



使用する前に

この章では、Cisco ASA の使用を開始する方法について説明します。

- [コマンドラインインターフェイス \(CLI\) のコンソールへのアクセス \(1 ページ\)](#)
- [ASDM アクセスの設定 \(10 ページ\)](#)
- [ASDM の起動 \(16 ページ\)](#)
- [ASDM 動作のカスタマイズ \(18 ページ\)](#)
- [工場出荷時のデフォルト設定 \(20 ページ\)](#)
- [設定の開始 \(30 ページ\)](#)
- [ASDM でのコマンドラインインターフェイス ツールの使用 \(31 ページ\)](#)
- [接続の設定変更の適用 \(33 ページ\)](#)

コマンドラインインターフェイス (CLI) のコンソールへのアクセス

ASDM アクセスの基本的な設定を、CLI を使用して行う必要がある場合があります。

初期設定を行うには、コンソールポートから直接CLIにアクセスします。その後、[#unique_39](#) に従って Telnet または SSH を使用して、リモート アクセスを設定できます。システムがすでにマルチ コンテキスト モードで動作している場合は、コンソールポートにアクセスするとシステムの実行スペースに入ります。



(注) ASAv のコンソールアクセスについては、ASAv のクイック スタートガイドを参照してください。

アプライアンス コンソールへのアクセス

アプライアンス コンソールにアクセスするには、次の手順に従います。

手順

ステップ 1 付属のコンソール ケーブルを使用してコンピュータをコンソール ポートに接続します。ターミナルエミュレータを回線速度 9600 ボー、データ ビット 8、パリティなし、ストップ ビット 1、フロー制御なしに設定して、コンソールに接続します。

コンソール ケーブルの詳細については、ASA のハードウェア ガイドを参照してください。

ステップ 2 Enter キーを押して、次のプロンプトが表示されることを確認します。

```
ciscoasa>
```

このプロンプトは、ユーザ EXEC モードで作業していることを示します。ユーザ EXEC モードでは、基本コマンドのみを使用できます。

ステップ 3 特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、Enter キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名](#)、[ドメイン名](#)、および[イネーブルパスワードと Telnet パスワードの設定](#)を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 4 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

例：

```
ciscoasa# configure terminal
ciscoasa(config)#
```

グローバル コンフィギュレーション モードから ASA の設定を開始できます。グローバル コンフィギュレーション モードを終了するには、**exit** コマンド、**quit** コマンド、または **end** コマンドを入力します。

Firepower 4100/9300 シャーシ上の ASA コンソールへのアクセス

初期設定の場合、Firepower 4100/9300 シャーシスーパーバイザに（コンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドラインインターフェイスにアクセスし、ASA セキュリティ モジュールに接続します。

手順

- ステップ 1** Firepower 4100/9300 シャーシスーパーバイザ CLI（コンソールまたは SSH）に接続し、次に ASA にセッション接続します。

connect module slot console

初めてモジュールにアクセスするときは、FXOS モジュールの CLI にアクセスします。その後 ASA アプリケーションに接続する必要があります。

connect asa

例：

```
Firepower# connect module 1 console
Firepower-module1> connect asa
```

asa>

- ステップ 2** 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、Enter キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定](#)を参照してください。

例：

```
asa> enable
Password:
asa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーション モードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

- ステップ 3** グローバル コンフィギュレーション モードを開始します。

configure terminal

例：

```
asa# configure terminal
```

```
asa(config)#
```

グローバル コンフィギュレーション モードを終了するには、**disable**、**exit**、または **quit** コマンドを入力します。

ステップ 4 Ctrl-a、d と入力し、アプリケーション コンソールを終了して FXOS モジュール CLI に移動します。

トラブルシューティングのために FXOS モジュールの CLI を使用する場合があります。

ステップ 5 FXOS CLI のスーパーバイザ レベルに戻ります。

a) ~ と入力

Telnet アプリケーションに切り替わります。

b) Telnet アプリケーションを終了するには、次を入力します。

```
telnet>quit
```

ASA サービス モジュール コンソールへのアクセス

初期設定の場合、スイッチに（コンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドライン インターフェイス（CLI）にアクセスし、ASASM に接続します。ASASM には工場出荷時のデフォルトコンフィギュレーションが含まれていないため、ASDM を使用してアクセスする前に CLI で設定を行う必要があります。ここでは、ASASM CLI にアクセスする方法について説明します。

接続方法について

スイッチ CLI から ASASM に接続するには、次の 2 つの方法が使用できます。

- 仮想コンソール接続： **service-module session** コマンドを使用して、ASASM への仮想コンソール接続を作成します。仮想コンソール接続には、実際のコンソール接続のすべての利点と制限があります。

利点を次に示します。

- 接続はリロード中も持続し、タイムアウトしません。
- ASASM リロード中も接続を維持でき、スタートアップメッセージを閲覧できます。
- ASASM がイメージをロードできない場合、ROMMON にアクセスできます。
- 初期パスワードの設定は必要ではありません。

制限を次に示します。

- 接続が低速です（9600 ボー）。
- 一度にアクティブにできるコンソール接続は 1 つだけです。

- このコマンドは、**Ctrl+Shift+6, x** がターミナル サーバプロンプトに戻るためのエスケープシーケンスであるターミナルサーバとともに使用することはできません。**Ctrl+Shift+6, x** は、**ASASM** コンソールをエスケープして、スイッチプロンプトに戻るためのシーケンスでもあります。したがって、この状況で**ASASM**を終了しようとすると、代わりにターミナルサーバプロンプトに戻ります。スイッチにターミナルサーバを再接続した場合、**ASASM** コンソールセッションがアクティブのままです。スイッチプロンプトを終了することはできません。コンソールをスイッチプロンプトに戻すには、直接シリアル接続を使用する必要があります。この場合、**Cisco IOS** でターミナルサーバまたはスイッチエスケープ文字を変更するか、または **Telnet session** コマンドを使用します。



(注) コンソール接続の永続性のため、**ASASM** を正しくログアウトしないと、意図よりも長く接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

- **Telnet** 接続 : **session** コマンドを使用して、**ASASM** への **Telnet** 接続を作成します。



(注) 新しい **ASASM** に対してはこの方式を使用して接続できません。この方式では、**ASASM** 上での **Telnet** ログインパスワードの設定が必要です (デフォルトのパスワードはありません)。**passwd** コマンドを使用してパスワードを設定した後に、この方式を使用できます。

利点を次に示します。

- **ASASM** への複数のセッションを同時に使用できます。
- **Telnet** セッションは、高速接続です。

制限を次に示します。

- **Telnet** セッションは、**ASASM** リロード時に終了し、タイムアウトします。
- **ASASM** が完全にロードするまで **ASASM** にはアクセスできません。したがって、**ROMMON** にアクセスできません。
- 最初に **Telnet** ログインパスワードを設定する必要があります。デフォルトのパスワードはありません。

ASA サービス モジュールへのログイン

初期設定の場合、スイッチに（スイッチのコンソールポートに、あるいは Telnet または SSH を使用してリモートで）接続してコマンドラインインターフェイスにアクセスし、ASASM に接続します。

システムがすでにマルチコンテキストモードで動作している場合は、スイッチ環境から ASASM にアクセスするとシステムの実行スペースに入ります。

その後は、Telnet または SSH を使用してリモートアクセスを ASASM に直接設定できます。

手順

ステップ 1 スイッチから、次のいずれかを実行します。

- 最初のアクセスで使用可能：スイッチ CLI からこのコマンドを入力し、ASASM にコンソールアクセスします。

service-module session [switch {1 | 2}] slot number

例：

