guard モジュールからゾーンに転送され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機能およびゾンビ防止機能によって送信元に返送され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.7-7 の「tcpdump 式の構文の設定」を参照してください。

次の例は、手動パケットダンプ キャプチャをアクティブにして、10 pps のサンプルレートで 1000 パケットを記録して、キャプチャしたパケットを表示する方法を示しています。

```
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 モジュールでは、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が記録された時点で、手動パケットダンプ キャプチャが停止します。ただし、指定した数のパケットが記録される前でも、次のいずれかの操作を実行すると、手動パケットダンプ キャプチャを停止できます。

- 開いている CLI セッションで **Ctrl+C** キーを押す。
- 新しい CLI セッションを開き、目的のゾーンの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

手動パケットダンプ キャプチャ ファイル用に Guard モジュールが割り当てたディスク スペースの現在の容量は、設定モードまたはグローバル モードで **show packet-dump** コマンドを使用することによって表示できます。Guard モジュールでは、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、単一ブロックのディスク スペースが割り当てられます。

次の例は、Guard モジュールがゾーンの手動パケットダンプ キャプチャ ファイルに割り当てるディスク スペースの現在の総計を表示する方法を示しています。

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

表 13-9 に、**show packet-dump** コマンド出力のフィールドを示します。

表 13-9　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	すべてのゾーンの手動パケットダンプ キャプチャ用に Guard モジュールが割り当てたディスク スペース総容量（メガバイト単位）。
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 ファイルによって使用されたパーセンテージ。

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

Guard モジュールは、FTP、SFTP、または SCP を使用してファイルを転送するネットワーク 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ように設定できます。自動エクスポート機能をイネーブルにすると、Guard モジュールでパケットダンプ バッファの内容がローカル ファイルに保存されるたびに、パケットダンプ キャプチャ ファイルがエクスポートされます。Guard モジュールは、gzip（GNU zip）プログラムで圧縮および符号化したパケットダンプ キャプチャ ファイルを PCAP 形式でエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。XML スキーマは、http://www.cisco.com/public/sw-center/ のソフトウェア センターからダウンロードできる Capture.xsd ファイルに記述されています。

Guard モジュールがパケットダンプ キャプチャ ファイルを自動的にエクスポートするように設定するには、設定モードで次のコマンドを使用します。

export packet-dump *file-server-name*

file-server-name 引数は、**file-server** コマンドを使用して設定したファイルをエクスポートするネットワーク サーバの名前を指定します。SFTP または SCP を使用するようにネットワーク サーバを設定する場合は、Guard モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。詳細については、P.14-7 の「ファイルの自動エクスポート」を参照してください。

次の例は、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-conf# export packet-dump Corp-FTP-Server
```

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

FTP、SFTP、または SCP を使用してファイルを転送するネットワーク サーバにパケットダンプ キャプチャ ファイルを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 モジュールは、gzip（GNU zip）プログラムで圧縮、符号化された PCAP 形式でパケットダンプ キャプチャ ファイルをエクスポートし、記録されたデータを説明する XML 形式のファイルを添付します。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。www.cisco.com からこのバージョンに付属の xsd ファイルをダウンロードできます。

パケットダンプ キャプチャ ファイルをネットワーク 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使用します。

- **copy zone** *zone-name* **packet-dump captures**[*capture-name*] **ftp** *server remote-path* [*login* [*password*]]
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] {**sftp** | **scp**} *server remote-path login*
- **copy zone** *zone-name* **packet-dump captures** [*capture-name*] *file-server-name*

表 13-10 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 13-10　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 *zone-name*	既存のゾーンの名前を指定します。
packet-dump captures	パケットダンプ キャプチャ ファイルのエクスポート。

表 13-10　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
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.13-24 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	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
remote-path	Guard モジュールがパケットダンプ キャプチャ ファイルを保存する場所の完全なパス名。
login	（オプション）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、Guard モジュールによってパスワードを要求されます。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用するネットワーク サーバを設定する場合は、Guard モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.14-7 の「ファイルの自動エクスポート」を参照してください。

SFTP および SCP は安全な通信を行うために SSH を使用します。したがって、**sftp** または **scp** オプションを指定して **copy** コマンドを入力したときに、Guard モジュールで使用される鍵が設定されていないと、Guard モジュールからパスワードの入力を求められます。Guard モジュールが安全な通信のために使用する鍵を設定する方法の詳細については、P.4-25 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 にエクスポートする方法を示しています。

