



# Guard の初期化

---

この章では、Cisco Guard (Guard) をネットワーク内で初期化するために必要な基本的作業と Guard の管理方法について説明します。

この章は、次の項で構成されています。

- [コマンドラインインターフェイスの使用](#)
- [Guard への初回のアクセス](#)
- [Guard のインターフェイスの設定](#)
- [デフォルト ゲートウェイの設定](#)
- [ルーティング テーブルへのスタティック ルートの追加](#)
- [プロキシ IP アドレスの設定](#)
- [Guard の管理](#)

## コマンドライン インターフェイスの使用

コマンドライン インターフェイス (CLI) を使用して、Guard の機能を制御できます。Guard のユーザ インターフェイスはさまざまなコマンド モードに分かれていて、CLI へのアクセス権はユーザの特権レベルに対応しています。ユーザが使用可能なコマンドは、現在どのモードにいるかによって異なります。

この項では、次のトピックについて取り上げます。

- ユーザの特権レベルについて
- コマンドモードについて
- CLI コマンドの入力
- CLI 使用のヒント

### ユーザの特権レベルについて

CLI へのアクセス権は、ユーザの特権レベルに対応しています。各特権レベルには、独自のコマンドのグループがあります。

表 2-1 に、ユーザの特権レベルを示します。

表 2-1 ユーザの特権レベル

ユーザの特権レベル	説明
管理者 (admin)	すべての操作にアクセスできます。
設定 (config)	ユーザの定義、削除、および修正に関連する操作を除いて、すべての操作にアクセスできます。
ダイナミック (dynamic)	監視と診断、保護、およびラーニングに関する操作にアクセスできます。dynamic 特権を持つユーザは、フレックスコンテンツ フィルタおよび動的フィルタを設定することもできます。
表示 (show)	監視操作と診断操作にアクセスできます。



(注) フィルタの設定はすべて、管理者の特権レベルまたは設定の特権レベルを持つユーザが実行することをお勧めします。これより下位の特権レベルしか持たないユーザも、動的フィルタを追加および削除できます。

## コマンド モードについて

この項では、Guard CLI で使用するコマンドおよび設定モードの概要を説明します。各コマンド モードで使用可能なコマンドのリストを入手するには、システム プロンプトで ? を入力します。

表 2-2 に、Guard のコマンド モードを示します。

表 2-2 Guard コマンド設定モード

モード	説明
グローバル	<p>リモート デバイスに接続してシステム情報を一覧表示できます。</p> <p>グローバル プロンプトは、Guard にログインしたときのデフォルトのプロンプトです。コマンド プロンプトは次のようになっています。</p> <pre>user@GUARD#</pre>
設定	<p>Guard 全体に影響する機能を設定できます。また、ユーザのアクセス権が制限されています。</p> <p>設定モードに入るには、グローバル モードで <b>configure</b> コマンドを使用します。コマンド プロンプトは次のようになっています。</p> <pre>user@GUARD-conf#</pre>
インターフェイス設定	<p>Guard ネットワーキング インターフェイスを設定できます。</p> <p>インターフェイス設定モードに入るには、設定モードで <b>interface</b> コマンドを使用します。コマンド プロンプトは次のようになっています。</p> <pre>user@GUARD-conf-if-&lt;interface-name&gt;#</pre>

表 2-2 Guard コマンド設定モード (続き)

モード	説明
ルータ設定	<p>Guard のルーティング設定を設定できます。</p> <p>ルータ設定モードに入るには、設定モードで <b>router</b> コマンドを使用します。コマンドプロンプトは次のようになっています。</p> <pre>router&gt;</pre>
ゾーン設定	<p>ゾーンのアトリビュートを設定できます。</p> <p>ゾーン設定モードに入るには、設定モードで <b>zone</b> コマンドを使用するか、グローバルモードで <b>configure</b> コマンドを使用します。コマンドプロンプトは次のようになっています。</p> <pre>user@GUARD-conf-zone-&lt;zone-name&gt;#</pre>
ポリシー テンプレート設定	<p>ゾーン ポリシーのテンプレートを設定できます。</p> <p>ポリシー テンプレート設定モードに入るには、ゾーン設定モードで <b>policy-template</b> コマンドを使用します。コマンドプロンプトは次のようになっています。</p> <pre>user@GUARD-conf-zone-&lt;zone-name&gt;-policy_template-&lt;policy-template-name&gt;#</pre>
ポリシー設定	<p>ゾーン ポリシーを設定できます。</p> <p>ポリシー設定モードに入るには、ゾーン設定モードで <b>policy</b> コマンドを使用します。コマンドプロンプトは次のようになっています。</p> <pre>user@GUARD-conf-zone-&lt;zone-name&gt;-policy-&lt;policy-path&gt;#</pre>