```
Router# service-module session slot 3
ciscoasa>
```

VSS 内のスイッチの場合、**switch** 引数を入力します。

モジュールのスロット番号を表示するには、スイッチプロンプトで **show module** コマンドを入力します。

ユーザ EXEC モードにアクセスします。

- ログインパスワードの設定後に使用可能：スイッチ CLI からこのコマンドを入力し、バックプレーンを介して ASASM に Telnet 接続します。

session [switch {1 | 2}] slot number processor 1

ログインパスワードの入力が求められます。

```
ciscoasa passwd:
```

例：

```
Router# session slot 3 processor 1
ciscoasa passwd: cisco
ciscoasa>
```

VSS 内のスイッチの場合、**switch** 引数を入力します。

session slot processor 0 コマンドは、他のサービスモジュールではサポートされていますが、ASASM ではサポートされていません。ASASM にはプロセッサ 0 がありません。

モジュールのスロット番号を表示するには、スイッチプロンプトで **show module** コマンドを入力します。

ASADM へのログインパスワードを入力します。 **passwd** コマンドを使用してパスワードを設定します。デフォルトのパスワードはありません。

ユーザ EXEC モードにアクセスします。

ステップ 2 最高の特権レベルである特権 EXEC モードにアクセスします。

enable

パスワードを入力するように求められます。デフォルトではパスワードは空白に設定されているため、Enter キーを押して先に進みます。イネーブルパスワードを変更するには、[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定](#)を参照してください。

例：

```
ciscoasa> enable
Password:
ciscoasa#
```

設定以外のすべてのコマンドは、特権 EXEC モードで使用できます。特権 EXEC モードからコンフィギュレーションモードに入ることもできます。

特権モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

ステップ 3 グローバル コンフィギュレーション モードにアクセスします。

configure terminal

グローバル コンフィギュレーション モードを終了するには、**disable** コマンド、**exit** コマンド、または **quit** コマンドを入力します。

関連トピック

[管理アクセスのガイドライン](#)

[ホスト名、ドメイン名、およびイネーブルパスワードと Telnet パスワードの設定](#)

コンソールセッションのログアウト

ASASM からログアウトしない場合、コンソール接続は維持され、タイムアウトはありません。ASASM コンソールセッションを終了してスイッチの CLI にアクセスするには、次の手順を実行します。

意図せずに開いたままになっている可能性のある、別のユーザのアクティブな接続を終了するには、[アクティブなコンソール接続の終了 \(8 ページ\)](#)を参照してください。

手順

スイッチ CLI に戻るには、次を入力します。

Ctrl+Shift+6, x

スイッチ プロンプトに戻ります。

```
asasm# [Ctrl-Shift-6, x]
Router#
```

(注) 米国および英国キーボードの Shift+6 はキャレット記号 (^) を出力します。別のキーボードを使用しており、単独の文字としてキャレット記号 (^) を出力できない場合、一時的または永続的に、エスケープ文字を別の文字に変更できます。 **terminal escape-character *ascii_number*** コマンド (このセッションで変更する)、または **default escape-character *ascii_number*** コマンド (永続的に変更する) を使用します。たとえば、現在のセッションのシーケンスを **Ctrl-w, x** に変更するには、**terminal escape-character 23** を入力します。

アクティブなコンソール接続の終了

コンソール接続の永続性のために、ASASM を正しくログアウトしないと、意図したよりも長い時間にわたって接続が存在する可能性があります。他の人がログインする場合は、既存の接続を終了する必要があります。

手順

ステップ 1 スイッチ CLI から、**show users** コマンドを使用して、接続されたユーザを表示します。コンソールユーザは「con」と呼ばれます。ホストアドレスは、127.0.0.slot0 と表示されます (slot はモジュールのスロット番号です)。

show users

たとえば、次のコマンド出力は、スロット 2 にあるモジュールのライン 0 のユーザ「con」を示しています。

```
Router# show users
Line      User      Host(s)              Idle      Location
* 0       con 0     127.0.0.20          00:00:02
```

ステップ 2 コンソール接続のあるラインをクリアするには、次のコマンドを入力します。

clear line number

次に例を示します。

```
Router# clear line 0
```

Telnet セッションのログアウト

Telnet セッションを終了してスイッチ CLI にアクセスするには、次の手順を実行します。

手順

スイッチ CLI に戻るには、ASASM 特権モードまたはユーザ EXEC モードから **exit** を入力します。コンフィギュレーションモードに入っている場合は、Telnet セッションが終了するまで繰り返し **exit** を入力します。

スイッチ プロンプトに戻ります。

```
asasm# exit  
Router#
```

(注) 代わりに、エスケープシーケンス Ctrl+Shift+6, x を使用して、Telnet セッションをエスケープすることができます。このエスケープシーケンスを使用すると、スイッチ プロンプトで Enter キーを押すことで、Telnet セッションを再開できます。スイッチ から Telnet セッションを切断するには、スイッチ CLI で **disconnect** を入力します。セッションを切断しない場合、ASASM 設定に従って最終的にタイムアウトします。

ソフトウェア モジュール コンソールへのアクセス

ASA 5506-X に ASA FirePOWER などのソフトウェア モジュールをインストールしている場合、モジュール コンソールへのセッションを実行できます。



(注) **session** コマンドを使用して ASA バックプレーンを介してハードウェア モジュール CLI にアクセスすることはできません。

手順

ASA CLI から、モジュールへのセッションを実行します。

```
session {sfr | cxsc | ips} console
```

例 :

```
ciscoasa# session sfr console
Opening console session with module sfr.
Connected to module sfr. Escape character sequence is 'CTRL-^X'.

