



Guard の診断ツールの使用

この章では、Cisco Guard (Guard) 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 の設定の表示](#)
- [Guard のゾーンの表示](#)
- [ゾーンのカウンタの表示](#)
- [ゾーンのステータスの表示](#)
- [Guard のログの表示](#)
- [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](#)
- [一般的な診断データの表示](#)
- [メモリ消費量の表示](#)
- [CPU 使用率の表示](#)
- [ARP キャッシュの操作](#)
- [netstat の使用](#)
- [traceroute の使用](#)
- [ping の使用](#)
- [デバッグ情報の取得](#)
- [Guard の自己保護設定の表示](#)

Guard の設定の表示

Guard 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 の設定に関する情報が含まれています。

Guard 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 | interfaces interface-name | router |
self-protection | zones]
```

表 10-1 に、`show running-config` コマンドのキーワードを示します。

表 10-1 show running-config コマンドのキーワード

パラメータ	説明
all	Guard のすべてのモジュール（Guard、ゾーン、インターフェイス、ルータ、および自己保護）の設定ファイルを表示します。
Guard	Guard の設定ファイルを表示します。
interfaces	Guard 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。
router	ルータの設定を表示します。
self-protection	Guard 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 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 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たり、別の Guard にその Guard 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.10-3 の「Guard のゾーンの表示」を参照してください。

Guard 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 10-2 で、さまざまなゾーンステータスについて説明します。

表 10-2 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。 Guard で、ゾーンが自動保護モードになっていて、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がラーニングされている場合、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 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 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 の Malicious カウンタと Legitimate カウンタを表示します。
- **show counters details** : Guard のカウンタをすべて表示します。
- **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 10-3 に、Guard のカウンタを示します。

表 10-3 Guard 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 によってゾーンに転送された正当なトラフィック。
Received	Guard 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 によってゾーンに転送された正当なトラフィック。
Dropped	Guard 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）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 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 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
```

ゾーンの状態の表示

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状態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。

- **ゾーンの状態**：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、ゾーンの基本設定を示します。詳細については、[P.5-9](#) 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せん。詳細については、[P.6-7](#) の「[フレックスコンテンツ フィルタの設定](#)」および [P.6-23](#) 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.10-4](#) 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-scanner# show
```

Guard のログの表示

Guard 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 のログを表示して、Guard のアクティビティを確認および追跡できます。

表 10-4 に、イベント ログのレベルを示します。

表 10-4 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 (emergencies、alerts、critical、errors、warnings、notification、informational、debugging) が表示されます。Guard 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.10-8 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.10-10 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 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 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 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ている Guard の動作を表示できます。Guard のイベントは Guard 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 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 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 のオンライン ログのエクスポート機能は、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 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) ログング 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 10-5 で、**logging** コマンドのキーワードについて説明します。

表 10-5 logging コマンドのキーワード

パラメータ	説明
facility	<p>エクスポート syslog ファシリティ。リモート syslog サーバは、ログング 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、ログング ファシリティを使用すると、リモート ユーザは、Guard 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。</p> <p>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。</p>
trap	<p>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。</p>



(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。

Guard のログの表示

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、*local3* ファシリティを使用して、*notification* 以上の重大度レベルのトラップが IP アドレス *10.0.0.191* の syslog サーバに送信されるように、Guard 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 のログを表示できます。Guard 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 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.5-40 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 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 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.3-36 の「SFTP 接続のための鍵の設定」を参照してください。

表 10-6 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 10-6 copy log ftp コマンドの引数

パラメータ	説明
<i>zone-name</i>	(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 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。
<i>server</i>	サーバの IP アドレス。
<i>remote-path</i>	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。

表 10-6 copy log ftp コマンドの引数 (続き)

パラメータ	説明
<i>login</i>	サーバのログイン名。 <i>login</i> 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。
<i>password</i>	(オプション) リモート FTP サーバのパスワード。パスワードを挿入しない場合、Guard によってパスワードを要求されません。

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 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 ファイルがテストセッションからの情報だけを反映する場合は、ログ ファイルをクリアすることができます。

Guard 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 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
```