## CLI コマンドの入力

この項では、CLI コマンドの入力規則について説明します。

- コマンドの **no** 形式の使用
- **show** コマンド構文
- CLI のエラー メッセージ

表 2-3 に、CLI コマンドの入力規則を示します。

**表 2-3 CLI の規則**

操作	キーボード シーケンス
コマンド履歴をスクロールして変更する	矢印キーを使用する
特定のコマンド モードで使用可能なコマンドを表示する	Shift キーを押して ? (疑問符) を入力する
コマンドの補完を表示する	コマンドの最初の部分を入力し、Tab キーを押す
コマンド構文の補完を表示する	コマンドを入力して、Tab キーを 2 回押す
<b>more</b> コマンドを使用してスクロールする	<b>more number-of-lines</b> コマンドを入力する。  <b>more</b> コマンドでは、Space キーを押したときにウィンドウに表示される追加の行数が設定されます。デフォルトは、その端末で表示可能な行数より 2 行少ない行数です。  <i>number-of-lines</i> 引数は、Space キーを押したときに表示される追加の行数を設定します。
一画面分スクロールする (コマンド出力内)	Space キーを押す
一画面分後方にスクロールする (コマンド出力内)	b キーを押す
スクロール動作を中止する	q キーを押す
文字列を前方に検索する	/ (スラッシュ記号) を押し、文字列を入力する
文字列を後方に検索する	? (疑問符) キーを押し、文字列を入力する

表 2-3 CLI の規則 (続き)

操作	キーボード シーケンス
アクションをキャンセルするか、パラメータを削除する	そのコマンドの <b>no</b> 形を使用する
現在の操作に関連する情報を表示する	<b>show</b> コマンドを入力する
現在のコマンド グループ レベルを終了して上位のグループ レベルに移る	<b>exit</b> コマンドを入力する
すべてのコマンド グループ レベルを終了してルート レベルに戻る	<b>end</b> コマンドを入力する
特定の文字列を含む最初の行も含めて、その行からコマンド出力を表示する	(縦線) を押し、 <b>begin string</b> コマンドを入力する
特定の文字列を含むコマンド出力の行を表示する	(縦線) を押し、 <b>include string</b> コマンドを入力する
特定の文字列を含まないコマンド出力の行を表示する	(縦線) を押し、 <b>exclude string</b> コマンドを入力する



(注) ルート レベルで **exit** コマンドを入力すると、CLI 環境が終了し、オペレーティング システムのログイン画面に戻ります。

## コマンドの no 形式の使用

ほとんどすべての設定コマンドに、**no** 形式があります。一般に、コマンドの **no** 形式は、特定の機能をディセーブルにする場合に使用します。ディセーブルになっている機能をイネーブルにするには、キーワード **no** を取ってそのコマンドを使用します。たとえば、**event monitor** コマンドではイベント モニタが有効になり、**no event monitor** コマンドでは無効になります。

## show コマンド構文

ゾーン設定モードから、ゾーン関連の **show** コマンドを実行できます。また、これらのコマンドは、グローバル モードまたは設定モードからも実行できます。

グローバル モードまたは設定モードの **show** コマンドの構文は、次のとおりです。

```
show zone zone-name parameters...
```

ゾーン設定モードの **show** コマンドの構文は、次のとおりです。

```
show parameters...
```



(注)

---

このマニュアルでは、明示的な指定がない限り、ゾーン設定モードの **show** コマンド構文を使用します。

---

## CLI のエラー メッセージ

Guard CLI では、次の場合にエラー メッセージが表示されます。

- コマンドの構文が不完全であるか、間違っている場合。
- コマンドがシステムの設定と一致しない場合。
- システムの障害のために操作を実行できなかった場合。この場合は、システムのログにエントリが作成されます。

## CLI 使用のヒント

この項では、CLI の使用に関するヒントを提供し、次のトピックについて取り上げます。

- [ヘルプの使用](#)
- [タブ補完の使用](#)
- [操作の方向の規定について](#)
- [コマンドの省略](#)
- [ワイルドカード文字の使用](#)

## ヘルプの使用

CLI では、コマンド階層のすべてのモードで状況依存のヘルプが用意されています。ヘルプの情報では、現在のコマンドモードで使用可能なコマンドが示され、各コマンドの簡単な説明が提供されます。

