ASDM を使用した ASA の展開

この章の対象読者

Cisco ISA 3000 は、強力なラックマウント型のファイアウォールです。この章では、ネットワークに ISA 3000 ASA を展開する方法と初期設定の方法について説明します。この章では以下の展開については取り上げていませんので、『ASA コンフィギュレーション ガイド』を参照してください。

- フェールオーバー
- CLI 設定
- （9.16 以前）FirePOWER モジュール

この章では、基本的なセキュリティポリシーの設定手順についても説明します。より高度な要件がある場合は設定ガイドを参照してください。

ISA 3000 ハードウェアでは、ASA ソフトウェアか 脅威に対する防御 ソフトウェアを実行できます。ASA と 脅威に対する防御 との間で切り替えを行う際には、デバイスの再イメージ化が必要になります。「Cisco ASA および Firepower Threat Defense 再イメージ化ガイド」を参照してください。

プライバシー収集ステートメント：ISA 3000 には個人識別情報は不要です。積極的に収集することもありません。ただし、ユーザー名などの設定では、個人識別情報を使用できます。この場合、設定作業時や SNMP の使用時に、管理者が個人識別情報を確認できる場合があります。

• 次のステップ （14 ページ）

ASA について

ASA は、1 つのデバイスで高度でステートフルなファイアウォール機能および VPN コンセントレーター機能を提供します。

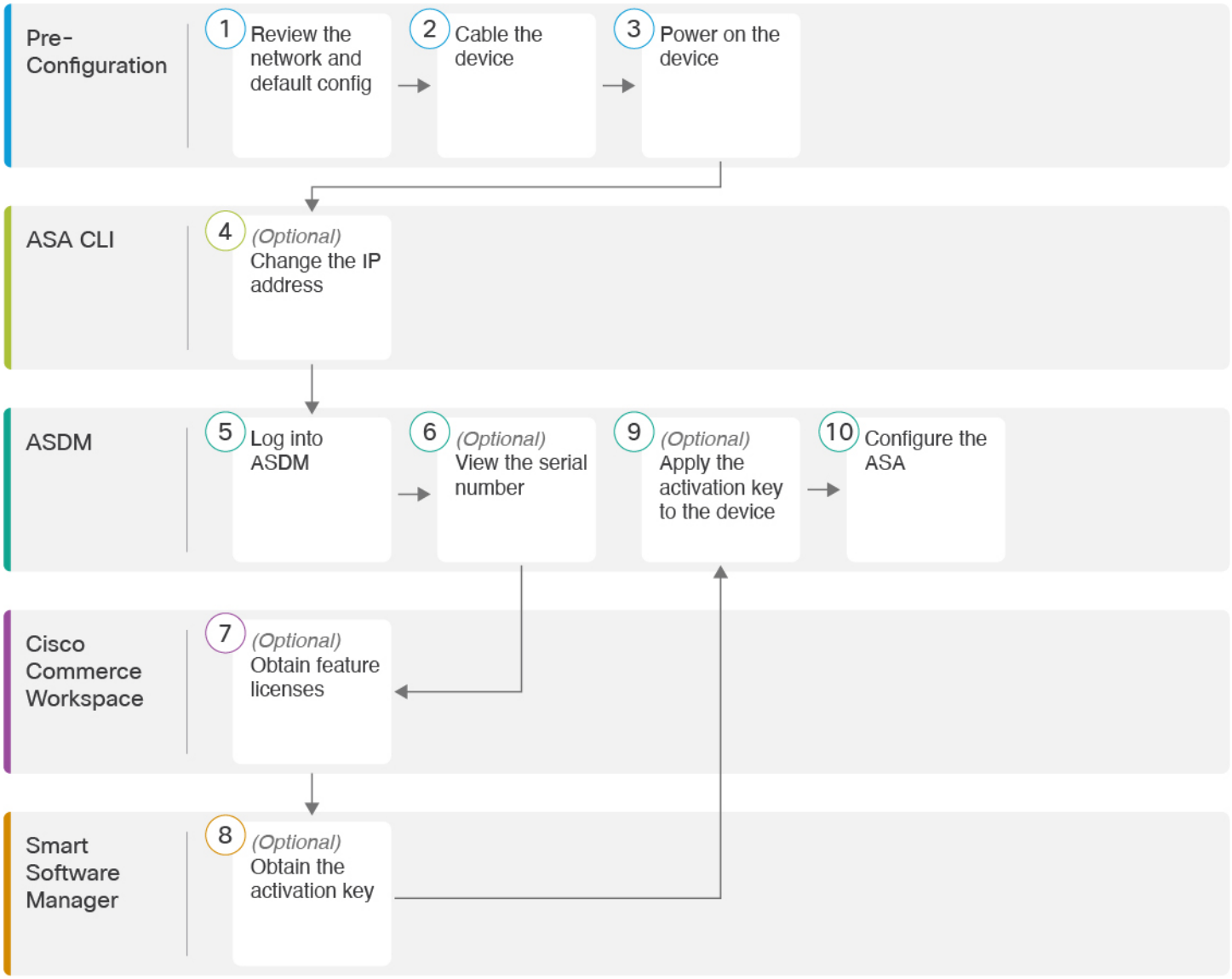
