基本設定

ここでは、設定を機能させるために FWSM で通常必要な基本設定について説明します。この章で説明する内容は、次のとおりです。

パスワードの変更

ここでは、ログイン パスワードとイネーブル パスワードの変更方法について説明します。内容は次のとおりです。

（注）　マルチコンテキスト　モードでは、各コンテキストとシステム実行スペースに、それぞれ専用のログイン ポリシーおよびパスワードがあります。

ログイン パスワードの変更

ログイン パスワードは、スイッチからのセッションおよび Telnet 接続と SSH 接続に使用します。デフォルトのログイン パスワードは、「cisco」です。パスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# {passwd | password} password
```

passwd または **password** を入力できます。*password* は、大文字と小文字が区別されるパスワードです。英数字と特殊記号を 16 文字まで使用できます。パスワードには疑問符とスペース以外、任意の文字を使用できます。

パスワードは暗号化されて設定に保存されるので、入力後に元のパスワードを表示することはできません。パスワードをデフォルトの設定に戻す場合は、**no password** コマンドを使用します。

イネーブル パスワードの変更

イネーブル パスワードを使用すると、イネーブル EXEC モードを開始できます。デフォルトのイネーブル パスワードは、ブランクです。イネーブル パスワードを変更するには、次のコマンドを入力します。

```
hostname(config)# enable password password
```

password は、大文字と小文字が区別されるパスワードです。英数字と特殊記号を 16 文字まで使用できます。パスワードには疑問符とスペース以外、任意の文字を使用できます。

このコマンドによって、最上位の権限レベルに対応するパスワードが変更されます。ローカルなコマンド許可を設定する場合は、0 ～ 15 の各権限レベルにイネーブル パスワードを設定できます。

パスワードは暗号化されて設定に保存されるので、入力後に元のパスワードを表示することはできません。パスワードを指定しないで **enable password** コマンドを入力すると、パスワードがデフォルトのブランクに設定されます。

メンテナンス ソフトウェア パスワードの変更

メンテナンス ソフトウェアは、トラブルシューティングに役立ちます。メンテナンス ソフトウェアから、たとえば、アプリケーション パーティションに新しいソフトウェアをインストールしたり、パスワードをリセットしたり、クラッシュ ダンプ情報を表示したりできます。メンテナンス ソフトウェアにアクセスする唯一の方法は、FWSM とのセッションを開始することです。

メンテナンス ソフトウェアには、アクセス権限の異なる 2 つのユーザ レベルがあります。

- root — ネットワーク パーティション パラメータの設定、アプリケーション パーティション上のソフトウェア イメージのアップグレード、ゲスト アカウント パスワードの変更、およびゲスト アカウントのイネーブル化またはディセーブル化を実行できます。

  デフォルトのパスワードは、「cisco」です。
- guest — ネットワーク パーティション パラメータを設定し、クラッシュ ダンプ情報を表示できます。

  デフォルトのパスワードは、「cisco」です。

両方のユーザのメンテナンス パーティション パスワードを変更する手順は、次のとおりです。

ステップ 1　スイッチのプロンプトに次のコマンドを入力して、メンテナンス パーティションで FWSM を再起動します。

```
Router# hw-module module mod_num reset cf:1
```

ステップ 2　次のコマンドを入力して、FWSM とのセッションを確立します。

```
Router# session slot mod_num processor 1
```

ステップ 3　次のコマンドを入力して、root としてログインします。

```
Login: root
```

ステップ 4　プロンプトにパスワードを入力します。

```
Password:
```

デフォルトのパスワードは、「cisco」です。

ステップ 5　次のコマンドを入力して、root パスワードを変更します。

```
root@localhost# passwd
```

ステップ 6　プロンプトに新しいパスワードを入力します。

```
Changing password for user root
New password:
```

ステップ 7　新しいパスワードを再入力します。

```
Retype new password:
passwd: all authentication tokens updated successfully
```

ステップ 8　次のコマンドを入力して、guest パスワードを変更します。

```
root@localhost# passwd-guest
```

ステップ 9　プロンプトに新しいパスワードを入力します。

```
Changing password for user guest
New password:
```

ステップ 10　新しいパスワードを再入力します。

```
Retype new password:
passwd: all authentication tokens updated successfully
```

次に、root アカウントのパスワードを設定する例を示します。

```
root@localhost# passwd
Changing password for user root
New password: *sh1p
Retype new password: *sh1p
passwd: all authentication tokens updated successfully
```

次に、guest アカウントのパスワードを設定する例を示します。