ヘルプを取得するには、**?**と入力します。

コマンドのヘルプを表示するには、そのコマンドの後ろに**?**を入力します。

モードで使用可能なすべてのコマンドとその簡単な説明を表示するには、コマンドプロンプトで**?**を入力します。

ヘルプには、現在のモードで使用可能なコマンドのみが表示されます。

## タブ補完の使用

タブ補完を使用すると、コマンドの入力に必要な文字数を減らすことができます。コマンドの初めの文字をいくつか入力して **Tab** キーを押すと、コマンドを補完することができます。

複数のオプションで値を指定するコマンドを入力し、**Tab** キーを 2 回押すと、使用可能な入力パラメータが表示されます。これにはシステム定義のパラメータとユーザ定義のパラメータも含まれます。たとえば、ゾーン設定モードで **policy-template** コマンドを入力し、**Tab** キーを 2 回押すと、ポリシーテンプレート名のリストが表示されます。設定モードで **zone** コマンドを入力し、**Tab** キーを 2 回押すと、定義済みのゾーンが表示されます。

タブ補完で複数のコマンドが一致する場合は、何も表示されず、入力した現在の行がもう一度表示されます。

タブ補完機能では、現在のモードで使用可能なコマンドのみが表示されます。

**aaa authorization commands zone-completion tacacs+** コマンドを使用すると、グローバルモードと設定モードですべてのコマンド (**zone** コマンドや **show zone** コマンドなど) におけるゾーン名のタブ補完をディセーブルにできます。詳細については、[P.3-19](#) の「ゾーン名のタブ補完のディセーブル化」を参照してください。



## 操作の方向の規定について

コマンド構文中のキーワードの順序によって、操作の方向が規定されます。コマンドを入力する前にキーワードを入力すると、Guard は Guard からサーバにデータをコピーします。キーワードを入力する前にコマンドを入力すると、Guard はサーバから Guard にデータをコピーします。たとえば、**copy log ftp** コマンドではログ ファイルが Guard から FTP サーバにコピーされます。**copy ftp new-version** コマンドでは、新規ソフトウェア バージョン ファイルが FTP サーバから Guard にコピーされます。

## コマンドの省略

コマンドやキーワードは、一意な省略形を保てる文字数まで短縮できます。

たとえば、**show** コマンドは **sh** まで短縮できます。

## ワイルドカード文字の使用

ワイルドカードとして、アスタリスク (\*) を使用できます。

たとえば、**learning policy-construction \*** コマンドを入力すると、Guard で設定されているすべてのゾーンでポリシー構築フェーズがアクティブになります。

**learning policy-construction scan\*** コマンドを入力すると、scan で始まる名前を持つ Guard で設定されているすべてのゾーン (scannet や scanserver など) でポリシー構築フェーズがアクティブになります。

**no zone \*** コマンドを入力すると、すべてのゾーンが削除されます。

## Guard への初回のアクセス

Guard には、管理者のユーザ特権レベルを持ったユーザ名が事前設定されています。

Guard に初めてアクセスするときには、次の手順を実行します。

---

**ステップ 1** Guard の前面にある電源制御ボタンを押します。

Guard のブートプロセスが完了すると、ユーザ名を入力するよう要求されます。



---

**(注)** 電源投入中は、Guard の前面にある緑色の電源 LED が点灯しています。

---

**ステップ 2** ユーザ名として **admin** を、パスワードとして **rhadmin** を入力します。

**ステップ 3** 管理（ルート）アカウントのパスワードを選択します。

パスワードは、6 文字以上の英数字の組み合わせである必要があります。確認のため、新しいパスワードを再入力します。

**ステップ 4** admin ユーザ名のパスワードを選択します。

パスワードは、6 文字以上の英数字の組み合わせである必要があります。確認のため、新しいパスワードを再入力します。

**ステップ 5** riverhead ユーザ名のパスワードを選択します。

パスワードは、6 文字以上の英数字の組み合わせである必要があります。確認のため、新しいパスワードを再入力します。



---

**(注)** admin および riverhead ユーザ名のパスワードはいつでも変更できます。詳細については、[P.3-10](#) の「[自分のパスワードの変更](#)」を参照してください。

---

**ステップ 6** ユーザ名として **admin** を入力し、**ステップ 4** で設定したパスワードを入力します。

次のプロンプト行が表示されます。

```
user@GUARD#
```

**ステップ 7** 次のコマンドを入力し、設定モードに入って Guard を設定する必要があります。

**configure [terminal]**

次の例は、設定モードに入る方法を示しています。

```
user@GUARD# configure  
user@GUARD-conf#
```

---

## Guard のインターフェイスの設定

Guard には、いくつかのネットワーク インターフェイス カード (NIC) があります。Eth0 および Eth1 (ファーストイーサネットとギガビットイーサネット) は、管理目的で使用されるアウトオブバンドの NIC を構成します。