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

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを **file-server** コマンドを使用して定義されたネットワーク サーバに手動でエクスポートする方法を示しています。

```
user@GUARD# copy zone scannet packet-dump captures cap-5-10-05 Corp-FTP-Server
```

パケットダンプ キャプチャ ファイルのインポート

ネットワーク サーバからパケットダンプ キャプチャ ファイルを Guard モジュールにインポートできるため、過去のイベントを分析することや、現在のネットワーク トラフィック パターンと Guard モジュールが以前に通常のトラフィック状態で記録したトラフィック パターンとを比較すること

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使用します。

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

表 13-11 に、**copy zone packet-dump** コマンドの引数とキーワードを示します。

表 13-11　copy zone packet-dump コマンドの引数とキーワード

パラメータ	説明
ftp	FTP を指定します。
sftp	SFTP を指定します。
scp	SCP を指定します。
zone *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を指定します。
server	ネットワーク サーバの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.10.2）。
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 プロセスが失敗する場合があります。
login	（オプション）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）FTP サーバのパスワード。パスワードを入力しない場合、Guard モジュールによってパスワードを要求されます。
file-server-name	ネットワーク サーバの名前。**file-server** コマンドを使用してネットワーク サーバを設定する必要があります。 SFTP または SCP を使用するネットワーク サーバを設定する場合は、Guard モジュールが SFTP 通信および SCP 通信で使用する SSH 鍵を設定する必要があります。 詳細については、P.14-7 の「ファイルの自動エクスポート」を参照してください。
capture-name	インポートするファイルの名前。Guard モジュールは、**file-server** コマンドを使用して、ネットワーク サーバとして定義したパスにファイルの名前を追加します。

SFTP および SCP は安全な通信を行うために SSH を使用します。したがって、**sftp** または **scp** オプションを指定して **copy** コマンドを入力したときに、Guard モジュールで使用される鍵が設定されていないと、Guard モジュールからパスワードの入力を求められます。Guard モジュールが安全な通信のために使用する鍵を設定する方法の詳細については、P.4-25 の「SFTP 接続および SCP 接続用の鍵の設定」を参照してください。

次の例は、ゾーン scannet のパケットダンプ キャプチャ ファイルを FTP サーバ 10.0.0.191 からインポートする方法を示しています。

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

次の例は、ネットワーク サーバからパケットダンプ キャプチャ ファイルをインポートする方法を示しています。

```
user@GUARD# copy CorpFTP running-config capture-1
```

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 モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。

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使用します。

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

表 13-12 に、**show packet-dump captures** コマンドの引数とキーワードを示します。

表 13-12　show packet-dump captures コマンドの引数とキーワード

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 モジュールはすべてのゾーンのパケットダンプ キャプチャ ファイルのリストを表示します。コマンド出力のフィールドの説明については、表 13-13 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。
ip summarization	記録されたパケットについての IP サマライズ情報を表示する。詳細については、「Guard モジュールの設定によるトラフィックの自動記録」の項を参照してください。
tcpdump-expression	（オプション）Guard モジュールでパケットダンプ キャプチャ ファイルを表示する際に使用されるフィルタ。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.7-7 の「tcpdump 式の構文の設定」を参照してください。

次の例は、パケットダンプ キャプチャ ファイルのリストを表示する方法を示しています。

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

表 13-13 に、**show packet-dump captures** コマンド出力のフィールドを示します。

表 13-13　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 ファイルの名前の説明については、表 13-7 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。単位はメガバイト。
Filter	Guard モジュールがトラフィックの記録時に使用する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.7-7 の「tcpdump 式の構文の設定」を参照してください。

次の例は、protect/PacketDump121_Oct-25-17:18:56_Oct-25-17:28:56_forwarded パケットダンプの IP サマライズ情報を表示する方法を示しています。

```
user@GUARD-conf-zone-scannet# show packet-dump captures
protect/PacketDump121_Oct-25-17:18:56_Oct-25-17:28:56_forwarded ip summarization
```