主にハードウェアに関連したイベント メッセージ (デバイスの電源を切るか再起動した回数など) が含まれる BIOS システム ログをクリアできます。

BIOS システム ログをクリアするには、設定モードで次のコマンドを入力します。

clear log bios

次の例を参考にしてください。

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

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、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 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 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。

フィルタを設定して、特定の基準を満たすトラフィックだけが Guard で記録されるようにすることができます。また、すべてのトラフィック データを記録したり、Guard で表示されるトラフィックをフィルタリングしたりすることもできます。

Guard では、トラフィックは gzip 圧縮された Packet Capture (PCAP) 形式で保存され、記録されたデータを記述する 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 には、記録されたトラフィックを分析して、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 では、次の 2 つ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。
- **手動**：トラフィック データはユーザが Guard のキャプチャ機能をアクティブにしたときにパケットダンプ 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。記録されたトラフィックを保存するには、Guard 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 FTP サーバまたは SFTP 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 では、同時に 10 ゾーンまでのトラフィックを手動で記録できます。

デフォルトでは、Guard 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 5 GB 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 ファイルは、50 GB まで保存できます。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。

- [トラフィックの自動記録の設定](#)
- [トラフィックの手動記録のアクティブ化](#)
- [トラフィックの手動記録の停止](#)
- [パケットダンプ キャプチャ ファイルのディスク スペースの管理](#)
- [手動パケットダンプ設定の表示](#)
- [自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](#)

トラフィックの自動記録の設定

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 Guard を設定できます。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 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 では、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 50MB に到達するか 10 分が経過すると、バッファは圧縮形式のローカル ファイルに保存されます。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 では、複数の自動パケットダンプ キャプチャ ファイルが保存されます。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 ファイルの名前には、Guard でトラフィックが記録された日時およびトラフィックの処理方法に関する情報が示されます。

表 10-7 で、自動パケットダンプ キャプチャ ファイルの名前のセクションについて説明します。

表 10-7 自動パケットダンプ キャプチャ ファイルの名前のセクション

セクション	説明
機能	パケットダンプ キャプチャの際に実行される Guard の機能。機能は次のいずれかになります。 <ul style="list-style-type: none"> • protect : ゾーンの保護中にトラフィックを記録。 • learn : 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 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 でトラフィックの記録が終了した時刻。Guard で現在トラフィックがファイルに記録されている場合、終了時刻は表示されません。

表 10-7 自動パケットダンプ キャプチャ ファイルの名前のセクション (続き)

セクション	説明
処理	<p>Guard でのトラフィックの処理方法。アクションは次のいずれかになります。</p> <ul style="list-style-type: none"> • forwarded : Guard によって正当なものと判断され、ゾーンに転送されたトラフィック。 • dropped : Guard によって悪意のあるものと判断され、ドロップされたトラフィック。 • 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、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、Guard から開始側のクライアントに応答が送信されたトラフィック。

ラーニング プロセスまたは保護およびラーニング プロセスをイネーブルにすると、Guard で作成されたすべてのパケットダンプ キャプチャ ファイルが保存されます。ゾーン保護をイネーブルにすると、過去のパケットダンプ キャプチャ ファイルが 1 セット分だけ保存されます。ゾーン保護がイネーブルなときに、すべてのパケットダンプ キャプチャ ファイルを保存するには、Guard で作成されたパケットダンプ キャプチャ ファイルが自動的に FTP サーバまたは SFTP サーバにエクスポートされるように設定します。