Giga0 および Giga1 (ギガビットイーサネット) インターフェイスは、Guard が管理およびゾーンのトラフィック送信に使用するインバンドの NIC を構成します。

Giga0 および Giga1 は、物理インターフェイスを提供し、その上に仮想インターフェイス (VLAN およびトンネル) が設定されます。Guard のインターフェイスの設定は、宛先変更手順の基礎となります。詳細については、[第 4 章「トラフィックの宛先変更の設定」](#) を参照してください。

Guard が正しく動作するように、Guard のインターフェイスを設定する必要があります。インターフェイス特性には、IP アドレスやインターフェイスの MTU などがあります。

多くの機能は、インターフェイス単位でイネーブルになります。**interface** コマンドを入力するときには、インターフェイスのタイプと番号を指定する必要があります。

次のガイドラインは、すべての物理インターフェイスおよび仮想インターフェイスの設定プロセスに適用されます。

- 各インターフェイスには、IP アドレスと IP サブネット マスクを設定する必要があります。
- **no shutdown** コマンドを使用して、各インターフェイスをアクティブにする必要があります。

インターフェイスの設定を表示するには、**show** または **show running-config** コマンドを入力します。

この項では、次のトピックについて取り上げます。

- [物理インターフェイスの設定](#)
- [VLAN の設定](#)
- [ループバック インターフェイスの設定](#)
- [トンネルの設定](#)
- [物理インターフェイスのカウンタのクリア](#)

## 物理インターフェイスの設定

Guard をネットワークに接続するには、物理インターフェイスを設定します。

Guard には、Eth0、Eth1、Giga0、および Giga1 の4つの物理インターフェイスがあります。アウトオブバンド インターフェイスは、Eth0 および Eth1（アウトオブバンド管理用のファースト イーサネットおよびギガビット イーサネットのソケット）です。

インバンド インターフェイス（銅またはファイバ ソケット）は Giga0 と Giga1 です。



### 注意

同じサブネット上で2つの物理インターフェイスを設定しないでください。Guard のルーティングが正しく機能しなくなる場合があります。

物理インターフェイスを設定するには、次の手順を実行します。

**ステップ 1** 設定モードで次のコマンドを入力し、インターフェイス設定モードに入ります。

```
interface if-name
```

*if-name* 引数には、インターフェイス名を指定します。

Guard では、次のインターフェイスをサポートしています。

- eth0 または eth1 : アウトオブバンド インターフェイス
- giga0 または giga1 : インバンド インターフェイス

**ステップ 2** 次のコマンドを入力して、インターフェイスの IP アドレスを設定します。

```
ip address ip-addr ip-mask
```

*ip-addr* 引数および *ip-mask* 引数には、インターフェイスの 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）。

## Guard のインターフェイスの設定

**ステップ 3** (オプション) 次のコマンドを入力して、インターフェイスの MTU を定義します。

```
mtu integer
```

*integer* 引数は、eth0 および eth1 インターフェイスの場合は 576 ~ 16,384 バイトの整数で、giga0 および giga1 インターフェイスの場合は 576 ~ 1,824 の整数です。

デフォルトの MTU の値は 1,500 バイトです。

**ステップ 4** (オプション) 次のコマンドを入力して、インターフェイスの速度とデュプレックス モードを設定します。

```
speed {auto | half speed | full speed}
```

表 2-4 に、**speed** コマンドの引数とキーワードを示します。

表 2-4 speed コマンドの引数とキーワード

パラメータ	説明
<b>auto</b>	インターフェイスのオートネゴシエーション機能を有効にします。インターフェイスは、ネットワーク設定で使用されているメディア タイプ、およびピア ルータ、ハブ、スイッチの伝送速度などの環境要因に応じて、10 Mbps、100 Mbps、1000 Mbps のいずれか、半二重または全二重で自動的に動作します。  このモードがデフォルトです。
<b>half</b>	半二重動作を指定します。
<b>full</b>	全二重動作を指定します。
<i>speed</i>	インターフェイスの速度。10 Mbps、100 Mbps、および 1000 Mbps にそれぞれ対応する 10、100、または 1000 を入力します。