```
root@localhost# passwd-guest
Changing password for user guest
New password: f1rc8t
Retype new password: f1rc8t
passwd: all authentication tokens updated successfully
```

ホスト名の設定

FWSM にホスト名を設定すると、その名前がコマンドライン プロンプトに表示されます。複数のデバイスとセッションを確立する場合は、ホスト名によって、コマンドの入力先を識別しやすくなります。

マルチコンテキスト モードの場合、システム実行スペースで設定したホスト名が、すべてのコンテキストのコマンドライン プロンプトに表示されます。コンテキスト内で任意に設定したホスト名はコマンドラインには表示されませんが、**banner** コマンド **$(hostname)** トークンによって使用できます。

FWSM 用のホスト名なのか、コンテキスト用のホスト名なのかを指定するには、次のコマンドを入力します。

```
hostname(config)# hostname name
```

名前に使用できる文字数は最大 63 文字です。ホスト名は始めと終わりは英字または数字でなければなりません。中間の文字として使用できるのは英字、数字、またはハイフンだけです。

この名前はコマンドライン プロンプトに表示されます。次に例を示します。

```
hostname(config)# hostname farscape
farscape(config)#
```

ドメイン名の設定

FWSM には非修飾名の接尾辞としてドメイン名が付けられます。たとえば、ドメイン名を「example.com」に設定し、syslog サーバに非修飾名「jupiter」を指定する場合、FWSM には「jupiter.example.com」という名前が与えられます。

デフォルトのドメイン名は default.domain.invalid です。

マルチコンテキスト モードの場合、各コンテキストにドメイン名を設定できます。また、システム実行スペースでもドメイン名を設定できます。

FWSM のドメイン名を指定するには、次のコマンドを入力します。

```
hostname(config)# domain-name name
```

たとえば、ドメインを example.com として設定する場合、次のコマンドを入力します。

```
hostname(config)# domain-name example.com
```

プロンプトの設定

ホスト名、コンテキスト名、ドメイン名、スロット、フェールオーバー ステータス、フェールオーバー プライオリティなどの CLI プロンプトに表示される情報を設定できます。マルチコンテキスト モードでは、システム実行スペースまたは管理（admin）コンテキストへのログイン時に拡張プロンプトを表示できます。管理（admin）以外のコンテキストでは、ホスト名とコンテキスト名を示すデフォルト プロンプトのみが表示されます。

プロンプトに含める情報を設定するには、次のコマンドを入力します。

```
hostname(config)# prompt [hostname] [context] [domain] [slot] [state] [priority]
```

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。各要素はスラッシュ（/）で区切られます。各キーワードについては、次の説明を参照してください。

- **hostname —** ホスト名を表示します。
- **domain —** ドメイン名を表示します。
- **context —**（マルチモード限定）現在のコンテキストを表示します。
- **priority —** フェールオーバー プライオリティを pri（プライマリ）または sec（セカンダリ）で表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。
- **slot —** スイッチ内のスロットの位置を表示します。
- **state —** 装置のトラフィック転送ステートを表示します。**state** キーワードには、次の値が表示されます。
  - act — フェールオーバーがイネーブルで、装置はトラフィックをアクティブに転送しています。
  - stby — フェールオーバーはイネーブルで、装置はトラフィックを転送しておらず、ステートはスタンバイ、失敗、またはその他の非アクティブ ステートです。
  - actNoFailover — フェールオーバーはイネーブルではなく、装置はトラフィックをアクティブに転送しています。
  - stbyNoFailover — フェールオーバーはイネーブルではなく、装置はトラフィックを転送していません。これは、スタンバイ ユニットのインターフェイス障害数がスレッシュホールドを超過した場合に発生することがあります。

たとえば、可能なすべての要素をプロンプトに表示するには、次のコマンドを入力します。

```
hostname(config)# prompt hostname context priority slot state
```

プロンプトが次の文字列に変わります。

```
hostname/admin/pri/6/act(config)#
```

ログイン バナーの設定

FWSM に接続するとき、Telnet を使用して FWSM にログインするとき、またはユーザ EXEC モードを開始するときに表示されるメッセージを設定できます。

ログイン バナーを設定するには、システム実行スペースで、またはコンテキスト内で、次のコマンドを入力します。