表 13-14 に、**show packet-dump captures ip summarization** コマンド出力のフィールドを示します。

表 13-14　show packet-dump captures ip summarization コマンド出力のフィールドの説明

フィールド	説明
Subnet	記録されたパケット タイプで最も頻繁に検出された IP アドレス。転送パケットおよびドロップ パケットの場合、リストに記載される IP アドレスはパケットの送信元 IP アドレスです。返送パケット タイプでは、IP アドレスはパケットの宛先 IP アドレスになります。
Subnet Mask	記録されたパケット タイプ（転送、ドロップ、返送）のサブネット マスク。
Weight(%)	記録されたサンプルの合計のうち、サブネット IP アドレスから送信され、Guard モジュールによって記録されたサンプル数のパーセンテージ。
Unique Addresses	サブネットに属する固有なアドレスの数。

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攻撃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同じタイプの将来の攻撃をすばやく識別できます。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 リストなどで）シグニチャが公開される前であっても、新しい DDoS 攻撃（分散型サービス拒絶攻撃）やインターネット ワームを検出できます。

Guard モジュールでは、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、攻撃シグニチャを生成できます。攻撃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、攻撃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.7-4 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。

攻撃シグニチャの生成プロセスを実行する際、クリーンな（正当な）トラフィックが含まれる参照用のパケットダンプ キャプチャ ファイルを指定することによって、生成される攻撃シグニチャの正確性を判定できます。Guard モジュールで悪意のあるトラフィックが含まれるパケットダンプ キャプチャ ファイルから攻撃シグニチャが生成されると、Guard モジュールにより分析が実行され、攻撃シグニチャが参照用のパケットダンプ キャプチャ ファイルのクリーンなトラフィックに現れる頻度が判定されます。分析の結果は、参照用のパケットダンプ キャプチャ ファイルにおけ

る、パケット数に対して攻撃シグニチャの出現数が占める割合として表示されます。割合の値が 10% 未満の場合、攻撃シグニチャは正確なので、このシグニチャを悪意のあるトラフィックの検出に使用できます。

割合の値が 10% を超える場合、シグニチャの生成プロセスは失敗したことになります。このシグニチャを悪意のあるトラフィックの検出に使用しないでください。Guard モジュールでクリーンなトラフィックが悪意のあるトラフィックとして誤認される結果になります。シグニチャの生成プロセスが失敗する原因として、次のようなことが考えられます。

- 悪意のあるトラフィックが含まれるパケットダンプ キャプチャ ファイルに、有効なトラフィックも含まれている。シグニチャの生成プロセスの間は、悪意のあるトラフィックだけが含まれるパケットダンプ キャプチャ ファイルを使用してください。
- Guard モジュールのシグニチャの生成アルゴリズムでは、悪意のあるトラフィックのサンプルから固有のシグニチャを検出できない。

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　**packet-dump capture** コマンドを使用して、Guard モジュールをアクティブにし、攻撃中のトラフィックを記録します。

詳細については、P.13-18 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」を参照してください。

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。パケットダンプ キャプチャ ファイルのリストを表示するには、**show packet-dump captures** コマンドを使用します。

詳細については、P.13-24 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 13-15 に、**show packet-dump signatures** コマンドの引数を示します。

表 13-15　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。Guard モジュールにより、分析が実行され、攻撃シグニチャが参照用のファイルに現れる頻度が判定されます。

表 13-16 に、**show packet-dump signatures** コマンド出力のフィールドを示します。

表 13-16　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のオフセット（バイト単位）。ここでパターンが開始します。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のオフセット（バイト単位）。ここでパターンが終了します。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 モジュールでは、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、シグニチャが生成されます。詳細については、P.7-10 の「パターン式構文の設定」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	参照用のパケットダンプ キャプチャ ファイルにおける、パケット数に対して攻撃シグニチャの出現数が占める割合。

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。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 ファイルをコピーする場合、Guard モジュールはこれらのファイルを手動ファイルとして保存します。既存の自動パケットダンプ キャプチャ ファイルを保存したい場合は、Guard モジュールによって新しいファイルで上書きされる前に、コピーを作成しておく必要があります。

ディスク スペースを解放する必要がある場合は、パケットダンプ キャプチャ ファイルを手動で削除します。詳細については、P.13-28 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使用します。

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

表 13-17 に、**copy zone packet-dump captures** コマンドの引数とキーワードを示します。

表 13-17　copy zone packet-dump captures 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	既存のパケットダンプ キャプチャ ファイルの名前。