**ステップ 5** 次のコマンドを入力して、インターフェイスをアクティブにします。

```
no shutdown
```

---

設定の変更を有効にするには、Guard をリロードする必要があります。

次の例は、インターフェイス `eth1` を設定してアクティブにする方法を示しています。

```
user@GUARD-conf# interface eth1
user@GUARD-conf-if-eth1# ip address 10.10.10.33 255.255.255.252
user@GUARD-conf-if-eth1# no shutdown
```

物理インターフェイスを非アクティブにするには、`shutdown` コマンドを使用します。

## VLAN の設定

VLAN は、インバンドインターフェイスのみで定義できます。

Guard 上で VLAN を定義するには、次の手順を実行します。

---

**ステップ 1** VLAN インターフェイスが存在する場合は、その設定モードに入ります。存在しない場合は、設定モードで次のコマンドを入力して、新しい VLAN を定義します。

```
interface gigaX.vlan-id
```

`vlan-id` 引数は、VLAN ID 番号を指定する整数です。VLAN ID は、TAG IEEE 802.1Q に従った番号です。

`x` 引数には、インターフェイスを指定します。インバンドインターフェイスに応じて 0 または 1 を入力します。

## Guard のインターフェイスの設定

**ステップ 2** 次のコマンドを入力して、VLAN IP アドレスを設定します。

```
ip address ip-addr ip-mask
```

*ip-addr* 引数および *ip-mask* 引数には、インターフェイスの 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)。

**ステップ 3** (オプション) 次のコマンドを入力して、インターフェイスの MTU を定義します。

```
mtu integer
```

*integer* 引数は、576 ~ 1,824 バイトの整数です。

デフォルトの MTU の値は 1,500 バイトです。

**ステップ 4** 次のコマンドを入力して、インターフェイスをアクティブにします。

```
no shutdown
```

---

次の例は、Guard 上で VLAN を設定する方法を示しています。

```
user@GUARD-conf#interface giga2.2
user@GUARD-conf-if-giga2.2# ip address 192.168.5.8 255.255.255.0
user@GUARD-conf-if-giga2.2# no shutdown
```

## ループバック インターフェイスの設定

ループバック インターフェイスと呼ばれる仮想インターフェイスが物理インターフェイスをエミュレーションするように指定できます。ループバック インターフェイスを使用すると、高度な宛先変更設定を設定できます。たとえば、遠隔宛先変更プロセスなどが可能です。



他のルータやアクセス サーバなどがこのループバック インターフェイスに到達しようとするアプリケーションでは、このループバック アドレスに割り当てられているサブネットを配信するためのルーティング プロトコルを設定する必要があります。

ループバック インターフェイスを設定するには、次の手順を実行します。

- ステップ 1** ループバック インターフェイスが存在する場合は、その設定モードに入ります。存在しない場合は、設定モードで次のコマンドを入力して、新しいループバック インターフェイスを定義します。

```
interface if-name
```

*if-name* 引数には、ループバック インターフェイス名を指定します。インターフェイス名は、*lo:integer* で、*integer* は 0 ~ 99 の整数です。

- ステップ 2** 次のコマンドを入力して、ループバック インターフェイスの IP アドレスを設定します。

```
ip address ip-addr ip-mask
```

*ip-addr* 引数および *ip-mask* 引数には、インターフェイスの 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)。

- ステップ 3** 次のコマンドを入力して、ループバック インターフェイス設定モードを終了します。

```
exit
```

次の例は、ループバック インターフェイスを設定する方法を示しています。

```
user@GUARD-conf# interface lo:0
user@GUARD-conf-if-lo:0# ip address 1.1.1.1 255.255.255.255
user@GUARD-conf-if-lo:0# exit
```

## トンネルの設定

GRE または IPIP トンネルを定義できます。Guard が宛先変更プロセスでトンネルを使用して、ゾーン トラフィックを Guard に宛先変更するように設定できます。

トンネルを定義するには、次の手順を実行します。

- ステップ 1** トンネルが存在する場合は、トンネル インターフェイス設定モードに入ります。存在しない場合は、設定モードで次のコマンドを入力して、新しいトンネルを定義します。

```
interface {greX | ipipY}
```

*X* 引数は、GRE トンネルに割り当てられる 0 ~ 1,024 バイトの整数です。

*Y* 引数は、IPIP トンネルに割り当てられる 0 ~ 1,024 バイトの整数です。

- ステップ 2** 次のコマンドを入力して、トンネルの IP アドレスを設定します。

```
ip address ip-addr [ip-mask]
```

*ip-addr* 引数および *ip-mask* 引数には、インターフェイスの 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)。デフォルトのサブネット マスクは、255.255.255.255 です。

