使用する前に

この章では、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

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、管理アクセスに従って 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。

コンソールポートに接続したときに、読み取れない文字が表示される場合は、ポートの設定を確認してください。設定が正しい場合は、同じ設定を使用して別のデバイスでそのケーブルを試します。ケーブルに問題がない場合は、コンソールポートのハードウェアを交換する必要がある可能性があります。別のワークステーションでの接続を試みることも検討してください。

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

ISA 3000 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、ユーザー EXEC モードで作業していることを示します。ユーザー 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

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 1000および Cisco Secure Firewall 200/1200/3100/4200/6100 コンソールにアクセスする

Firepower 1000および Cisco Secure Firewall 200/1200/3100/4200/6100 コンソールポートを使用して、ASA CLIに接続します。ASA CLI から、トラブルシューティングのために Telnet を使用して FXOS CLI に接続できます。

手順

ステップ 1 管理コンピュータをコンソール ポートに接続します。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#
```

ASA で設定したイネーブルパスワードは、FXOS **管理者**のユーザーパスワードでもあり、ASA の起動に失敗した場合は、FXOS フェールセーフ モードに移行します。

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。

ステップ 4 （任意） FXOS CLI に接続します。

connect fxos [**admin**]

- **admin**：管理者レベルのアクセスを提供します。このオプションを指定しないと、ユーザーのアクセス権は読み取り専用アクセスになります。管理者モードであっても、コンフィギュレーション コマンドは使用できないことに注意してください。

ユーザーはクレデンシャルの入力を求められません。現在の ASA ユーザー名が FXOS に渡されるため、追加のログインは必要ありません。ASA CLI に戻るには、**exit** と入力するか、**Ctrl+Shift+6** を押し、**x** と入力します。

FXOS 内では、**scope security/show audit-logs** コマンドを使用してユーザーアクティビティを表示できます。

例：

```
ciscoasa# connect fxos admin
Connecting to fxos.
Connected to fxos. Escape character sequence is 'CTRL-^X'.
firepower#
firepower# exit
Connection with FXOS terminated.
Type help or '?' for a list of available commands.
ciscoasa#
```

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** | **telnet**}

Telnet 接続を使用する利点は、モジュールに同時に複数のセッションを設定でき、接続速度が速くなることです。

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

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：

```
asa> enable
Password:
The enable password is not set. Please set it now.
Enter Password: ******
Repeat 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 のスーパバイザ レベルに戻ります。

コンソールを終了します。

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**

Telnet セッションを終了します。

a) **Ctrl-], .** と入力

FIPS モードの有効化

連邦情報処理標準（FIPS）は、米国およびカナダ政府の認証規格です。暗号化モジュールで順守する必要がある要件が規定されています。Cisco ASA の特定のバージョンは、米国の国立標準技術研究所（NIST）に従って、FIPS 140-3 に準拠しています。

Cisco ASA で FIPS を有効化することに加え、FIPS に準拠する暗号も構成する必要があります。

クラスタリングに対して FIPS を有効にすることはできません。

始める前に

- FIPS モードは、FIPS 準拠のリリースだけでサポートされます。FIPS に準拠していないバージョンをアップグレードする前に FIPS を無効にする必要があります。

  FIPS に準拠しているリリースに関する情報とそれらの認定を確認するには、https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html?flt0_general-table0=asaを参照してください。

- フェールオーバーでは、両方のユニットが FIPS モードである必要があります。

手順

ステップ 1 Cisco ASA で FIPS を有効にします。

fips enable

例：

```
ciscoasa(config)# fips enable
WARNING: FIPS mode change will not take effect until you save configuration and reboot
the device
```