Cisco ASA SFR Boot Image 5.3.1
asasfr login: admin
Password: Admin123
```

ASA 5506W-X ワイヤレス アクセス ポイント コンソールへのアクセス

ワイヤレス アクセス ポイント コンソールにアクセスするには、次の手順を実行します。

手順

ステップ 1 ASA CLI から、アクセス ポイントへのセッションを実行します。

session wlan console

例：

```
ciscoasa# session wlan console
opening console session with module wlan
connected to module wlan. Escape character sequence is 'CTRL-^X'

ap>
```

ステップ 2 アクセス ポイント CLI については、『[Cisco IOS Configuration Guide for Autonomous Aironet Access Points](#)』 [英語] を参照してください。

ASDM アクセスの設定

ここでは、デフォルト コンフィギュレーションで ASDM にアクセスする方法、およびデフォルト設定がない場合にアクセスを設定する方法について説明します。

ASDM アクセス（アプライアンス、ASA v）に対する工場出荷時のデフォルト コンフィギュレーションの使用

工場出荷時のデフォルト コンフィギュレーションでは、ASDM 接続はデフォルトのネットワーク設定で事前設定されています。

手順

次のインターフェイスおよびネットワーク設定を使用して ASDM に接続します。

- 管理インターフェイスは、ご使用のモデルによって異なります。
 - Firepower 4100/9300：展開時に定義された管理タイプインターフェイスと IP アドレス。管理ホストは任意のネットワークからアクセスできます。
 - ASA 5506-X、ASA 5508-X および ASA 5516-X：内部 GigabitEthernet 1/2（192.168.1.1）および ASA 5506W-X、Wi-Fi GigabitEthernet 1/9（192.168.10.1）用。内部ホストは 192.168.1.0/24 ネットワークに限定され、Wi-Fi ホストは 192.168.10.0/24 に限定されます。
 - ASA 5512-X 以降：管理 0/0（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。
 - ASA：管理 0/0（導入時に設定）。管理ホストは管理ネットワークに限定されます。
 - ISA 3000：管理 1/1（192.168.1.1）。管理ホストは 192.168.1.0/24 ネットワークに限定されます。

(注) マルチ コンテキスト モードに変更すると、上記のネットワーク設定を使用して管理コンテキストから ASDM にアクセスできるようになります。

関連トピック

[工場出荷時のデフォルト設定](#)（20 ページ）

[マルチ コンテキスト モードの有効化またはディセーブル化](#)

[ASDM の起動](#)（16 ページ）

ASDM アクセスのカスタマイズ

この手順は、ASA サービス モジュールを除くすべてのモデルに適用されます。

次の条件に 1 つ以上当てはまる場合は、この手順を使用します。

- 工場出荷時のデフォルト コンフィギュレーションがない。
- トランスペアレント ファイアウォール モードに変更したい。
- マルチ コンテキスト モードに変更したい。

シングルルーテッドモードの場合、ASDM に迅速かつ容易にアクセスするために、独自の管理 IP アドレスを設定できるオプションを備えた工場出荷時のデフォルト コンフィギュレーションを適用することを推奨します。この項に記載されている手順は、特別なニーズ（トランスペアレントモードやマルチ コンテキスト モードの設定など）がある場合や、他の設定を維持する必要がある場合にのみ使用してください。



- (注) ASA v の場合、導入時にトランスペアレントモードを設定できるため、この手順は、設定をクリアする必要がある場合など、導入後に特に役立ちます。

手順

ステップ 1 コンソールポートで CLI にアクセスします。

ステップ 2 (オプション) トランスペアレントファイアウォールモードをイネーブルにします。

このコマンドは、設定をクリアします。

firewall transparent

ステップ 3 管理インターフェイスを設定します。

```
interface interface_id
  nameif name
  security-level level
  no shutdown
  ip address ip_address mask
```

例 :

```
ciscoasa(config)# interface management 0/0
ciscoasa(config-if)# nameif management
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
```

security-level は、1 ~ 100 の数字です。100 が最も安全です。

ステップ 4 (直接接続された管理ホスト用) 管理ネットワークの DHCP プールを設定します。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例 :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 management
ciscoasa(config)# dhcpd enable management
```

その範囲にインターフェイスアドレスが含まれていないことを確認します。

ステップ 5 (リモート管理ホスト用) 管理ホストへのルートを設定します。

```
route management_ifc management_host_ip mask gateway_ip 1
```

例 :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50 1
```

ステップ 6 ASDM の HTTP サーバをイネーブルにします。

http server enable

ステップ 7 管理ホストの ASDM へのアクセスを許可します。

http ip_address mask interface_name

例 :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

ステップ 8 設定を保存します。

write memory

ステップ 9 (オプション) モードをマルチ モードに設定します。

mode multiple

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASA をリロードするよう求められます。

例

次の設定では、ファイアウォール モードがトランスペアレント モードに変換され、Management 0/0 インターフェイスが設定され、管理ホストに対して ASDM がイネーブルにされます。

```
firewall transparent
interface management 0/0

ip address 192.168.1.1 255.255.255.0
nameif management
security-level 100
no shutdown

dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
http server enable
http 192.168.1.0 255.255.255.0 management
```

関連トピック

- [工場出荷時のデフォルト設定の復元 \(21 ページ\)](#)
- [ファイアウォール モード \(シングル モード\) の設定](#)
- [アプライアンス コンソールへのアクセス \(1 ページ\)](#)
- [ASDM の起動 \(16 ページ\)](#)

ASA サービス モジュールの ASDM アクセスの設定

ASASMには物理インターフェイスがないため、ASDMアクセスが事前設定されていません。ASASMのCLIを使用してASDMアクセスを設定する必要があります。ASDMアクセス用にASASMを設定するには、次の手順を実行します。

始める前に

ASASMのクイックスタートガイドに従って、ASASMにVLANインターフェイスを割り当てます。

手順

ステップ1 ASASMに接続し、グローバルコンフィギュレーションモードにアクセスします。

ステップ2 (オプション) トランスペアレントファイアウォールモードをイネーブルにします。

firewall transparent

このコマンドは、設定をクリアします。

ステップ3 ご使用のモードに応じて、次のいずれかの操作を行って管理インターフェイスを設定します。

- ルーテッドモード：インターフェイスをルーテッドモードで設定します。

```
interface vlan number
  ip address ip_address [mask]
  nameif name
  security-level level
```

例：

```
ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1～100の数字です。100が最も安全です。

- トランスペアレントモード：ブリッジ仮想インターフェイスを設定し、ブリッジグループに管理VLANを割り当てます。

```
interface bvi number
  ip address ip_address [mask]

interface vlan number
  bridge-group bvi_number
  nameif name
  security-level level
```

例：

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0

ciscoasa(config)# interface vlan 1
ciscoasa(config-if)# bridge-group 1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
```

security-level は、1 ～ 100 の数字です。100 が最も安全です。

- ステップ 4** (直接接続された管理ホスト用) 管理インターフェイス ネットワーク上の管理ホストの DHCP をイネーブルにします。

```
dhcpd address ip_address-ip_address interface_name
dhcpd enable interface_name
```

例 :