- ステップ 3** 次のコマンドを入力して、トンネルの送信元 IP アドレスを設定します。

```
tunnel source source ip
```

*source ip* 引数には、トンネルの送信元 IP アドレスを指定します。この IP アドレスは、トンネル内のパケットの送信元アドレスとして使用されます。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 192.168.100.1)。

**ステップ 4** 次のコマンドを入力して、トンネルの宛先 IP アドレスを設定します。

```
tunnel destination destination-ip
```

*destination ip* 引数には、トンネルの宛先 IP アドレスを指定します。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 192.168.100.1）。

**ステップ 5** (オプション) 次のコマンドを入力して、インターフェイスの MTU を定義します。

```
mtu integer
```

*integer* 引数は、576 ~ 1,480 の整数です。

IPIP トンネルのデフォルト値は、1,480 バイトです。

GRE トンネルのデフォルト値は、1,476 バイトです。

**ステップ 6** インターフェイスをアクティブにします。次のコマンドを入力します。

```
no shutdown
```

---

次の例は、GRE トンネルを設定する方法を示しています。

```
user@GUARD-conf# interface gre2
user@GUARD-conf-if-gre2# ip address 192.168.121.1 255.255.255.0
user@GUARD-conf-if-gre2# tunnel source 192.168.8.8
user@GUARD-conf-if-gre2# tunnel destination 192.168.250.2
user@GUARD-conf-if-gre2# no shutdown
```

## GRE トンネルのステータスの確認

GRE トンネルでキープアライブ メッセージをイネーブルにできます。キープアライブ機能をイネーブルにすると、キープアライブ パケットが指定された間隔で送信され、インターフェイスがアクティブに保たれます。Guard が応答のないキープアライブ パケットの送信を何回試行するとトンネルがダウン状態になるかを指定できます。

キープアライブの間隔を設定することができます。この間隔は、GRE トンネルが活動中であることを確認するために Guard がメッセージを送信する頻度で、1 秒単位で調整が可能です。デフォルトのリトライ値を変更していない場合、キープアライブ パケットを受信せずに 10 回の間隔が過ぎると、GRE トンネルはダウンを宣言されます。



### 注意

GRE トンネルがダウンを宣言されると、Guard はそのトンネルを注入に使用することを中止します。トラフィックの注入手段が他に存在しなければ、Guard はゾーンのトラフィックの宛先変更を停止します。

Guard は、GRE トンネルがダウンを宣言されている場合でも、キープアライブメッセージの送信を続けます。トンネル側がキープアライブメッセージを返すと、Guard はトンネルをアクティブにし、トラフィックの宛先変更を再開します。

GRE トンネルでキープアライブメッセージをイネーブルにするには、GRE インターフェイス設定モードで次のコマンドを入力します。

```
keepalive [refresh-time [retries]]
```

表 2-5 に、keepalive コマンドの引数を示します。

表 2-5 keepalive コマンドの引数

パラメータ	説明
<i>refresh-time</i>	(オプション) キープアライブメッセージが送信される間隔 (秒)。1 ~ 32767 の整数を入力します。  デフォルトのリフレッシュ時間は 3 秒です。
<i>retries</i>	(オプション) Guard が応答のないキープアライブパケットの送信を何回続けるとトンネルインターフェイスプロトコルがダウン状態になるかを指定します。1 ~ 255 の整数を入力します。  デフォルトのリトライ回数は 10 回です。

次の例は、GRE トンネル上でキープアライブ メッセージをイネーブルにする方法を示しています。

```
user@GUARD-conf-if-gre2# keepalive 60 5
```

## 物理インターフェイスのカウンタのクリア

テストを行う予定があり、データ（ギガ）に使用される物理インターフェイスのカウンタにテストセッションの情報だけを反映する場合は、このカウンタをクリアすることができます。

物理インターフェイスのカウンタをクリアするには、インターフェイス設定モードで次のコマンドを入力します。

### **clear counters**

次の例は、インターフェイス `giga2` のカウンタをクリアする方法を示しています。

```
user@GUARD-conf-if-giga2# clear counters
```

## デフォルト ゲートウェイの設定

デフォルト ゲートウェイは、ローカル ネットワークで未知の IP アドレスを持つパケットの受信と転送を行います。ほとんどの場合、Guard のデフォルト ゲートウェイの IP アドレスは、Guard とインターネットの間に存在する隣接ルータです。デフォルト ゲートウェイ アドレスは、Guard のネットワーク インターフェイスの IP アドレスのいずれかと同じネットワーク上にある必要があります。



(注)