表 13-17　copy zone packet-dump captures コマンドの引数とキーワード（続き）

パラメータ	説明
tcpdump-expression	（オプション）Guard モジュールでパケットダンプ キャプチャ ファイルのコピーに使用されるフィルタ。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.7-7 の「tcpdump 式の構文の設定」を参照してください。
new-name	新しいパケットダンプ キャプチャ ファイルの名前。 名前は、1 ～ 63 文字の英数字の文字列で、スペースを含めることはできませんが、アンダースコアを含めることはできます。

次の例は、パケットダンプ キャプチャ ファイル capture-1 の一部で capture-2 という名前のキャプチャ ファイルに適合する部分をコピーする方法を示しています。

```
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。

ゾーンごとに保存できる手動パケットダンプ キャプチャ ファイルは 1 つだけです。また、Guard モジュールに保存できるパケットダンプ キャプチャ ファイルは 10 個までです。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使用します。

- **clear zone** *zone-name* **packet-dump captures** {***** | *name*}（設定モードで）
- **clear packet-dump captures** {***** | *name*}（ゾーン設定モードで）

表 13-18 に、**clear packet-dump** コマンドの引数とキーワードを示します。

表 13-18　clear packet-dump コマンドの引数とキーワード

パラメータ	説明
zone *zone-name*	既存のゾーンの名前を指定します。
*****	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	削除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 ファイルを削除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

一般的な診断データを表示するには、次のコマンドを使用します。

show diagnostic-info [**details**]

診断データには、次の情報があります。

- Line Card Number：Guard モジュール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 モジュールの BIOS のベンダー。
- BIOS Version：Guard モジュールの BIOS バージョン。
- Total available memory：Guard モジュールで使用可能なメモリの合計量。
- Size of compact flash：Guard モジュールのコンパクト 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番号（スイッチまたはルータのモデル番号に応じて、1 ～ 13）。
- CFE version：CFE 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** コマンドを使用します。詳細については、P.14-17 の「新しいフラッシュ バージョンの焼き付けによる CFE のアップグレード」を参照してください。

- Recognition Average Sample Loss：計算済みの平均パケット 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 の値が大きい場合、Guard モジュールのトラフィックが過負荷の状態に陥っています。複数の Guard モジュールを負荷分散型構成に設置することをお勧めします。

フラッシュ メモリの使用率の表示

Guard モジュールは、アクティビティ ログおよびゾーン攻撃レポートを保持します。ディスクの使用率が 75% を超えている場合、または Guard モジュールに多数のゾーン（500 を超える）が定義されている場合は、ファイル履歴パラメータの値を小さくすることをお勧めします。使用されているディスク スペースが最大ディスク容量の約 80% に達すると、Guard モジュールは syslog に警告メッセージを表示します。

Guard モジュールが警告メッセージを表示した場合、ゾーン攻撃レポートをネットワーク サーバにエクスポートし、古い攻撃レポートを削除できます（P.12-14 の「攻撃レポートのエクスポート」および P.12-17 の「攻撃レポートの削除」を参照）。

Guard モジュールのレコードをネットワーク サーバに定期的に格納してから、ログをクリアすることをお勧めします。

（注）　ディスク使用率がディスクの最大キャパシティの 80% に達すると、Guard モジュールは情報を消去して、ディスク使用率を約 75% に減らします。

Guard モジュール上にインストールしたフラッシュの全体量の中で利用できるフラッシュの容量を表示するには、グローバル モードで次のコマンドを使用します。

show flash-usage

次の例は、フラッシュ メモリの使用率を表示する方法を示しています。

```
user@GUARD# show flash-usage
2%
```

メモリ消費量の表示

Guard モジュールは次の情報を表示します。

- メモリ使用量（KB 単位）。
- Guard モジュール統計エンジンが Anomaly Detection Engine Used Memory フィールドとして使用するメモリのパーセンテージ。

異常検出エンジンのメモリ使用量は、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）　異常検出エンジンのメモリ使用率が 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。

Guard モジュールのメモリ消費量を表示するには、次のコマンドを使用します。

show memory

次の例は、Guard モジュールのメモリ消費量を表示する方法を示しています。

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

    Anomaly detection engine used memory: 0.3%
```

（注）　Guard モジュールの空きメモリの合計量は、空きメモリとキャッシュ メモリの合計です。

CPU 使用率の表示

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（負のナイス値を持つタスク、ナイス値はプロセスの優先順位を表す）、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の両方で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。