```
ciscoasa(config)# dhcpd address 192.168.1.2-192.168.1.254 inside
ciscoasa(config)# dhcpd enable inside
```

この範囲内には管理アドレスを含めないでください。

- ステップ 5** (リモート管理ホスト用) 管理ホストへのルートを設定します。

```
route management_ifc management_host_ip mask gateway_ip 1
```

例 :

```
ciscoasa(config)# route management 10.1.1.0 255.255.255.0 192.168.1.50
```

- ステップ 6** ASDM の HTTP サーバをイネーブルにします。

```
http server enable
```

- ステップ 7** 管理ホストの ASDM へのアクセスを許可します。

```
http ip_address mask interface_name
```

例 :

```
ciscoasa(config)# http 192.168.1.0 255.255.255.0 management
```

- ステップ 8** 設定を保存します。

```
write memory
```

- ステップ 9** (オプション) モードをマルチ モードに設定します。

```
mode multiple
```

プロンプトが表示されたら、既存の設定を管理コンテキストに変換することを承認します。ASASM をリロードするよう求められます。

例

次のルーテッドモードの設定では、VLAN 1 のインターフェイスを設定し、管理ホストの ASDM のイネーブルにします。

```
interface vlan 1
nameif inside
ip address 192.168.1.1 255.255.255.0
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

次の設定では、ファイアウォールモードをトランスペアレントモードに変換し、VLAN 1 インターフェイスを設定して BVI 1 に割り当てた後、管理ホストの ASDM をイネーブルにします。

```
firewall transparent
interface bvi 1

ip address 192.168.1.1 255.255.255.0
interface vlan 1
bridge-group 1
nameif inside
security-level 100

dhcpd address 192.168.1.3-192.168.1.254 inside
dhcpd enable inside
http server enable
http 192.168.1.0 255.255.255.0 inside
```

関連トピック

[ASA サービス モジュール コンソールへのアクセス \(4 ページ\)](#)

[接続方法について \(4 ページ\)](#)

[コンソールセッションのログアウト \(7 ページ\)](#)

[アクティブなコンソール接続の終了 \(8 ページ\)](#)

[Telnet セッションのログアウト \(9 ページ\)](#)

[ファイアウォールモード \(シングルモード\) の設定](#)

ASDM の起動

ASDM は、次の 2 つの方法で起動できます。

- **ASDM-IDM ランチャ**：ランチャは、ASA から Web ブラウザを使用してダウンロードされるアプリケーションです。これを使用すると、任意の ASA IP アドレスに接続できます。他の ASA に接続する場合、ランチャを再度ダウンロードする必要はありません。
- **Java Web Start**：管理する ASA ごとに Web ブラウザで接続して、Java Web Start アプリケーションを保存または起動する必要があります。任意でコンピュータにショートカットを保存できます。ただし、ASA IP アドレスごとにショートカットを分ける必要があります。



- (注) Web Start を使用する場合は、Java キャッシュをクリアしてください。クリアしない場合、Hostscan などのログイン前ポリシーに対する変更が失われる可能性があります。この問題は、ランチャを使用している場合には発生しません。

ASDM では、管理のために別の ASA IP アドレスを選択できます。ランチャと Java Web Start の機能の違いは、主に、ユーザが最初にどのように ASA に接続し、ASDM を起動するかにあります。

ここでは、まず ASDM に接続する方法について説明します。次にランチャまたは Java Web Start を使用して ASDM を起動する方法について説明します。

ASDM はローカルの \Users\\.asdm ディレクトリ内にキャッシュ、ログ、および設定などのファイルを保存し、Temp ディレクトリ内にも AnyConnect プロファイルなどのファイルを保存します。

手順

ステップ 1 ASDM クライアントとして指定したコンピュータで次の URL を入力します。

https://asa_ip_address/admin

次のボタンを持つ ASDM 起動ページが表示されます。

- **Install ASDM Launcher and Run ASDM**
- **Run ASDM**
- **Run Startup Wizard**

ステップ 2 ランチャをダウンロードするには、次の手順を実行します。

- a) [Install ASDM Launcher and Run ASDM] をクリックします。
- b) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名およびイネーブルパスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注**：HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

- c) インストーラをコンピュータに保存して、インストーラを起動します。インストールが完了すると、ASDM-IDM ランチャが自動的に開きます。
- d) 管理IPアドレス、および同じユーザ名とパスワード（新規インストールの場合は空白）を入力し、[OK] をクリックします。

ステップ 3 Java Web Start を使用するには：

- a) [Run ASDM] または [Run Startup Wizard] をクリックします。
- b) プロンプトが表示されたら、ショートカットをコンピュータに保存します。オプションで、アプリケーションを保存せずに開くこともできます。
- c) ショートカットから Java Web Start を起動します。
- d) 表示されたダイアログボックスに従って、任意の証明書を受け入れます。Cisco ASDM-IDM Launcher が表示されます。
- e) ユーザ名とパスワードのフィールドを空のままにし（新規インストールの場合）、[OK] をクリックします。HTTPS 認証が設定されていない場合は、ユーザ名およびイネーブルパスワード（デフォルトで空白）を入力しないで ASDM にアクセスできます。**注：**HTTPS 認証をイネーブルにした場合、ユーザ名と関連付けられたパスワードを入力します。認証が有効でない場合でも、ログイン画面で（ユーザ名をブランクのままにしないで）ユーザ名とパスワードを入力すると、ASDM によってローカルデータベースで一致がチェックされます。

ASDM 動作のカスタマイズ

アイデンティティ証明書をインストールして ASDM を正常に起動するだけでなく、ASDM ヒープメモリを増大することもできるため、より大きいサイズのコンフィギュレーションを処理できます。

ASDM のアイデンティティ証明書のインストール

Java 7 Update 51 以降を使用する場合、ASDM ランチャには信頼できる証明書が必要です。証明書の要件は、自己署名付きの ID 証明書をインストールすることによって簡単に満たすことができます。証明書をインストールするまで、Java Web Start を使用して ASDM を起動することができます。

ASDM で使用するために ASA に自己署名された ID 証明書をインストールし、Java を使用して証明書を登録するには、次のマニュアルを参照してください。

<http://www.cisco.com/go/asdm-certificate>

ASDM コンフィギュレーションメモリの増大

ASDM でサポートされる最大設定サイズは 512 KB です。このサイズを超えると、パフォーマンスの問題が生じることがあります。たとえば、コンフィギュレーションのロード時には、完了したコンフィギュレーションの割合がステータスダイアログボックスに表示されます。この

とき、サイズの大きいコンフィギュレーションでは、ASDM によってまだコンフィギュレーションの処理が行われていても、完了した割合の増分が停止し、操作が中断されているように見えます。このような状況が発生した場合は、ASDM システム ヒープメモリの増大を検討することを推奨します。

Windows での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリ サイズを増大するには、次の手順を実行して **run.bat** ファイルを編集します。