FIPS が有効な場合、起動時に、FIPS POST が実行され次のコンソールメッセージが出力されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend
Use, duplication, or disclosure by the Government is subject to restrictions as set forth
 in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at
FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and
Computer Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
ciscoasa>
```

ステップ 2 構成を保存してリロードします。

write memory

reload

ステップ 3 （任意） 電源投入時自己診断テスト（POST）を実行します。

fips self-test poweron

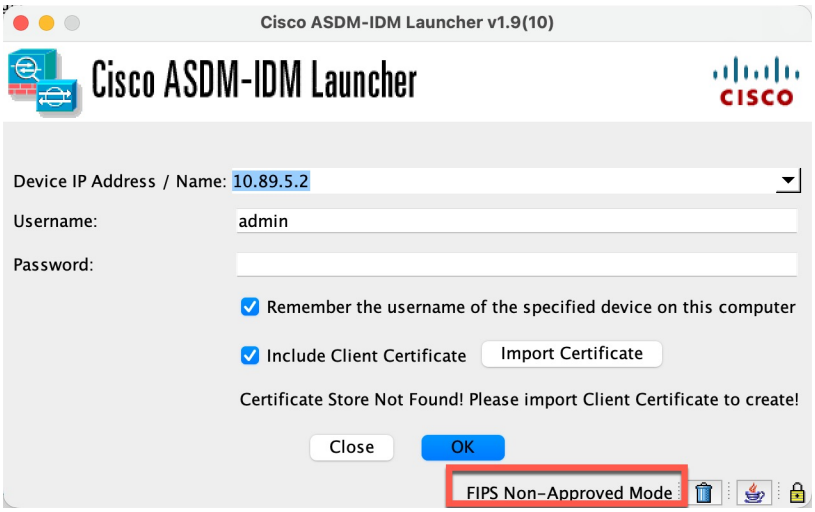
テストには、暗号化アルゴリズムテスト、ソフトウェア完全性テスト、および重要機能のテストがあります。

ステップ 4 ASDM に対して FIPS を有効にします。

- Windows—FIPS.conf ファイルで、**fips_mode** 値を **true** に変更します。FIPS.conf ファイルは、ASDM ランチャーのインストールディレクトリにあります。
- MacOS—FIPS.plist ファイルで、**fipsMode** 値を **true** に変更します。FIPS.plist ファイルは、dm-launcher の Contents フォルダにあります。

FIPS モードは、ログイン画面に次のように表示されます。

図 *1 : FIPS* モード（*FIPS Mode*）



（注）
DNS のリバースルックアップエラーが原因で、FIPS モードで ASDM ランチャーを起動すると 3 分以上かかることがあります。この遅延は、DNS サーバーがリバース DNS ルックアップの有効な PTR レコードを返さない場合に発生します。そのため、ASDM は NetBIOS ネームサービスにフォールバックし、スタートアップ時間に数分かかることがあります。

ASDM アクセスの設定

ここでは、デフォルト設定で 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 アクセスの工場出荷時のデフォルト設定の使用

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 1010、Cisco Secure Firewall 1210/1220：管理 1/1（192.168.45.1）、または内部イーサネット 1/2 ～ 1/8（1010 および 1210）または 1/10（1220）（192.168.1.1）。

管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。

- Firepower 1100、Cisco Secure Firewall 200/1230/1240/1250、3100/4200/6100：内部イーサネット 1/2（192.168.1.1）または管理 1/1（DHCP から）。内部ホストは 192.168.1.0/24 ネットワークに限定されます。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。
- 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 仮想：管理 0/0（展開時に設定）。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 （15 ページ）
マルチ コンテキスト モードの有効化または無効化
ASDM の起動 （11 ページ）

ASDM アクセスのカスタマイズ

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） ASAv 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 サーバー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 （17 ページ）
ファイアウォール モード（シングル モード）の設定
ISA 3000 コンソールへのアクセス （2 ページ）
ASDM の起動 （11 ページ）

ASDM の起動

ASDM Launcher を使用して ASDM を起動します。ランチャは、Cisco 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 Cisco 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。

ASDM では、管理のために別の Cisco ASA IP アドレスを選択できます。

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\<user_id>\.asdm ディレクトリ内にキャッシュ、ログ、設定などのファイルを保存し、Temp ディレクトリ内にもセキュアクライアント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**

（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 要求を HTTPS に自動的に転送しません。

次のボタンを持つ ASDM 起動ページが表示されます。

ASDM Launcher のインストール

ステップ 2 ランチャをダウンロードして、ASDM を起動するには、次の手順を実行します。

a) **[ASDM Launcherのインストール（Install ASDM Launcher）] をクリックします。**

図 *2 : ASDM Launcher* のインストール

b) ユーザー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、ユーザー名および**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。CLIで**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。ASDMにログインしたときには、この動作は適用されません。空白のままにしないように、できるだけ早くイネーブルパスワードを変更することをお勧めします。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。**注**：HTTPS 認証をイネーブルにした場合、ユーザー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（ユーザー名をブランクのままにしないで）ユーザー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 Launcher は自動起動します。
d) 管理IPアドレス、および同じユーザー名とパスワード（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。

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。

ASDM で使用するために Cisco 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。メモリが枯渇していることを確認するには、Java コンソールで「java.lang.OutOfMemoryError」メッセージをモニターします。

さらに、可能であれば、未使用のオブジェクトを削除するなどして、構成サイズを減らすことをお勧めします。

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。

非常に大規模な構成では、最大 2 GB のヒープサイズを指定する必要がある場合があります。

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。

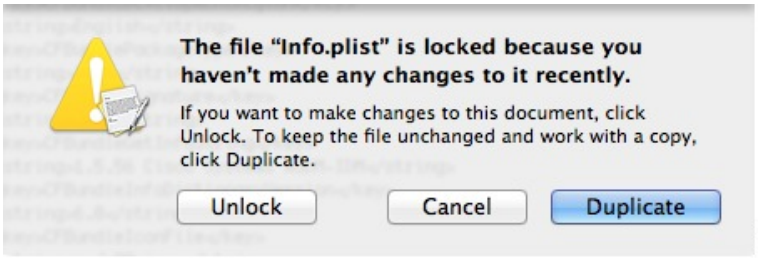
```
    <key>CFBundleIconFile</key>
    <string>asdm32.icns</string>