現在の CPU 使用率を表示するには、次のコマンドを使用します。

show cpu

次の例は、現在の CPU 使用率の表示方法を示しています。

```
user@GUARD# show cpu
Host CPU1: 0.0% user, 0.1% system, 0.1% nice, 98.0% idle
```

システム リソースの監視

グローバル モードまたは設定モードで次のコマンドを入力することで、Guard モジュールがシステム ステータスの分析および監視の支援に使用しているリソースの概要を表示できます。

show resources

次の例は、システム リソースを表示する方法を示しています。

```
user@GUARD# show resources
```

表 13-19 に、**show resources** コマンド出力のフィールドを示します。

表 13-19　show resources コマンド出力のフィールドの説明

フィールド	説明
Host CPU1	ユーザ モード、システム モード、ナイス値が負のタスク（負のナイス値を持つタスクで、プロセスの優先順位を表す）、およびアイドル状態における CPU1 の CPU 時間のパーセンテージ。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。
Flash space usage Flash space usage	Guard モジュールが使用している、割り当て済みのフラッシュ スペースのパーセンテージ。 フラッシュ スペースの使用率がフラッシュの最大キャパシティの約 75% に達すると、Guard モジュールは syslog に警告メッセージを表示し、トラップを送信します。 **（注）** フラッシュ使用率がフラッシュの最大キャパシティの 80% に達すると、Guard モジュールは情報を自動的に消去して、フラッシュ使用率を約 75% に減らします。 Guard モジュールのレコードをネットワーク サーバに定期的に格納してから、古いレコードを削除することをお勧めします。 フラッシュ スペースの使用率が 80% に達した場合、ゾーン トラフィック レポートをネットワーク サーバにエクスポートし、古い攻撃レポートを削除できます（P.12-14 の「攻撃レポートのエクスポート」および P.12-17 の「攻撃レポートの削除」を参照）。
Accelerator card memory usage	アクセラレータ カードがポート単位（1 Gbps 動作の場合はポート 1 つ、3 Gbps 動作の場合はポート 3 つ）で使用するメモリのパーセンテージ。 アクセラレータ カードのメモリ使用率が 85 パーセントを超えると、Guard モジュールは SNMP トラップを生成します。値が大きいときは、Guard モジュールが大量のトラフィックを監視している場合があります。
Accelerator card CPU utilization	ポート単位（1 Gbps 動作の場合はポート 1 つ、3 Gbps 動作の場合はポート 3 つ）で活用されるアクセラレータ カード CPU のパーセンテージ。 アクセラレータ カードの CPU の使用率が 85 パーセントを超えた場合、Guard モジュールは SNMP トラップを生成します。値が大きいときは、Guard モジュールが大量のトラフィックを監視している場合があります。

表 13-19　show resources コマンド出力のフィールドの説明（続き）

フィールド	説明
Anomaly detection engine used memory	Guard モジュール統計エンジンが使用するメモリのパーセンテージを指定。異常検出エンジンのメモリ使用率は、アクティブなゾーンの数、各ゾーンが監視するサービスの数、Guard モジュールが監視しているスプーフィングされていないトラフィックの合計に影響されます。 異常検出エンジンのメモリ使用率が 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。
Dynamic filters used	すべてのゾーンでアクティブな動的フィルタの総数。Guard モジュールは、アクティブな動的フィルタの数と、Guard モジュールがサポートする動的フィルタの総数（150,000）に対するアクティブな動的フィルタのパーセンテージを表示します。アクティブな動的フィルタの数が 150,000 に到達すると、Guard モジュールは重大度 EMERGENCY の SNMP トラップを生成します。アクティブな動的フィルタの数が 135,000 に到達すると、Guard モジュールは、重大度 WARNING の SNMP トラップを生成します。 値が大きいときは、Guard モジュールが大量の DDoS 攻撃のトラフィックを監視していることを示します。
Top proxy usage	使用中のプロキシ ポートのパーセンテージ。Guard モジュールのポート単位（1 Gbps 動作の場合はポート 1 つ、3 Gbps 動作の場合はポート 3 つ）で表示されます。特定のゾーンのプロキシ使用率を表示するには、「ゾーンのプロキシ使用率の表示」の項を参照してください。

Guard モジュールが生成するトラップの詳細については、表 4-14 を参照してください。

ARP キャッシュの管理

Address Resolution Protocol（ARP; アドレス解決プロトコル）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。ARP キャッシュを管理するには、設定モードで次のコマンドを使用します。

arp {**-a** [*arp_hostname*] | **-d** *arp_hostname* | **-n** [*arp_hostname*] | **-s** *arp_hostname hw_addr*}