---

ゾーン保護がイネーブルになっているときは、デフォルト ゲートウェイに IP アドレスを割り当てないでください。

---



注意

---

デフォルト ゲートウェイの IP アドレスを設定していない場合、Guard がネットワークにアクセスできないことがあります。

---

デフォルト ゲートウェイ アドレスを割り当てるには、設定モードで次のコマンドを入力します。

```
default-gateway ip-addr
```

*ip-addr* 引数には、デフォルト ゲートウェイの IP アドレスを指定します。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 192.168.100.1)。

デフォルト ゲートウェイ アドレスを変更するには、このコマンドを再入力します。

次の例は、デフォルト ゲートウェイを設定する方法を示しています。

```
user@GUARD-conf# default-gateway 192.168.100.1
```

## ルーティング テーブルへのスタティック ルートの追加

Guard のルーティング テーブルにスタティック ルートを追加できます。スタティック ルートは、Guard の IP インターフェイスに関連付けられたローカル ネットワークの外側にあるサーバやネットワークのルートを指定するために追加します。

スタティック ルートは永続的に追加され、Guard のリブート後も削除されません。

Guard のルーティング テーブルにスタティック ルートを追加するには、設定モードで次のコマンドを入力します。

```
ip route ip-addr ip-mask nexthop-ip [if-name]
```

表 2-6 に、`ip route` コマンドの引数を示します。

表 2-6 ip route コマンドの引数

パラメータ	説明
<i>ip-addr</i>	ルートの宛先ネットワーク。宛先には、IP ネットワーク アドレス（ネットワーク アドレスのホスト ビットは 0 に設定）またはホスト ルートの IP アドレスを指定できます。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 192.168.100.1）。
<i>ip-mask</i>	宛先ネットワークに関連付けられたサブネット マスク。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 255.255.255.0）。
<i>nexthop-ip</i>	宛先ネットワークとサブネット マスクによって定義された一連のアドレスへの到達を可能にする転送アドレスまたはネクストホップ IP アドレス。ネクストホップ IP アドレスは、インターフェイスのサブネット内にある必要があります。ローカル サブネット ルートでは、ネクストホップ IP アドレスは、そのサブネットに接続されたインターフェイスに割り当てられている IP アドレスです。1 つ以上のルータをまたいで使用可能なリモート ルートの場合、ネクストホップ IP アドレスは、ネイバールータに割り当てられている直接到達可能な IP アドレスです。

## ■ ルーティングテーブルへのスタティック ルートの追加

表 2-6 ip route コマンドの引数 (続き)

パラメータ	説明
<i>if-name</i>	(オプション) 宛先への到達が可能な Guard のインターフェイス。インターフェイスを指定しなかった場合、Guard のルーティング テーブルに従って、使用されるインターフェイスはネクストホップ IP アドレスによって判別されます。

次の例は、スタティック ルートを設定する方法を示しています。

```
user@GUARD-conf# ip route 172.16.31.5 255.255.255.255 192.168.100.34
```

ルーティング テーブルを表示するには、**show ip route** コマンドを入力します。



## プロキシ IP アドレスの設定

Guard のプロキシ IP アドレスは、プロキシ モードのスプーフィング防止保護メカニズムで必要になります。このメカニズムで、Guard はゾーンに対して TCP プロキシの役割を果たします。Guard はまず新しい接続を認証し、その後自分自身の IP アドレスを発信元 IP アドレスとして使用して、ゾーンとの接続を開始します。ゾーン保護をアクティブにする前に、プロキシ IP アドレスを設定する必要があります。



### 注意

プロキシ IP アドレスを定義しないと、ゾーン保護をアクティブにできません。

ゾーン保護がイネーブルになっているときには、Guard にプロキシ IP アドレスを割り当てないでください。

ネットワークでロード バランシングを使用してネットワークの過負荷を分散している場合、または多数の同時接続が必要な場合は、プロキシ IP アドレスを 3 つまたは 4 つ設定することをお勧めします。

プロキシ IP アドレスは最大 60 個設定できますが、プロキシ IP アドレスの数が増えるとメモリ リソースの消費量も増えるため、プロキシ IP アドレスは 20 個以上設定しないことをお勧めします。

Guard のスプーフィング防止プロキシ IP アドレスを設定するには、設定モードで次のコマンドを入力します。

```
proxy ip-addr
```

*ip-addr* 引数には、プロキシ IP アドレスを指定します。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 192.168.100.1)。

各ゾーンと Guard のプロキシ IP アドレス間のルートを確認する必要があります。Guard は、プロキシ IP アドレスに対する ping 要求には応答しません。