次のいずれかのマネージャを使用して ASA を管理できます。

- ASDM（このガイドで説明）：デバイスに含まれる単独のデバイスマネージャ。
- CLI
- CDO：シンプルなクラウドベースのマルチデバイスマネージャ。
- Cisco Security Manager：別のサーバー上のマルチデバイス マネージャ。

エンドツーエンドの手順

シャーシで ASA を展開して設定するには、次のタスクを参照してください。

図 *1*: エンドツーエンドの手順



1	事前設定	ネットワーク配置とデフォルト設定の確認 （4 ページ）。
2	事前設定	ファイアウォールのケーブル接続 （7 ページ）。
3	事前設定	デバイスの電源投入 （8 ページ）。
4	ASA CLI	（任意）IP アドレスの変更 （8 ページ）。
5	ASDM	ASDM へのログイン （9 ページ）。

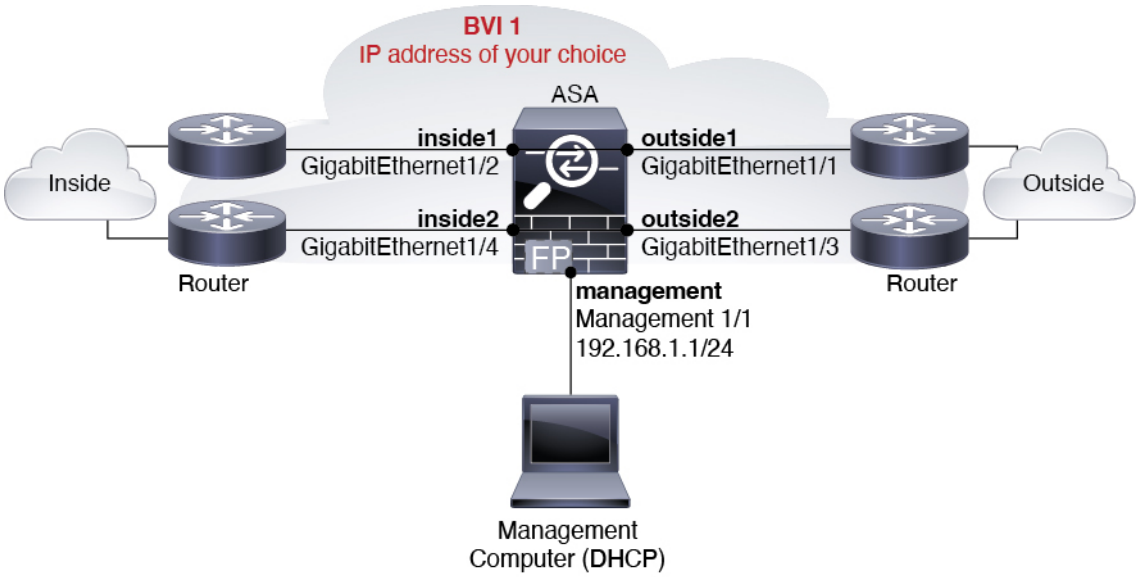
6	ASDM	（任意）ASA ライセンスの設定 （10 ページ）：シリアル番号を表示します。
7	Cisco Commerce Workspace	（任意）ASA ライセンスの設定 （10 ページ）：機能ライセンスを取得します。
8	Smart Software Manager	（任意）ASA ライセンスの設定 （10 ページ）：アクティベーションキーを取得します。
9	ASDM	（任意）ASA ライセンスの設定 （10 ページ）：アクティベーションキーをデバイスへ適用します。
10	ASDM	ASA の設定 （12 ページ）。