表 13-20 に、**arp** コマンドの引数とキーワードを示します。

表 13-20　arp コマンドの引数とキーワード

キーワード	説明
-a [*arp_hostname*]	ホストのエントリを代替（BSD）形式で表示します。オプションのホスト名を入力すると、指定したホストのみのエントリが表示されます。グローバル コンフィギュレーション モードでこの **arp** コマンド オプションを実行することもできます。
-d *hostname*	指定したホストのエントリを削除します。
-n *arp_hostname*	ホストの数値アドレスを表示します。オプションのホスト名を入力すると、指定したホストのみの数値アドレスが表示されます。グローバル コンフィギュレーション モードでこの **arp** コマンド オプションを実行することもできます。
-s *arp_hostname hw_addr*	ハードウェア アドレスを *hw_addr* クラス値に設定して、hostname の ARP アドレス マッピング エントリを作成します。

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に精通している必要があります。

ネットワーク統計情報の表示

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、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するには、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-users**] [**--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-users**] [**--continuous** | **-c**] [*delay*]

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

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

netstat {**--masquerade** | **-M**} [**--extend** | **-e**] [**--numeric** | **-n**] [**--numeric-hosts**] [**--numeric-ports**] [**--numeric-users**] [**--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 13-21 に、**netstat** コマンドの引数とキーワードを示します。

（注）　キーワードを完全に入力することも、キーワードの省略形を入力することもできます。キーワードの省略形には、先頭にダッシュ（-）が付きます。完全なキーワードには先頭にダッシュが 2 つ（--）付きます。

表 13-21　netstat コマンドの引数とキーワード

パラメータ名の省略形	パラメータの完全な名前	説明
address_family_options		（オプション）アドレス ファミリ オプションは、次のいずれかです。 • [--protocol={inet,unix,ipx,ax25,netrom,ddp}[,...]] • [--unix|-x] [--inet|--ip] [--ax25] [--ipx] [--netrom] • [--ddp]
-r	**--route**	Guard モジュールのルーティング テーブルを表示します。
-g	**--groups**	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。
-i *iface*	**--interface** ***iface***	すべてのネットワーク インターフェイスまたはオプションの *iface* 値のテーブルを表示します。

表 13-21　netstat コマンドの引数とキーワード（続き）

パラメータ名の省略形	パラメータの完全な名前	説明
-M	**--masquerade**	Network Address Translation（NAT; ネットワーク アドレス変換）が使用されたマスカレード接続のリストを表示します。
-s	**--statistics**	各プロトコルのサマリー統計情報を表示します。
-v	**--verbose**	（オプション）出力を詳細に表示します。
-n	**--numeric**	（オプション）数値アドレスを表示します。
	--numeric-hosts	（オプション）数値ホスト アドレスを表示しますが、ポートまたはユーザ名の解決には影響を与えません。
	--numeric-ports	（オプション）数値ポート番号を表示しますが、ホストまたはユーザ名の解決には影響を与えません。
	--numeric-users	（オプション）数値ユーザ ID を表示しますが、ホストまたはポート名の解決には影響を与えません。
-c	**--continuous**	（オプション）選択した情報を 1 秒ごとに継続的に表示します。
-e	**--extend**	（オプション）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**	（オプション）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**	（オプション）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。
-l	**--listening**	（オプション）リスニング ソケットだけを表示します。デフォルトでは、これらのソケットは省略されます。
-a	**--all**	（オプション）リスニング ソケットおよび非リスニング ソケットの両方を表示します。
delay		（オプション）*delay* 秒ごとに、netstat が統計情報からの出力を繰り返します。