ゾーン保護をアクティブにするか、Guard 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。

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 Guard 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 トラフィックが自動的に記録されるように Guard 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 FTP サーバまたは SFTP サーバにエクスポートします。P.10-16 の「[トラフィックの自動記録の設定](#)」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-scanner# packet-dump auto-capture
```

Guard 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。

トラフィックの手動記録のアクティブ化

Guard 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。これによって、特定の期間内のトラフィックを記録したり、Guard でトラフィックの記録に使用される基準を変更したりすることができます。

指定した数のパケットが記録されるか、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は停止し、手動パケットダンプ キャプチャがファイルに保存されます。

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 では、同時に 10 ゾーンまでの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。キャプチャの進行中に作業を継続するには、Guard との新しいセッションを確立します。

表 10-8 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 10-8 **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 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。
<i>capture-name</i>	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。
<i>pdump-rate</i>	サンプル レート (pps)。1 ~ 10000 の値を入力します。  (注) Guard 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。
<i>pdump-count</i>	記録対象のパケットの数。Guard 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。
dropped	Guard でドロップされたトラフィックだけをキャプチャします。

表 10-8 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 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 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。
<i>tcpdump-expression</i>	(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 では、フィルタの式に適合するトラフィックだけがキャプチャされます。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.6-12 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
```

トラフィックの手動記録の停止

Guard 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に、手動パケットダンプ キャプチャを停止できません。

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 は、パケットダンプ キャプチャ ファイルを保存します。

パケットダンプ キャプチャ ファイルのディスク スペースの管理

デフォルトでは、Guard は、ゾーンの自動パケットダンプ キャプチャ ファイル用に 2 GB のディスク スペースを割り当てています。

Guard によってゾーンの自動パケットダンプ キャプチャ ファイル用に割り当てられたディスク スペースの容量を変更するには、ゾーン設定モードで次のコマンドを入力します。

```
packet-dump disk-space disk-space
```

引数 *disk-space* には、ゾーンの自動パケットダンプ キャプチャ ファイル用に割り当てられたディスク スペースの容量を MB 単位で指定します。1 ~ 51200 の整数を入力します。

次の例を参考にしてください。

```
user@GUARD-conf-zone-scannet# packet-dump disk-space 500
```

Guard は、過去のパケットダンプ キャプチャ ファイルが gzip 圧縮された PCAP 形式で保存されます。

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方法については、[P.10-21](#) の「[手動パケットダンプ設定の表示](#)」を参照してください。

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 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。

次の例を参考にしてください。

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

[表 10-9](#) 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 10-9 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 キャプチャ用に割り当てられたディスク スペースの総容量を MB 単位で指定します。
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。

自動パケットダンプ設定の表示

ゾーンの自動パケットダンプ 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、ゾーン設定モードで **show packet-dump** コマンドを使用します。

次の例を参考にしてください。

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

表 10-10 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 10-10 自動の 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
Automatic-capture	自動パケットダンプ キャプチャプロセスの状態。
Allocated disk-space	自動パケットダンプ キャプチャ用に割り当てられたディスク スペースの容量を MB 単位で指定します。
Occupied disk-space	割り当てられたディスク スペースのパーセンテージ (自動パケットダンプ キャプチャによる現在の使用量) を指定します。

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 ファイルが自動的に FTP サーバまたは SFTP サーバにエクスポートされるように Guard 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 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。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 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.3-36 の「SFTP 接続のための鍵の設定」](#)を参照してください。

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

表 10-11 export packet-dump コマンドの引数

パラメータ	説明
<code>ftp</code>	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。
<code>sftp</code>	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。
<code>server</code>	サーバの IP アドレス。
<code>remote-path</code>	Guard 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。

表 10-11 export packet-dump コマンドの引数 (続き)

パラメータ	説明
<i>login</i>	サーバのログイン名。 <i>login</i> 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。
<i>password</i>	(オプション) リモート FTP サーバのパスワード。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

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せん。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。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 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.3-36](#) の「**SFTP 接続のための鍵の設定**」を参照してください。

表 10-12 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 10-12 **copy zone packet-dump** コマンドの引数とキーワード