ネットワーク配置とデフォルト設定の確認

次の図に、ISA 3000 で推奨されるネットワーク展開を示します。

（注） ASDM アクセスにデフォルト管理 IP アドレスを使用できない場合は、ASA CLI で管理 IP アドレスを設定できます。「（任意）IP アドレスの変更 （8 ページ）」を参照してください。

図 *2 : ISA 3000* ネットワーク



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。

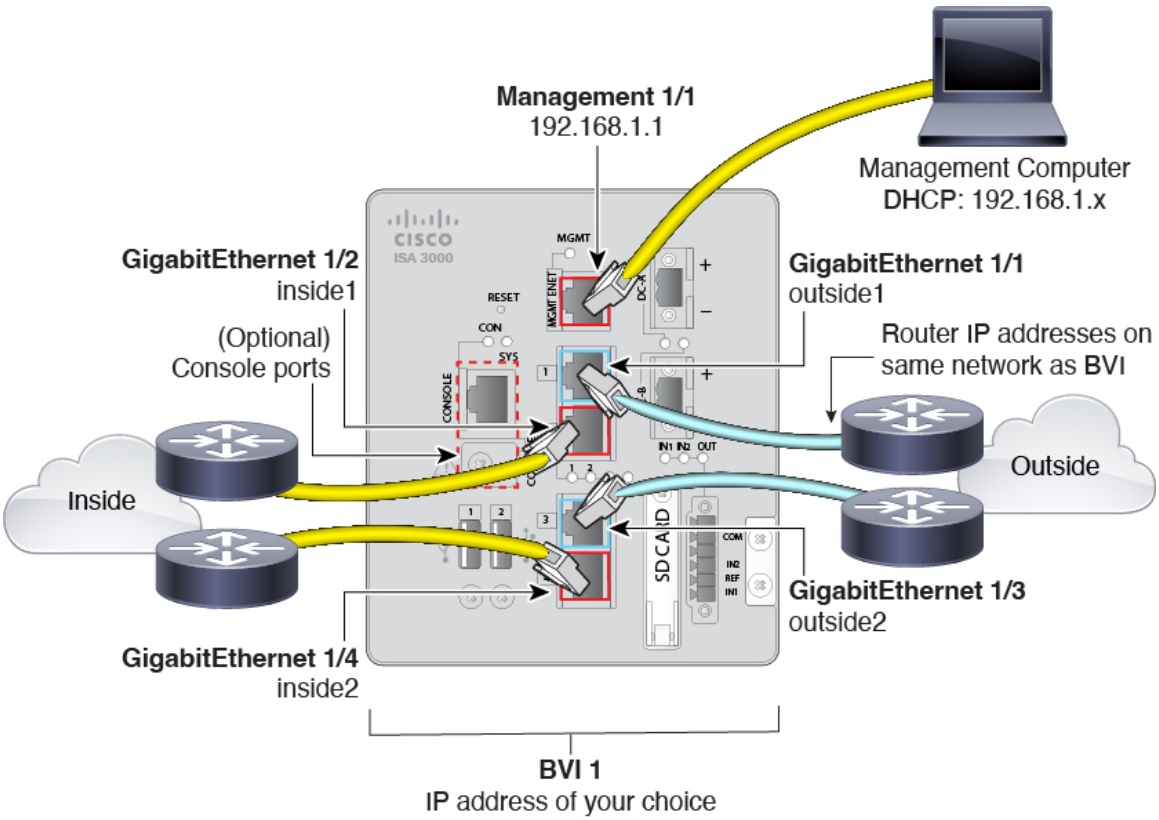
このコンフィギュレーションは次のコマンドで構成されています。

```
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
```

ファイアウォールのケーブル接続

図 *3:* ファイアウォールのケーブル接続



Management 1/1 インターフェイスで ISA 3000 を管理します。

手順

ステップ 1 GigabitEthernet 1/1 を外部ルータに接続し、GigabitEthernet 1/2 を内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。

ステップ 2 GigabitEthernet 1/3 を冗長外部ルータに接続し、GigabitEthernet 1/4 を冗長内部ルータに接続します。

これらのインターフェイスによってハードウェアバイパスペアが形成されます。これらのインターフェイスは、他方のペアで障害が発生した場合に冗長ネットワークパスを提供します。これら 4 つのデータインターフェイスはすべて、選択した同じネットワーク上に存在します。BVI 1 の IP アドレスを、内部ルータおよび外部ルータと同じネットワーク上に配置するように設定する必要があります。