手順

-
- ステップ 1** ASDM インストールディレクトリ（たとえば、C:\Program Files (x86)\Cisco Systems\ASDM）に移動します。
 - ステップ 2** 任意のテキストエディタを使用して **run.bat** ファイルを編集します。
 - ステップ 3** 「start javaw.exe」で始まる行で、「-Xmx」のプレフィックスが付いた引数を変更し、目的のヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。
 - ステップ 4** **run.bat** ファイルを保存します。
-

Mac OS での ASDM コンフィギュレーションメモリの増大

ASDM ヒープメモリ サイズを増大するには、次の手順を実行して **Info.plist** ファイルを編集します。

手順

-
- ステップ 1** [Cisco ASDM-IDM] アイコンを右クリックし、[Show Package Contents] を選択します。
 - ステップ 2** [Contents] フォルダで、Info.plist ファイルをダブルクリックします。開発者ツールをインストールしている場合は、**プロパティリストエディタ**で開きます。そうでない場合は、**TextEdit** で開きます。
 - ステップ 3** [Java]>[VMOptions] で、「-Xmx」のプレフィックスが付いた文字列を変更し、必要なヒープサイズを指定します。たとえば、768 MB の場合は -Xmx768M に変更し、1 GB の場合は -Xmx1G に変更します。

```

<key>CFBundleIconFile</key>
<string>asdm32.icns</string>

<key>VMOptions</key>
<string>-Xms64m -Xmx512m</string>

<key>CFBundleDocumentTypes</key>
<array>

```

ステップ4 このファイルがロックされると、次のようなエラーが表示されます。



ステップ5 [Unlock] をクリックし、ファイルを保存します。

[Unlock] ダイアログボックスが表示されない場合は、エディタを終了します。[Cisco ASDM-IDM] アイコンを右クリックし、[Copy Cisco ASDM-IDM] を選択して、書き込み権限がある場所（デスクトップなど）に貼り付けます。その後、このコピーからヒープサイズを変更します。

工場出荷時のデフォルト設定

工場出荷時のデフォルト設定とは、シスコが新しい ASA に適用したコンフィギュレーションです。

- ASA 5506-X、5508-X および 5516-X：工場出荷時のデフォルト設定により、機能内部/外部設定が有効になります。ASA は、内部インターフェイスから ASDM を使用して管理できます。
- ASA 5512-X ～ ASA 5585-X：管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- Firepower 4100/9300 シャーシ：ASA のスタンドアロンまたはクラスタを展開する場合、管理用のインターフェイスは工場出荷時のデフォルト設定によって設定されるため、ASDM を使用してこのインターフェイスに接続して設定を完了できます。
- ASA v：ハイパーバイザによっては、導入の一環として、管理用のインターフェイス導入設定（初期の仮想導入設定）によって設定されるため、ASDM を使用してこのインター

フェイスに接続して設定を完了できます。フェールオーバー IP アドレスも設定できます。また、必要に応じて、「工場出荷時のデフォルト」コンフィギュレーションを適用することもできます。

- **ASASM** : デフォルト設定はありません。コンフィギュレーションを開始するには、[ASA サービス モジュール コンソールへのアクセス \(4 ページ\)](#) を参照してください。
- **ISA 3000** : 工場出荷時のデフォルト設定は、同じネットワーク上のすべての内部および外部インターフェイスを使用した、ほぼ完全なトランスペアレントファイアウォールモード設定です。ASDM を使用して管理インターフェイスに接続し、ネットワークの IP アドレスを設定できます。ハードウェアバイパスは2つのインターフェイスペアに対して有効になっており、すべてのトラフィックはインラインタップモニター専用モードで ASA FirePOWER モジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

アプライアンス および Firepower 4100/9300 シャーシ の場合、工場出荷時のデフォルト設定は、ルーテッドファイアウォールモードとシングルコンテキストモードのみで使用できます。ASA の場合、導入時にトランスペアレントモードまたはルーテッドモードを選択できます。



- (注) イメージファイルと (隠された) デフォルト コンフィギュレーションに加え、`log/`、`crypto_archive/`、および `coredumpinfo/coredump.cfg` がフラッシュ メモリ内の標準のフォルダとファイルです。フラッシュ メモリ内で、これらのファイルの日付は、イメージファイルの日付と一致しない場合があります。これらのファイルは、トラブルシューティングに役立ちますが、障害が発生したことを示すわけではありません。

工場出荷時のデフォルト設定の復元

この項では、工場出荷時のデフォルト コンフィギュレーションを復元する方法について説明します。CLI および ASDM の両方の手順が提供されています。ASA では、この手順を実行することで導入設定が消去され、ASA 5525-X の場合と同じ工場出荷時のデフォルト設定が適用されます。



- (注) ASASM で出荷時のデフォルト コンフィギュレーションを復元すると、設定は消去されます。工場出荷時のデフォルト コンフィギュレーションはありません。

Firepower 4100/9300 では、工場出荷時のデフォルト設定を復元すると単に設定が消去されるだけです。デフォルト設定を復元するには、スーパバイザから ASA をもう一度展開する必要があります。

始める前に

この機能は、ルーテッドファイアウォールモードでのみ使用できます。トランスペアレントモードの場合、インターフェイスの IP アドレスがサポートされません。さらに、この機能は

シングル コンテキスト モードでのみ使用できます。コンフィギュレーションがクリアされた ASA には、この機能を使用して自動的に設定する定義済みコンテキストがありません。

手順

ステップ 1 工場出荷時のデフォルト コンフィギュレーションを復元します。

configure factory-default [*ip_address* [*mask*]]

例 :

```
ciscoasa(config)# configure factory-default 10.1.1.1 255.255.255.0
```

ip_address を指定する場合は、デフォルトの IP アドレスを使用する代わりに、お使いのモデルに応じて、内部または管理インターフェイスの IP アドレスを設定します。*ip_address* オプションで設定されているインターフェイスについては、次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 : 効果はありません。
- ASA v : 管理インターフェイスの IP アドレスを設定します。
- ASA 5506-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5508-X および 5516-X : 内部インターフェイスの IP アドレスを設定します。
- ASA 5512-X、5515-X、5525-X、5545-X、5555-X : 管理インターフェイスの IP アドレスを設定します。
- ASA 5585-X : 管理インターフェイスの IP アドレスを設定します。
- ISA 3000 : 管理インターフェイスの IP アドレスを設定します。
- ASASM : 効果はありません。

http コマンドでは、ユーザが指定するサブネットが使用されます。同様に、**dhcpd address** コマンドの範囲は、指定したサブネット内のアドレスで構成されます。