パラメータ	説明
<i>zone-name</i>	既存のゾーンの名前。
<i>capture-name</i>	(オプション) 既存の packets dump キャプチャ ファイルの名前。 packets dump キャプチャ ファイルの名前を指定しない場合、すべてのゾーンの packets dump キャプチャ ファイルがエクスポートされます。詳細については、 P.10-28 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。
<i>server</i>	サーバの IP アドレス。
<i>remote-path</i>	Guard 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。
<i>login</i>	サーバのログイン名。 <i>login</i> 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。
<i>password</i>	(オプション) リモート FTP サーバのパスワード。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

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 にインポートできます。これによって、過去のイベントの分析や、ネットワークの現在のトラフィック パターンと Guard 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。Guard では、パケットダンプ キャプチャ ファイルが XML と PCAP の両方の形式でインポートされます。

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 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.3-36 の「[SFTP 接続のための鍵の設定](#)」を参照してください。

表 10-13 で、`copy zone packet-dump` コマンドの引数について説明します。

表 10-13 `copy zone packet-dump` コマンドの引数

パラメータ	説明
<code>zone-name</code>	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。
<code>ftp</code>	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。
<code>sftp</code>	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。
<code>server</code>	サーバの IP アドレス。

表 10-13 copy zone packet-dump コマンドの引数 (続き)

パラメータ	説明
<i>full-file-name</i>	<p>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。</p> <p> (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。</p>
<i>login</i>	<p>サーバのログイン名。</p> <p><i>login</i> 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。</p>
<i>password</i>	<p>(オプション) リモート FTP サーバのパスワード。パスワードを挿入しない場合、Guard によってパスワードを要求されます。</p>

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、すべてのゾーンのパケットダンプ キャプチャ ファイルのリストが表示されます。

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 10-14 で、**show packet-dump captures** コマンドの引数について説明します。

表 10-14 show packet-dump captures コマンドの引数

パラメータ	説明
<i>capture-name</i>	(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、すべてのゾーンのパケットダンプ キャプチャ ファイルのリストが表示されます。コマンド出力のフィールドの説明については、表 10-15 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た場合は、ファイルが TCPDump 形式で表示されます。
<i>tcpdump-expression</i>	(オプション) Guard 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 では、パケットダンプ キャプチャ ファイルでフィルタリング基準を満たす部分だけが表示されます。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.6-12 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 10-15 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 10-15 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 10-7 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 でトラフィックの記録時に使用され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.6-12 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 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 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、攻撃シグニチャが生成されます。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.6-7 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。

トラフィックが通常状態のとき（平時）に記録されたパケットダンプ キャプチャ ファイルを、参照のために追加で指定できます。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 では、異常なトラフィックのシグニチャが生成され、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が特定されます。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、攻撃のパターンを意味するとは限りません。

■ 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

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** 攻撃進行中にトラフィックが記録されるように Guard をアクティブにします。**packet-dump capture** コマンドを使用します (P.10-18 の「トラフィックの手動記録のアクティブ化」を参照)。
- ステップ 2** 攻撃進行中に Guard で記録されたパケットダンプ キャプチャ ファイルを特定します。**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.10-28 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** 攻撃トラフィックのシグニチャが生成されるように Guard をアクティブにします。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 10-16 で、**show packet-dump signatures** コマンドの引数について説明します。

表 10-16 show packet-dump signatures コマンドの引数

パラメータ	説明
<i>capture-name</i>	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。
<i>reference-capture-name</i>	(オプション) トラフィックが通常状態のときに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は、シグニチャが参照用のパケットダンプ キャプチャ ファイルに存在する時間の割合が表示されます。

表 10-17 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 10-17 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	<p>パケット ペイロード開始からのオフセット (バイト単位)。ここでパターンが開始します。</p> <p>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 <i>start-offset</i> 引数にコピーします。</p>
End Offset	<p>パケット ペイロード開始からのオフセット (バイト単位)。ここでパターンが終了します。</p> <p>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 <i>end-offset</i> 引数にコピーします。</p>
Pattern	<p>Guard で生成されたシグニチャ。Guard 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.6-15 の「パターン式の構文について」を参照してください。</p> <p>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。</p>
Percentage	シグニチャが <i>reference-capture-name</i> 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、新しい名前でもコピーできます。