追加のプロキシ IP アドレスを設定するには、このコマンドを再入力します。

次の例は、プロキシ IP アドレスを設定する方法を示しています。

```
user@GUARD-conf# proxy 192.168.100.34
```

## Guard の管理

最初は、コンソールからローカルに Guard を管理することができます。初めて Guard の電源をオンにするときに、コンソール接続を使用して CLI にアクセスし、初期セットアップ プロシージャを実行することができます。詳細については、P.3-14 の「パスワードを使用した特権レベルの割り当て」を参照してください。

Guard のネットワーク機能を設定した後は (P.2-12 の「Guard のインターフェイスの設定」を参照)、次のいずれかの方法を使用して Guard にアクセスし、管理することができます。

- Secure Shell (SSH; セキュア シェル) のセッションを使用したアクセス。
- Web-Based Manager (WBM) を使用した Guard へのアクセス。
- DDoS 検知ネットワーク要素からのアクセス。詳細については、該当するマニュアルを参照してください。

この項では、次のトピックについて取り上げます。

- [Web-Based Manager による Guard の管理](#)
- [SSH を使用した Guard へのアクセス](#)

## Web-Based Manager による Guard の管理

WBM を使用すると、Web ブラウザを使用して Web から Guard を管理できます。

WBM を使用して Guard を管理するには、次の手順を実行します。

---

**ステップ 1** 設定モードで次のコマンドを入力して、WBM サービスをイネーブルにします。

```
service wbm
```

**ステップ 2** 設定モードで次のコマンドを入力して、リモート マネージャの IP アドレスから Guard へのアクセスを許可します。

```
permit wbm ip-addr [ip-mask]
```

*ip-addr* 引数および *ip-mask* 引数には、リモート マネージャの 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。

**ステップ 3** ブラウザを開いて、次のアドレスを入力します。

```
https://Guard-ip-address/
```

*Guard-ip-address* 引数は、Guard の IP アドレスです。

Guard の WBM ウィンドウが表示されます。



**(注)** Web ベース管理制御をイネーブルにするには、HTTP ではなく HTTPS が使用されます。

**ステップ 4** ユーザ名とパスワードを入力し、**OK** をクリックします。

ユーザ名とパスワードを正しく入力すると、Guard のホームページが表示されません。

TACACS+ 認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。TACACS+ サーバ上で高度な認証アトリビュート (パスワードの有効期限など) が設定されている場合、Guard が TACACS+ サーバ上のユーザ設定に基づいて新しいパスワードの入力を要求したり、パスワードがいつ期限切れになるかを通知したりします。

次の例は、Guard WBM をイネーブルにする方法を示しています。

```
user@GUARD-conf# service wbm
user@GUARD-conf# permit wbm 192.168.30.32
```

## SSH を使用した Guard へのアクセス

セキュア シェル (SSH) の接続を使用して、Guard にアクセスすることができません。

SSH サービスは、デフォルトでイネーブルになっています。

SSH を使用して Guard にアクセスするには、次の手順を実行します。

- ステップ 1** 設定モードで次のコマンドを入力して、リモート ネットワークの IP アドレスから Guard へのアクセスを許可します。

```
permit ssh ip-addr [ip-mask]
```

*ip-addr* 引数および *ip-mask* 引数には、リモート ネットワークの 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 アドレスとして 192.168.10.2 を、サブネット マスクとして 255.255.255.252 を入力)。

- ステップ 2** リモート ネットワーク アドレスから接続を確立し、ログイン ユーザ名とパスワードを入力します。

TACACS+ 認証が設定されている場合は、ローカル データベースの代わりに TACACS+ ユーザ データベースがユーザ認証に使用されます。TACACS+ サーバ上で高度な認証アトリビュート (パスワードの有効期限など) が設定されている場合、Guard が TACACS+ サーバ上のユーザ設定に基づいて新しいパスワードの入力を要求したり、パスワードがいつ期限切れになるかを通知したりします。

ログイン ユーザ名とパスワードを入力しないで SSH 接続をイネーブルにするには、次の手順を実行します。

- ローカルに設定されたログインとパスワードを認証に使用するように Guard を設定します。詳細については、[P.3-6 の「認証の設定」](#)を参照してください。
- リモート接続 SSH の公開鍵を Guard SSH 鍵リストに追加します。詳細については、[P.3-37 の「SSH 鍵の管理」](#)を参照してください。

次の例は、Guard への SSH 接続をイネーブルにする方法を示しています。

```
user@GUARD-conf# permit ssh 192.168.30.32
```