Firepower 2100 の場合 : このモデルでは、**boot system** コマンドは使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合 : このコマンドは、残りの設定とともに **boot system** コマンドをクリアします (存在する場合)。**boot system** コマンドを使用すると、特定のイメージから起動できます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュメモリの最初のイメージからブートします。内部フラッシュメモリにイメージがない場合、ASA はブートしません。

ステップ 2 デフォルト コンフィギュレーションをフラッシュメモリに保存します。

write memory

このコマンドでは、事前に **boot config** コマンドを設定して、別の場所を設定していた場合でも、実行コンフィギュレーションはスタートアップコンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションがクリアされると、このパスもクリアされます。

ステップ 3 (ASDM での手順。) メイン ASDM アプリケーション ウィンドウで、次を実行します。

a) **[File] > [Reset Device to the Factory Default Configuration]** の順に選択します。

[Reset Device to the Default Configuration] ダイアログボックスが表示されます。

b) (オプション) デフォルトアドレスを使用する代わりに、管理または内部インターフェイスの**管理 IP アドレス**を入力します。

モデルごとに設定されているインターフェイス IP の詳細については、前述の CLI 手順を参照してください。

c) (オプション) ドロップダウン リストから **[Management Subnet Mask]** を選択します。

d) **[OK]** をクリックします。

確認用のダイアログボックスが表示されます。

(注) Firepower 2100 の場合：このモデルでは、ブートイメージの場所は使用されません。パッケージは FXOS によって管理されます。

その他すべてのモデルの場合：この操作により、残りの設定とともにブートイメージの場所もクリアされます (存在する場合)。**[Configuration] > [Device Management] > [System Image/Configuration] > [Boot Image/Configuration]** ペインでは、外部メモリ上のイメージを含む、特定のイメージからブートできます。出荷時の設定に戻した後、次回 ASA をリロードすると、内部フラッシュメモリの最初のイメージからブートします。内部フラッシュメモリにイメージがない場合、ASA はブートしません。

e) **[Yes]** をクリックします。

f) デフォルト設定を復元したら、この設定を内部フラッシュメモリに保存します。**[File] > [Save Running Configuration to Flash]** を選択します。

このオプションを選択すると、以前に別の場所を設定している場合でも、実行コンフィギュレーションがスタートアップコンフィギュレーションのデフォルトの場所に保存されます。コンフィギュレーションをクリアした場合は、このパスもクリアされています。

ASA v 導入設定の復元

この項では、ASA v の導入 (第 0 日) 設定を復元する方法について説明します。

手順

ステップ 1 フェールオーバーを行うために、スタンバイ装置の電源を切ります。

スタンバイユニットがアクティブになることを防ぐために、電源をオフにする必要があります。電源を入れたままにした場合、アクティブ装置の設定を消去すると、スタンバイ装置がアクティブになります。以前のアクティブユニットをリロードし、フェールオーバーリンクを介して再接続すると、古い設定は新しいアクティブユニットから同期し、必要な導入コンフィギュレーションが消去されます。

ステップ 2 リロード後に導入設定を復元します。フェールオーバーを行うために、アクティブ装置で次のコマンドを入力します。

write erase

(注) ASA が現在の実行イメージをブートするため、元のブートイメージには戻りません。元のブートイメージを使用するには、**boot image** コマンドを参照してください。コンフィギュレーションは保存しないでください。

ステップ 3 ASA をリロードし、導入設定をロードします。

reload

ステップ 4 フェールオーバーを行うために、スタンバイ装置の電源を投入します。

アクティブ装置のリロード後、スタンバイ装置の電源を投入します。導入設定がスタンバイ装置と同期されます。

ASA 5506-X、5508-X、および 5516-X のデフォルト設定

ASA 5506-X シリーズ、5508-X、および 5516-X の工場出荷時のデフォルト設定は、次のとおりです。

- 内部 --> 外部へのトラフィックフロー：GigabitEthernet 1/1（外部）、GigabitEthernet 1/2（内部）
- DHCP の外部 IP アドレス、内部 IP アドレス：192.168.1.1
- (ASA 5506W-X) WiFi<--> 内部のトラフィックフロー、WiFi --> 外部へのトラフィックフロー：GigabitEthernet 1/9（WiFi）
- (ASA 5506W-X) WiFi の IP アドレス：192.168.10.1
- 内部および WiFi 上のクライアントに対する DHCP。アクセスポイント自体とそのすべてのクライアントが ASA を DHCP サーバとして使用します。
- 管理 1/1 インターフェイスが稼働しているが、そうでない場合は未設定。ASA FirePOWER モジュールは、このインターフェイスを使用して ASA 内部ネットワークに接続し、内部インターフェイスをインターネットへのゲートウェイとして使用できます。
- ASDM アクセス：内部ホストと WiFi ホストが許可されます。

- NAT : 内部、WiFi、および管理から外部へのすべてのトラフィックのインターフェイス PAT。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface Management1/1
  management-only
  no nameif
  no security-level
  no ip address
  no shutdown
interface GigabitEthernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
interface GigabitEthernet1/2
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  no shutdown
!
object network obj_any
  subnet 0.0.0.0 0.0.0.0
  nat (any,outside) dynamic interface
!
http server enable
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.5-192.168.1.254 inside
dhcpd enable inside
!
logging asdm informational
```

ASA 5506W-X の場合は、次のコマンドも含まれます。

```
same-security-traffic permit inter-interface
!
interface GigabitEthernet 1/9
  security-level 100
  nameif wifi
  ip address 192.168.10.1 255.255.255.0
  no shutdown
!
http 192.168.10.0 255.255.255.0 wifi
!
dhcpd address 192.168.10.2-192.168.10.254 wifi
dhcpd enable wifi
```

ASA 5512-X ~ ASA 5585-X デフォルト設定

ASA 5512-X ~ ASA 5585-X の工場出荷時のデフォルト設定は、次のとおりです。

- 管理インターフェイス : Management 0/0 (管理)。
- IP アドレス : 管理アドレスは 192.168.1.1/24 です。

- DHCP サーバ：管理ホストでは DHCP サーバがイネーブルにされているため、管理インターフェイスに接続するコンピュータには、192.168.1.2～192.168.1.254 の間のアドレスが割り当てられます。
- ASDM アクセス：管理ホストに許可されます。

このコンフィギュレーションは次のコマンドで構成されています。

```
interface management 0/0
 ip address 192.168.1.1 255.255.255.0
 nameif management
 security-level 100
 no shutdown
!
asdm logging informational
asdm history enable
!
http server enable
http 192.168.1.0 255.255.255.0 management
!
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd enable management
```

Firepower 4100/9300 シャーシ デフォルト設定

Firepower 4100/9300 シャーシ 上に ASA を展開した場合、ASDM を使用して管理インターフェイスへの接続が可能になる多くのパラメータを事前設定できます。一般的な構成には次の設定があります。

- 管理インターフェイス：
 - Firepower 4100/9300 シャーシスーパーバイザ上で定義された任意の管理タイプインターフェイス
 - 名前は「management」
 - 任意の IP アドレス
 - セキュリティ レベル 0
 - 管理専用
- 管理インターフェイス内のデフォルト ルート
- ASDM アクセス：すべてのホストが許可されます。

スタンドアロンユニットの設定は、次のコマンドで構成されます。クラスタ ユニットの追加の設定については、[ASA クラスターの作成](#) を参照してください。