ステップ 3 Management 1/1 を管理コンピュータ（またはネットワーク）に接続します。

ステップ 4 （任意） 管理コンピュータをコンソールポートに接続します。

管理 IP アドレスをデフォルトから変更する必要がある場合は、管理コンピュータをコンソールポートにケーブル接続する必要もあります。「（任意）IP アドレスの変更 （8 ページ）」を参照してください。

デバイスの電源投入

システムの電源は DC 電源で制御されます。電源ボタンはありません。

手順

ステップ 1 電源プラグは DC 電源に配線した後に ISA 3000 に接続します。

電源プラグの正しい配線手順については、『ハードウェア設定ガイド』の「DC 電源への接続」を参照してください。

ステップ 2 ISA 3000 デバイスの前面にあるシステム LED を確認します。緑色に点灯している場合は、デバイスの電源が入っています。緑色に点滅している場合、デバイスはブートアップ フェーズおよび POST（電源投入時自己診断テスト）の状態です。

すべてのデバイスが ISA 3000 に正しく接続されているか確認するには、『ハードウェア設置ガイド』の「接続の確認」を参照してください。

（任意）IP アドレスの変更

ASDM アクセスにデフォルトの IP アドレスを使用できない場合は、ASA CLI で管理インターフェイスの IP アドレスを設定できます。

（注） この手順では、デフォルト設定を復元し、選択した IP アドレスも設定します。このため、保持する ASA 設定に変更を加えた場合は、この手順を使用しないでください。

手順

ステップ 1 ASA コンソールポートに接続し、グローバル コンフィギュレーション モードに入ります。詳細については、「ASA CLI へのアクセス （13 ページ）」を参照してください。

ステップ 2 選択した IP アドレスを使用してデフォルト設定を復元します。

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

例：

```
ciscoasa(config)# configure factory-default 10.1.1.151 255.255.255.0
Based on the management IP address and mask, the DHCP address
pool size is reduced to 103 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
Executing command: interface management1/1
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.1.1.151 255.255.255.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.1.1.0 255.255.255.0 management
Executing command: dhcpd address 10.1.1.152-10.1.1.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

ステップ 3 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

ASDM へのログイン

ASDM を起動して、ASA を設定できるようにします。

始める前に

- ASDM を実行するための要件については、Cisco.com の『ASDM リリース ノート』を参照してください。

手順

ステップ 1 ブラウザに次の URL を入力します。

- **https://192.168.1.1**：管理インターフェイスの IP アドレス。

（注） **http://** や IP アドレス（デフォルトは HTTP）ではなく、必ず **https://** を指定してください。ASA は、HTTP リクエストを HTTPS に自動的に転送しません。

[Cisco ASDM] Web ページが表示されます。ASA に証明書がインストールされていないために、ブラウザのセキュリティ警告が表示されることがありますが、これらの警告は無視して、Web ページにアクセスできます。

ステップ 2 使用可能なオプション [Install ASDM Launcher] または [Run ASDM] のいずれかをクリックします。

ステップ 3 画面の指示に従ってオプションを選択し、ASDM を起動します。