既存の自動パケットダンプ キャプチャ ファイルは、新しいファイルで上書きされます。自動パケットダンプ キャプチャ ファイルをコピーすると、手動パケットダンプ キャプチャ ファイルとして保存され、新しい自動パケットダンプ キャプチャ ファイルで上書きされることはありません。つまり、ディスク スペースを解放するには、そのコピー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と、元のファイルのコピーも保存されます。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.10-33](#) 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 10-18](#) で、`copy packet-dump captures` コマンドの引数について説明します。

表 10-18 `copy packet-dump captures` コマンドの引数

パラメータ	説明
<i>zone-name</i>	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。
<i>capture-name</i>	既存のパケットダンプ キャプチャ ファイルの名前。
<i>tcpdump-expression</i>	(オプション) Guard 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 では、パケットダンプ キャプチャ ファイルでフィルタリング基準を満たす部分だけがコピーされます。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.6-12 の「 TCPDump 式の構文について 」を参照してください。

表 10-18 copy packet-dump captures コマンドの引数 (続き)

パラメータ	説明
<i>new-name</i>	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 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 5 GB 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 ファイルは、50 GB まで保存できます。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 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 10-19 で、clear packet-dump コマンドの引数について説明します。

表 10-19 clear packet-dump コマンドの引数

パラメータ	説明
<i>zone-name</i>	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。
<i>name</i>	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 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。

- **Accelerator card CPU speed**: アクセラレータ カードの CPU 速度を示します。
- **Accelerator card revision**: アクセラレータ カードのリビジョン番号を示します。
- **Accelerator card serial**: アクセラレータ カードのシリアル番号を示します。
- **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.11-13 の「[新しいフラッシュ バージョンの焼き付け](#)」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** の値が大きい場合、Guard のトラフィックが過負荷の状態に陥っています。負荷分散型の構成で複数の Guard をインストールすることをお勧めしません。

- **Fan Speeds**: 各ファンの速度。この値は、最大 RPM のパーセンテージです。
- **Maximum Fans**: システムがサポートするファンの最大数。
- **Installed Fans**: システムに現在搭載されているファンの数。

- **Running Fans** : 動作中のファンのリスト。
- **The number of system restarts** : システムが再起動された回数。
- **System UUID** : システムの Universal Unique ID (UUID)。
- **CPU Temperature** : 搭載されている各 CPU の現在の温度 (摂氏)。
- **DASD Temperature** : ハードディスク ドライブの現在の温度 (摂氏)。
- **Ambient Temperature** : システムの周囲温度 (摂氏)。

Guard には、内部のステータスを示すいくつかの LED があります。これらの LED は、通常、オフになっています。オンになった場合は、ハードウェアの障害を示します。そのような場合は、Guard が syslog メッセージと SNMP トラップを発行し、問題を通知します。

メモリ消費量の表示

Guard のメモリ消費量を表示できます。Guard は、メモリ使用量を KB 単位で表示します。さらに、Guard 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 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 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 10-20 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 10-20 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 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 10-20 arp コマンドの引数とキーワード (続き)

パラメータ	説明
<code>-i If</code> 、 <code>--device If</code>	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 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 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る必要があります。
<code>-s hostname hw_addr</code> 、 <code>--set hostname</code>	ハードウェア アドレスを <code>hw_addr</code> クラスに設定して、ホスト <code>hostname</code> 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。
<code>-f filename</code> 、 <code>--file filename</code>	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 <code>filename</code> 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 の ARP キャッシュを設定するには、Guard 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 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 10-21 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 10-21 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 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 <i>iface</i>	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 <i>iface</i> 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 <i>family</i>	接続を表示するアドレス低レベル プロトコル (ファミリー) 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 10-21 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。
<i>delay</i>	<i>delay</i> 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 10-22 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 10-22 **traceroute** コマンドの引数とキーワード