```
interface <management_ifc>
 management-only
 ip address <ip_address> <mask>
 ipv6 address <ipv6_address>
```

```
ipv6 enable
nameif management
security-level 0
no shutdown
!
http server enable
http 0.0.0.0 0.0.0.0 management
http ::/0 management
!
route management 0.0.0.0 0.0.0.0 <gateway_ip> 1
ipv6 route management ::/0 <gateway_ipv6>
```

ISA 3000 のデフォルト設定

ISA 3000 の工場出荷時のデフォルト設定は、次のとおりです。

- トランスペアレントファイアウォールモード：トランスペアレントファイアウォールは、「Bump In The Wire」または「ステルスファイアウォール」のように動作するレイヤ2ファイアウォールであり、接続されたデバイスへのルータホップとしては認識されません。
- 1ブリッジ仮想インターフェイス：すべてのメンバーインターフェイスは同じネットワーク内に存在しています（IPアドレスは事前設定されていません。ネットワークと一致するように設定する必要があります）：GigabitEthernet 1/1（outside1）、GigabitEthernet 1/2（inside1）、GigabitEthernet 1/3（outside2）、GigabitEthernet 1/4（inside2）
- すべての内部および外部インターフェイスは相互通信できます。
- 管理 1/1インターフェイス：ASDM アクセスの 192.168.1.1/24。
- 管理上のクライアントに対する DHCP。
- ASDM アクセス：管理ホストに許可されます。
- ハードウェアバイパスは、次のインターフェイスペアで有効になっています。GigabitEthernet 1/1 および 1/2。GigabitEthernet 1/3 および 1/4



(注) ISA 3000 への電源が切断され、ハードウェアバイパスモードに移行すると、通信できるのは上記のインターフェイスペアのみになります。inside1 と inside2 および outside1 と outside2 は通信できなくなります。これらのインターフェイス間の既存の接続がすべて失われます。電源が再投入されると、ASA がフローを引き継ぐため、接続が短時間中断されます。

- ASA Firepower モジュール：すべてのトラフィックが、Inline Tap Monitor-Only モードのモジュールに送信されます。このモードでは、モニタリング目的でのみトラフィックの重複ストリームが ASA Firepower モジュールに送信されます。

このコンフィギュレーションは次のコマンドで構成されています。

```

firewall transparent

interface GigabitEthernet1/1
  bridge-group 1
  nameif outside1
  security-level 0
  no shutdown
interface GigabitEthernet1/2
  bridge-group 1
  nameif inside1
  security-level 100
  no shutdown
interface GigabitEthernet1/3
  bridge-group 1
  nameif outside2
  security-level 0
  no shutdown
interface GigabitEthernet1/4
  bridge-group 1
  nameif inside2
  security-level 100
  no shutdown
interface Management1/1
  management-only
  no shutdown
  nameif management
  security-level 100
  ip address 192.168.1.1 255.255.255.0
interface BVI1
  no ip address

access-list allowAll extended permit ip any any
access-group allowAll in interface outside1
access-group allowAll in interface outside2

same-security-traffic permit inter-interface

hardware-bypass GigabitEthernet 1/1-1/2
hardware-bypass GigabitEthernet 1/3-1/4

http server enable
http 192.168.1.0 255.255.255.0 management

dhcpd address 192.168.1.5-192.168.1.254 management
dhcpd enable management

access-list sfrAccessList extended permit ip any any
class-map sfrclass
  match access-list sfrAccessList
policy-map global_policy
  class sfrclass
    sfr fail-open monitor-only
service-policy global_policy global

```

ASAv 導入設定

ASAv 上に ASA を展開した場合、ASDM を使用して管理 0/0 インターフェイスへの接続が可能になる多くのパラメータを前もって設定できます。一般的な構成には次の設定があります。

- ルーテッドファイアウォールモードまたはトランスペアレントファイアウォールモード
- Management 0/0 インターフェイス：
 - 名前は「management」
 - IP アドレスまたは DHCP
 - セキュリティ レベル 0
- 管理ホスト IP アドレスのスタティック ルート（管理サブネット上にない場合）
- HTTP サーバの有効または無効
- 管理ホスト IP アドレス用の HTTP アクセス
- （オプション） GigabitEthernet 0/8 用のフェールオーバー リンク IP アドレス、 Management0/0 のスタンバイ IP アドレス
- DNS サーバ
- スマート ライセンス ID トークン
- スマート ライセンスのスループット レベルおよび標準機能ティア
- （オプション） Smart Call Home HTTP プロキシ URL およびポート
- （オプション） SSH 管理設定：
 - クライアント IP アドレス
 - ローカル ユーザ名とパスワード
 - ローカル データベースを使用する SSH に必要な認証
- （オプション） REST API の有効または無効



(注) Cisco 認証局に正常に登録するには、ASA v をインターネット アクセスが必要です。インターネット アクセスを実行して正常にライセンス登録するには、導入後に追加の設定が必要になることがあります。

スタンドアロンユニットについては、次の設定例を参照してください。

```
interface Management0/0
  nameif management
  security-level 0
  ip address ip_address

  no shutdown
http server enable
http management_host_IP mask management
route management management_host_IP mask gateway_ip 1
dns server-group DefaultDNS
```

```

name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent

```

フェールオーバー ペアのプライマリ ユニットについては、次の設定例を参照してください。