[Cisco ASDM-IDM ランチャー（Cisco ASDM-IDM Launcher）] が表示されます。

ステップ 4 ユーザー名とパスワードのフィールドを空のままにして、[OK] をクリックします。

メイン ASDM ウィンドウが表示されます。

（任意）ASA ライセンスの設定

ISA 3000 には、注文されたバージョンに応じて**基本**ライセンスまたは **Security Plus** ライセンスが含まれます。**Security Plus** ライセンスによって、複数のファイアウォール接続、VPN 接続、フェールオーバー機能と VLAN が提供されます。

ライセンスの使用に制限を付ける場合は、**Strong Encryption**（**3DES/AES**）ライセンスもプリインストールします。このライセンスは、アメリカ合衆国の輸出管理ポリシーによって、一部の国では使用可能できせん。Strong Encryption ライセンスによって、VPN トラフィックなどの高度に暗号化されたトラフィックが許可されます。

この手順では、追加のライセンスを取得してアクティブ化する方法について説明します。新規ライセンスを取得しない場合は、この手順に従う必要がありません。

無料の Strong Encryption ライセンスを手動でリクエストする必要がある場合は、https://www.cisco.com/go/license を参照してください。

必要に応じて、**AnyConnect Plus** または **Apex** ライセンスを購入することができます。このライセンスによって、AnyConnect VPN クライアントの接続が許可されます。

追加の ASA ライセンスをインストールするには、次の手順を実行します。

手順

ステップ 1 **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** を選択して、ASDM で ASA のシリアル番号を取得します。

（注） ライセンスに使用されるシリアル番号は、ハードウェアの外側に印刷されているシャーシのシリアル番号とは異なります。シャーシのシリアル番号は、テクニカルサポートで使用され、ライセンスには使用されません。ライセンスのシリアル番号を表示するには、**show version | grep Serial** コマンドを入力するか、ASDM の [Configuration] > [Device Management] > [Licensing Activation Key] ページを参照してください。

ステップ 2 PID（**L-ASA-SC-5=**）を使用して 5 セキュリティ コンテキスト ライセンスを購入するには、http://www.cisco.com/go/ccw を参照してください。ASA は、PID（**L-ISA3000SEC+-K9=**）を使用して、基本ライセンスと Security Plus ライセンスを持った 2 つのコンテキストをサポートしています。

AnyConnect ライセンスの場合、『Cisco AnyConnect 発注ガイド』および『AnyConnect ライセンスによく寄せられる質問（FAQ）』も参照してください。

ライセンスを購入すると、製品認証キー（PAK）が記載された電子メールを受け取り、ライセンス アクティベーション キーを取得できます。AnyConnect ライセンスの場合、ユーザー セッションの同じプールを使用する複数の ASA に適用できるマルチユース PAK を受け取ります。場合によっては、PAK が記載された電子メールを受け取るまで数日かかることがあります。

ステップ 3 以下のライセンス Web サイトからアクティベーションキーを取得します。 https://www.cisco.com/go/license

プロンプトが表示されたら、次の情報を入力します。

- 製品認証キー
- ASA のシリアル番号
- 電子メール アドレス

アクティベーション キーが自動的に生成され、指定した電子メールアドレスに送信されます。このキーには、永続ライセンス用にそれまでに登録した機能がすべて含まれています。

ステップ 4 ASDM の **[Configuration]** > **[Device Management]** > **[Licensing]** > **[Activation Key]** ペインで、**新しいアクティベーションキー**を入力します。

キーは、5 つの要素で構成される 16 進ストリングで、各要素は 1 つのスペースで区切られています。先頭の 0x 指定子は任意です。すべての値が 16 進数と見なされます。次に例を示します。