（注）　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。

次の例は、netstat 情報を詳細に表示する方法を示しています。

```
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

次のコマンドを入力することで、ネットワーク問題をデバッグするために、パケットがネットワーク ホストに到達するまでに取るルートを決定できます。

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 13-22 に、**traceroute** コマンドの引数とキーワードを示します。

表 13-22　traceroute コマンドの引数とキーワード

パラメータ	説明
ip-address	ルートがトレースされる IP アドレス。
-F	（オプション）*don't fragment* ビットを設定します。
-f *first_ttl*	（オプション）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。
-g *gateway*	（オプション）ルース ソース ルート ゲートウェイを指定します。各ゲートウェイに対して **-g** を使用することで、2 つ以上のゲートウェイを指定できます。ゲートウェイの最大数は 8 個です。
-i *iface*	（オプション）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*	（オプション）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*	（オプション）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。
-q *nqueries*	（オプション）ttl 値に対して定義されるプローブの数を設定します。デフォルトは 3 です。
-s *src_addr*	（オプション）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。
-t *tos*	（オプション）プローブ パケットのタイプ オブ サービスを、*tos* の値に設定します。デフォルトはゼロです。
-w *waittime*	（オプション）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。
packetlen	（オプション）プローブ パケットの長さを設定します。

次の例は、IP アドレス 10.10.10.34 へのルートをトレースする方法を示しています。

```
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
```

接続の確認

次のコマンドを入力することにより、ネットワーク ホストに ICMP ECHO_REQUEST パケットを送信して、接続を確認できます。

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 13-23 に、**ping** コマンドの引数とキーワードを示します。

表 13-23　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*	（オプション）ECHO_REQUEST パケットを *count* 個送信します。deadline オプションが指定されている場合、このコマンドはタイムアウトになるまで *count* 個の ECHO_REPLY パケットを待ちます。
-i *interval*	（オプション）パケットの送信を待ちます。この間隔は秒で表されます。デフォルトでは、1 秒に設定されます。
-l *preload*	（オプション）応答を待たずに *preload* 個のパケットを送信します。
-s *packetsize*	（オプション）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	（オプション）IP の TTL を設定します。
-w *deadline*	（オプション）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。
-F *flow label*	（オプション）各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。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 *interface*	（オプション）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。
-Q *tos*	（オプション）Internet Control Message Protocol（ICMP; インターネット制御メッセージ プロトコル）データグラムに Type of Service（ToS; タイプ オブ サービス）関連のビットを設定します。
-T *timestamp option*	（オプション）特別な IP タイムスタンプ オプションを設定します。
-W *timeout*	（オプション）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。

次の例は、1 つの ICMP ECHO_REQUEST パケットを IP アドレス 10.10.10.30 に送信する方法を示しています。

```
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 TAC 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。

デバッグ情報をリモート 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 ログ ファイルを表示します。

詳細については、P.13-12 の「ログ ファイルの表示」を参照してください。

ステップ 2　デバッグ情報を抽出する時期を判断するため、問題を示す最初のログ　メッセージを識別します。Guard モジュールは、指定した時間から現在の時間までのデバッグ情報を抽出します。

ステップ 3　グローバル モードで次のコマンドを入力して、FTP サーバにデバッグ情報を抽出します。

```
copy debug-core time {ftp | scp | sftp} server full-file-name [login [password]]
```

表 13-24 に、**copy debug-core** コマンドの引数とキーワードを示します。

表 13-24　copy debug-core コマンドの引数とキーワード

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）。
ftp	FTP を指定します。
scp	SCP を指定します。
sftp	SFTP を指定します。
server	リモート 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、Guard モジュールによってパスワードを要求されます。

次の例は、今年の 11 月 9 日 午前 6:45 のデバッグ情報を FTP サーバ 10.0.0.191 に抽出する方法を示しています。

```
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。Guard モジュールの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。不要な設定変更を行うと、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。

自己保護設定モードに入って、Guard モジュールの自己防衛保護設定を変更するには、設定モードで次のコマンドを使用します。

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するコマンドと同じです。詳細については、次の章を参照してください。

- 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」
- 第 11 章「インタラクティブ保護モードの使用方法」

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、P.13-3 の「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について

デフォルトでは、Guard モジュールのフレックスコンテンツ フィルタは、明示的に指定されない限り、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 13-25 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 13-25　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
mdm	6	*	1334	yes

フレックスコンテンツ フィルタのデフォルト設定で、次の機能がイネーブルになります。

- Guard モジュールによって開始される FTP サーバとの FTP 通信。ただし、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。
- 認証、認可、アカウンティングのための TACACS+ サーバとの TACACS 通信。ただし、送信元ポート 49 からの着信 SYN パケットをブロックする。
- 着信および発信 SSH 通信。
- 着信 HTTPS 通信。
- ICMP 通信。
- SNMP 通信。
- SSL 通信。
- Cisco MultiDevice Manager（MDM）通信。