パラメータ	説明
<i>ip-address</i>	どの IP アドレスへのルートをトレースするか。
-f <i>first_ttl</i>	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	<i>don't fragment</i> ビットを設定します。
-g <i>gateway</i>	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 <i>iface</i>	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 <i>max_ttl</i>	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 <i>port</i>	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。
<i>packetlen</i>	プローブのパケットの長さを設定します。
-s <i>src_addr</i>	IP アドレス <i>src_addr</i> 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 10-22 traceroute コマンドの引数とキーワード (続き)

パラメータ	説明
<code>-t tos</code>	プローブ パケットのサービス タイプを、 <code>tos</code> の値に設定します。デフォルトはゼロです。
<code>-w waittime</code>	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] [-I preload] [-s packetsize] [-t ttl] [-w
deadline] [-F flowlabel] [-I interface]
[-Q tos] [-T timestamp option] [-W timeout]
```

表 10-23 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 10-23 ping コマンドの引数とキーワード

パラメータ	説明
<i>ip-address</i>	宛先 IP アドレス。
-c <i>count</i>	<i>count</i> 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 <i>flow label</i>	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 <i>interval</i>	パケットの送信間隔を <i>interval</i> 秒に設定します。デフォルトでは、1 秒に設定されます。
-I <i>interface</i>	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。
-I <i>preload</i>	応答を待たずに <i>preload</i> 個のパケットを送信します。
-Q <i>tos</i>	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 <i>packetsize</i>	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 <i>ttl</i>	IP の TTL を設定します。
-T <i>timestamp option</i>	特別な IP タイムスタンプ オプションを設定します。

表 10-23 ping コマンドの引数とキーワード (続き)

パラメータ	説明
<code>-w deadline</code>	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。
<code>-W timeout</code>	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 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 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 のデバッグ コア ファイルには、Guard の誤動作のトラブルシューティング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 のログ ファイルを表示します。詳細については、[P.10-10 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 10-24](#) で、**copy debug-core** コマンドの引数について説明します。

表 10-24 copy debug-core コマンドの引数

パラメータ	説明
<i>time</i>	<p>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、<i>MMDDhhmm</i>[[<i>CC</i>]<i>YY</i>][<i>.ss</i>] という形式を使用します。</p> <ul style="list-style-type: none"> • <i>MM</i> : 月 (数値)。 • <i>DD</i> : 日。 • <i>hh</i> : 時 (24 時間表記)。 • <i>mm</i> : 分。 • <i>CC</i> : (オプション) 年の最初の 2 桁 (たとえば 2005)。 • <i>YY</i> : (オプション) 年の最後の 2 桁 (たとえば 2005)。 • <i>.ss</i> : (オプション) 秒 (小数点が必要)。
<i>server</i>	FTP サーバの IP アドレス。
<i>full-file-name</i>	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。
<i>login</i>	(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。
<i>password</i>	(オプション) FTP サーバのパスワード。パスワードを挿入しない場合、Guard によってパスワードを要求されます。

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 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 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 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 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 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 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 5 章「ゾーンの設定」](#)、[第 6 章「ゾーンのフィルタの設定」](#)、[第 7 章「ポリシー テンプレートとポリシーの設定」](#)、および[第 8 章「インタラクティブ保護モード」](#)を参照してください。

Guard 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 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 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 10-25 に、Guard 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 10-25 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
ntp	17	*	123	—
ntp	17	123	*	—
bgp	6	179	*	no
ospf	89	*	*	—
rip	17	520	*	—
rip	17	*	520	—
gre	47	*	*	—

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 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、アカウントिंग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。
- NTP 通信をイネーブルにする。
- ポート 179 で、Guard によって開始される BGP 通信をイネーブル化し、送信元ポート 179 の着信 SYN パケットをブロックする。この設定により、Guard によって開始されるトラフィックの宛先変更元ルータへの BGP 接続が可能になります。
- OSPF 通信をイネーブルにする。
- RIP 通信をイネーブルにする。
- GRE 通信をイネーブルにする。