```
ASA0xd11b3d48 0xa80a4c0a 0x48e0fd1c 0xb0443480 0x843fc490
```

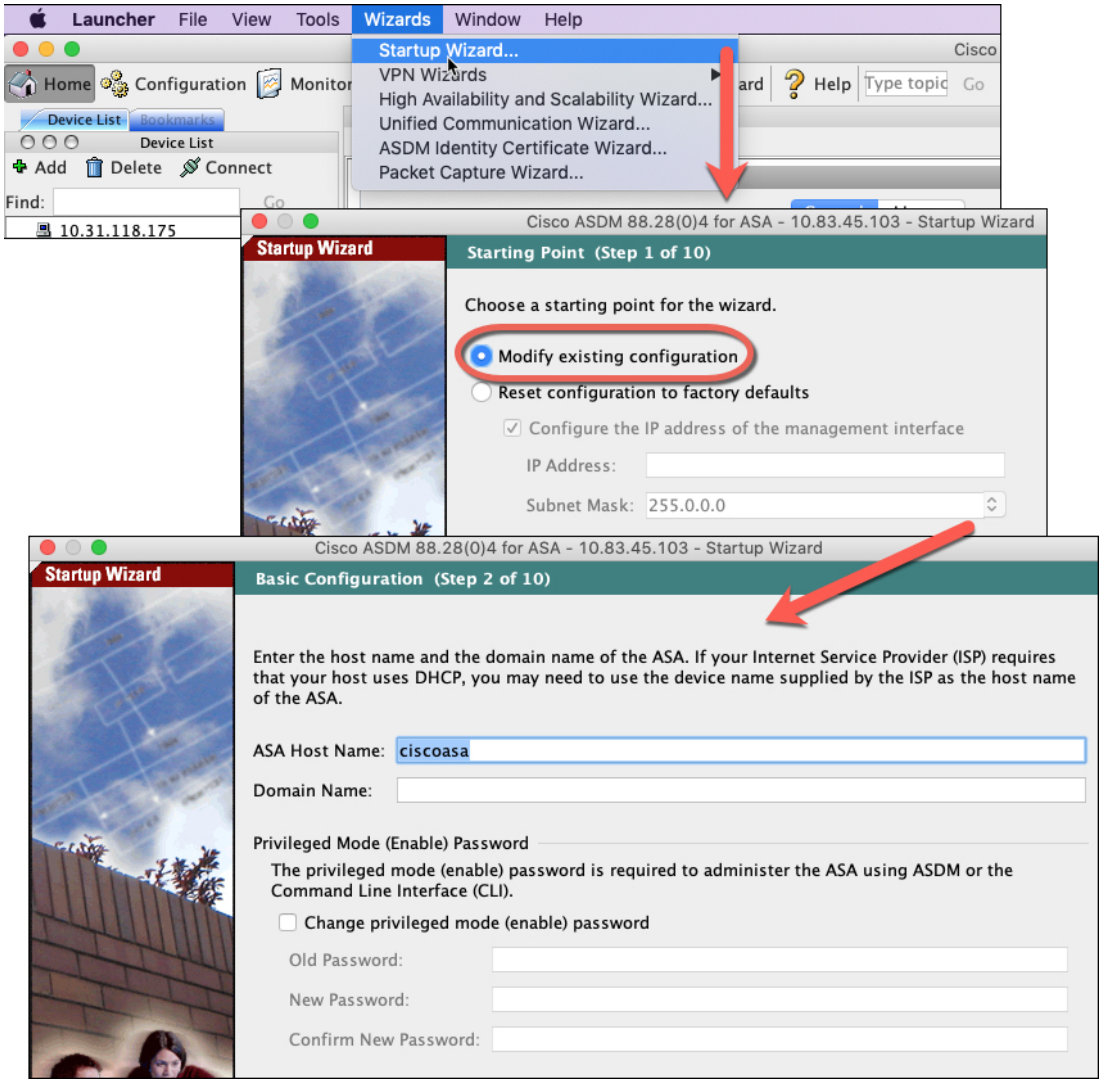
ステップ 5 [Update Activation Key] をクリックします。

ASA の設定

ASDM を使用する際、基本機能および拡張機能の設定にウィザードを使用できます。ウィザードに含まれていない機能を手動で設定することもできます。 ネットワークに合わせて BVI 1 IP アドレスを設定する必要があります。

手順

ステップ 1 [Wizards] > [Startup Wizard] の順に選択し、[Modify existing configuration] オプション ボタンをクリックします。



ステップ 2 [Startup Wizard] では、手順を追って以下を設定できます。

- イネーブル パスワード

- インターフェイス（内部および外部のインターフェイス IP アドレスの設定やインターフェイスの有効化など）
- スタティック ルート
- DHCP サーバー
- その他...

ステップ 3 （任意）[Wizards] メニューから、その他のウィザードを実行します。

ステップ 4 ASA の設定を続行するには、『Navigating the Cisco ASA Series Documentation』でソフトウェアバージョンに応じたマニュアルを参照してください。

ASA CLI へのアクセス

ASA CLI を使用して、ASDM を使用する代わりに ASA のトラブルシューティングや設定を行うことができます。CLI には、コンソール ポートに接続してアクセスできます。後で任意のインターフェイスでの ASA への SSH アクセスを設定できます。SSH アクセスはデフォルトで無効になっています。詳細については、ASA の一般的な操作の設定ガイドを参照してください。

手順

ステップ 1 管理コンピュータをコンソール ポート、RJ-45 ポートまたはミニ USB ポートのいずれかに接続します。ご使用のオペレーティング システムに必要な USB シリアル ドライバを必ずインストールしてください。次のシリアル設定を使用します。

- 9600 ボー
- 8 データ ビット
- パリティなし
- 1 ストップ ビット

ASA CLI に接続します。デフォルトでは、コンソール アクセスに必要なユーザー クレデンシャルはありません。

ステップ 2 特権 EXEC モードにアクセスします。

enable

enable コマンドを最初に入力したときに、パスワードを変更するように求められます。

例：

```
ciscoasa> enable
Password:
The enable password is not set. Please set it now.
```

```
Enter Password: ******
Repeat 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 EXEC 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 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

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**、**quit**、または **end** コマンドを入力します。

次のステップ

- ASA の設定を続行するには、Cisco ASA シリーズの操作マニュアルの中から、お使いのソフトウェアバージョンに応じたマニュアルを参照してください。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。