```

nameif management
security-level 0
ip address ip_address standby standby_ip

no shutdown
route management management_host_IP mask gateway_ip 1
http server enable
http management_host_IP mask management
dns server-group DefaultDNS
  name-server ip_address
call-home
  http-proxy ip_address port port
license smart
  feature tier standard
  throughput level {100M | 1G | 2G}
  license smart register idtoken id_token
aaa authentication ssh console LOCAL
username username password password
ssh source_IP_address mask management
rest-api image boot:/path
rest-api agent
failover
failover lan unit primary
failover lan interface fover gigabitethernet0/8
failover link fover gigabitethernet0/8
failover interface ip fover primary_ip mask standby standby_ip

```

設定の開始

ASA を設定してモニタするには、次の手順を実行します。



- (注) ASDM では、最大 512 KB の設定をサポートしています。このサイズを超えると、パフォーマンスの問題が生じることがあります。[ASDM コンフィギュレーションメモリの増大 \(18 ページ\)](#) を参照してください。

手順

- ステップ 1 Startup Wizard を使用して初期設定を行うには、[Wizards] > [Startup Wizard] を選択します。
- ステップ 2 IPsec VPN Wizard を使用して IPsec VPN 接続を設定するには、[Wizards] > [IPsecVPN Wizard] を選択して、表示される各画面で設定を行います。
- ステップ 3 SSL VPN Wizard を使用して SSL VPN 接続を設定するには、[Wizards] > [SSL VPN Wizard] を選択して、表示される各画面で設定を行います。
- ステップ 4 高可用性とスケーラビリティに関する設定値を設定するには、[Wizards] > [High Availability and Scalability Wizard] を選択します。
- ステップ 5 Packet Capture Wizard を使用してパケットキャプチャを設定するには、[Wizards] > [Packet Capture Wizard] を選択します。
- ステップ 6 ASDM GUI で使用できるさまざまな色とスタイルを表示するには、[View] > [Office Look and Feel] を選択します。
- ステップ 7 機能を設定するには、ツールバーの [Configuration] ボタンをクリックし、いずれかの機能ボタンをクリックして、関連する設定ペインを表示します。

(注) [Configuration] 画面が空白の場合は、ツールバーで [Refresh] をクリックして、画面のコンテンツを表示します。
- ステップ 8 ASA をモニタするには、ツールバーの [Monitoring] ボタンをクリックし、機能ボタンをクリックして、関連するモニタリング ペインを表示します。

ASDM でのコマンドラインインターフェイス ツールの使用

この項では、ASDM を使用してコマンドを入力する方法および CLI の使用方法について説明します。

コマンドライン インターフェイス ツールの使用

この機能には、コマンドを ASA に送信して結果を表示する、テキストベースのツールが用意されています。

CLI ツールによって入力可能なコマンドは、ユーザ権限によって異なります。メイン ASDM アプリケーションウィンドウの下部にあるステータスバーの権限レベルを見て、CLI 特権コマンドを実行するために必要な特権があるかどうかを確認してください。

始める前に

- ASDM の CLI ツールから入力するコマンドは、ASA の接続ターミナルから入力するコマンドと動作が異なる場合があります。

- コマンドエラー：誤った入力コマンドによってエラーが発生した場合、その誤ったコマンドはスキップされ、その他のコマンドは処理されます。[Response] 領域には、他の関連情報とともに、エラーが発生したかどうかについての情報を示すメッセージが表示されます。
- インタラクティブ コマンド：インタラクティブ コマンドは、CLI ツールではサポートされていません。これらのコマンドを ASDM で使用するには、次のコマンドに示すように、**noconfirm** キーワード（使用可能な場合）を使用します。

```
crypto key generate rsa modulus 1024 noconfirm
```

- 他の管理者との競合を回避：複数の管理ユーザが ASA の実行コンフィギュレーションをアップデートできます。ASDM の CLI ツールでコンフィギュレーションを変更する場合は、アクティブな管理セッションが他にないことを事前に確認してください。複数のユーザが同時に ASA を設定した場合、最新の変更が有効になります。

同じ ASA で現在アクティブな他の管理セッションを表示するには、[Monitoring]>[Properties]>[Device Access] の順に選択します。

手順

ステップ 1 メイン ASDM アプリケーション ウィンドウで、[Tools] > [Command Line Interface] の順に選択します。

[Command Line Interface] ダイアログボックスが表示されます。

ステップ 2 必要なコマンドのタイプ（1行または複数行）を選択し、ドロップダウンリストからコマンドを選択するか、または表示されたフィールドにコマンドを入力します。

ステップ 3 [Send] をクリックしてコマンドを実行します。

ステップ 4 新しいコマンドを入力するには、[Clear Response] をクリックしてから、実行する別のコマンドを選択（または入力）します。

ステップ 5 この機能の状況依存ヘルプを表示するには、[Enable context-sensitive help (?)] チェックボックスをオンにします。文脈依存ヘルプをディセーブルにするには、このチェックボックスをオフにします。

ステップ 6 設定を変更した場合は、[Command Line Interface] ダイアログボックスを閉じた後に、[Refresh] をクリックして ASDM での変更内容を表示します。

ASDM によって無視されるコマンドのデバイス上での表示

この機能により、ASDM がサポートしていないコマンドの一覧を表示できます。通常 ASDM は、これらのコマンドを無視します。ASDM は、実行コンフィギュレーションのこれらのコマンドを変更、削除することはありません。詳細については、「サポートされていないコマンド」を参照してください。

手順

ステップ1 メイン ASDM アプリケーション ウィンドウで、[Tools] > [Show Commands Ignored by ASDM on Device] の順に選択します。

ステップ2 完了したら、[OK] をクリックします。

接続の設定変更の適用

コンフィギュレーションに対してセキュリティポリシーの変更を加えた場合は、すべての新しい接続で新しいセキュリティポリシーが使用されます。既存の接続は、接続の確立時に設定されたポリシーを引き続き使用します。古い接続の **show** コマンド出力には古い設定が反映され、古い接続に関するデータを含まない場合があります。

たとえば、インターフェイスから **QoS service-policy** を削除し、修正バージョンを再度追加する場合、**show service-policy** コマンドには、新しいサービス ポリシーと一致する新規接続と関連付けられている **QoS** カウンタのみ表示されます。古いポリシーの既存の接続はコマンド出力には表示されません。

すべての接続が新しいポリシーを確実に使用するように、現在の接続を解除し、新しいポリシーを使用して再度接続できるようにします。

接続を解除するには、次のいずれかのコマンドを入力します。

- **clear local-host** [*ip_address*] [**all**]

このコマンドは、接続制限値や初期接続の制限など、クライアントごとのランタイム ステートを再初期化します。これにより、このコマンドは、これらの制限を使用しているすべての接続を削除します。ホストごとの現在のすべての接続を表示するには、**show local-host all** コマンドを参照してください。

引数を指定しないと、このコマンドは、影響を受けるすべての **through-the-box** 接続をクリアします。**to-the-box** 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。特定の IP アドレスへの、または特定の IP アドレスからの接続をクリアするには、*ip_address* 引数を使用します。

- **clear conn**[**all**] [**protocol** {**tcp** | **udp**}] [**address src_ip** [-*src_ip*] [**netmask mask**] [**port src_port** [-*src_port*] [**address dest_ip** [-*dest_ip*] [**netmask mask**] [**port dest_port** [-*dest_port*]

このコマンドは、すべての状態の接続を終了します。現在のすべての接続を表示するには、**show conn** コマンドを参照してください。

引数を指定しないと、このコマンドはすべての **through-the-box** 接続をクリアします。**to-the-box** 接続もクリアするには（現在の管理セッションを含む）、**all** キーワードを使用します。送信元 IP アドレス、宛先 IP アドレス、ポート、プロトコルに基づいて特定の接続をクリアするには、必要なオプションを指定できます。