```
hostname(config)# banner {motd | login | exec} text
```

motd キーワードでは、初回接続時にバナーが表示されます。

The **login** キーワードでは、Telnet を使用して FWSM にログインするときにバナーが表示されます。

exec キーワードでは、ユーザ EXEC モードにアクセスするときにバナーが表示されます。

ユーザが FWSM に接続すると、最初に MoTD（Message-of-The-Day）バナーが表示され、続いてログイン バナーとプロンプトが表示されます。このバナーは Telnet 接続以外では表示されません。さらに、ユーザが FWSM に正しくログインすると（Telnet 接続の場合）、exec バナーが表示されます。

CLI を使用してバナーのテキストにスペースを含めることができますが、タブを入力することはできません。**$(hostname)** および **$(domain)** という文字列を指定することによって、FWSM のホスト名またはドメイン名を動的に追加できます。システム コンフィギュレーションでバナーを設定すると、コンテキスト コンフィギュレーションで **$(system)** という文字列を使用することによって、コンテキスト内でそのバナー テキストを使用できます。

複数行にする場合は、各行の前に banner コマンドを指定します。

たとえば、MoTD バナーを追加する場合は、次のように入力します。

```
hostname(config)# banner motd Welcome to $(hostname)
hostname(config)# banner motd Contact me at admin@example.com for any
hostname(config)# banner motd issues
```

透過ファイアウォール モードと NAT を設定しない場合の接続制限の設定

NAT を設定すると、トラフィックの接続限度を設定できます。透過ファイアウォール モード（NAT をサポートしません）または NAT を設定しないルーテッド モード コンフィギュレーションの場合、スタティック アイデンティティ NAT を設定して接続制限を設定できます。スタティック アイデンティティ NAT を使用すると、限度を設定し、なおかつ変換を実行しないアドレスを指定できます（ルーテッド モードの場合、NAT 除外など NAT をバイパスする任意の方法を使用して、制限を設定できます。詳細については、「NAT のバイパス」[p.12-32] を参照してください。透過モードの場合、FWSM がサポートするのは次の方式だけです）。

Modular Policy Framework を使用して接続制限（初期接続制限は設定できません）を設定することもできます。詳細については、「接続制限とタイムアウトの設定」（p.19-2）を参照してください。初期接続制限は NAT を使用する場合のみ設定できます。両方の方法を使用する同一トラフィックに対してこれらを設定した場合、FWSM は低い制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルになっている場合、FWSM は TCP シーケンスのランダム化をディセーブルにします。

初期接続数を制限することで、DoS 攻撃からシステムを保護できます。FWSM は初期接続制限を使用して、TCP 代行受信機能をトリガーします。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。TCP 代行受信では、SYN クッキー アルゴリズムを使用して、TCP SYN フラッディング攻撃を阻止します。SYN フラッディング攻撃では、通常、スプーフィングされた IP アドレスから一連の SYN パケットが送信されます。継続的に送信される SYN パケットにより、サーバの SYN キューが常に満杯状態になり、接続要求を処理できなくなります。接続が、初期接続スレッシュホールドに達すると、FWSM はサーバのプロキシとして動作し、クライアントの SYN 要求に対して SYN-ACK 応答を生成します。FWSM は、クライアントから ACK の返信を受信すると、そのクライアントを認証し、サーバへの接続を許可します。

接続制限を設定するには、次のコマンドを入力します。

```
hostname(config)# static (real_interface,mapped_interface) real_ip real_ip [netmask
mask] [dns] [[tcp] tcp_max_conns [emb_limit]] [udp udp_max_conns] [norandomseq]
```

両方の *real_ip* 引数に、同じ IP アドレスを指定します。

norandomseq キーワードは TCP Initial Sequence Number（ISN）ランダム化をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化し、その結果、データのスクランブルが発生する場合だけです。TCP 接続ごとに、ISN を 2 つずつ使用します。1 つはクライアントが作成し、もう 1 つはサーバが作成します。FWSM はホスト / サーバによって生成された ISN をランダム化します。攻撃側が次の ISN を予測してセッションをハイジャックする可能性を排除するために、ISN の少なくとも一方はランダムに生成する必要があります。

tcp *tcp_max_conns* および **udp** *udp_max_conns* キーワードはサブネット全体における同時 TCP/UDP 接続の最大数（65,536 まで）を設定します。デフォルトはどちらのプロトコルでも 0 で、これは最大接続数を意味します。

emb_limit 引数は、ホストあたりの最大初期接続数（65,536 まで）を設定します。初期接続とは、送信元と宛先間で所定のハンドシェイクが完了していない接続要求です。この制限によって、TCP 代行受信機能を使用できます。デフォルトは 0 で、これは初期接続の最大数を意味します。*emb_limit* を入力する前に、**tcp** *tcp_max_conns* を入力する必要があります。*tcp_max_conns* にはデフォルト値を使用し、*emb_limit* は変更する場合は、*tcp_max_conns* に **0** を入力します。

たとえば、ホスト 10.1.1.1 にオプションを設定する場合は、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) 10.1.1.1 10.1.1.1 netmask 255.255.255.255
tcp 1000 200 udp 1000 norandomseq
```