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


  <key>CFBundleDocumentTypes</key>
    <array>
```

非常に大規模な構成では、最大 2 GB のヒープサイズを指定する必要がある場合があります。

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。

- Firepower 1010：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、管理インターフェイスまたは内部スイッチ ポートから ASDM を使用して管理できます。
- Firepower 200：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、管理インターフェイスまたは内部スイッチ ポートから ASDM を使用して管理できます。
- Firepower 1100：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、管理インターフェイスまた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。

- Cisco Secure Firewall 1210/1220：工場出荷時のデフォルト構成により、機能内部/外部構成が有効になります。ASAは、管理インターフェイスまたは内部スイッチポートからASDMを使用して管理できます。
- Cisco Secure Firewall 1230/1240/1250：工場出荷時のデフォルト構成により、機能内部/外部構成が有効になります。ASAは、管理インターフェイスまた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。
- Secure Firewall 3100：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、Management 1/1インターフェイスまた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。
- Secure Firewall 4200：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、Management 1/1インターフェイスまた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。
- Secure Firewall 6100：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、Management 1/1インターフェイスまた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。
- 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仮想：ハイパーバイザによっては、展開の一環として、展開設定（初期の仮想展開設定）によって管理用のインターフェイスが設定されるため、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。
- 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いて。

アプライアンスの場合、工場出荷時のデフォルト設定は、工場出荷時のデフォルト設定がトランスペアレントモードでのみ使用可能なISA 3000を除き、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 仮想 および Firepower 4100/9300 シャーシ の場合、展開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 仮想 では、この手順を実行することで展開設定が消去され、次の設定が適用されます。

```
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
```

（注） 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、ISA 3000 を除き、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（ISA 3000 では、このコマンドはトランスペアレントモードでのみサポートされます）。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 1010：**管理**インターフェイスの IP アドレスを設定します。
- Firepower 200：**管理**インターフェイスの IP アドレスを設定します。
- Firepower 1100：**内部**インターフェイスの IP アドレスを設定します。
- Cisco Secure Firewall 1210/1220：**管理**インターフェイスの IP アドレスを設定します。
- Cisco Secure Firewall 1230/1240/1250：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 3100：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 4200：**内部**インターフェイスの IP アドレスを設定します。
- Secure Firewall 6100：**内部**インターフェイスの IP アドレスを設定します。
- Firepower 4100/9300：効果はありません。
- ASA 仮想：**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。

http コマンドでは、ユーザー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 IP アドレスよりも大きい使用可能なすべてのアドレスで構成されます。たとえば、サブネットマスク 255.255.255.0 で 10.5.6.78 を指定した場合、DHCP アドレスの範囲は 10.5.6.79 ～ 10.5.6.254 になります。

Firepower 1000、および Cisco Secure Firewall 1200、3100、4200、6100 の場合、このコマンドは、残りの設定とともに **boot system** コマンドが存在する場合は、そのコマンドをクリアします。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

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。

例：

```
docs-bxb-asa3(config)# configure factory-default 10.86.203.151 255.255.254.0
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
WARNING: The new maximum-session limit will take effect after the running-config is saved
 and the system boots next time. Command accepted
WARNING: Local user database is empty and there are still 'aaa' commands for 'LOCAL'.
Executing command: interface management0/0
```

```
Executing command: nameif management
INFO: Security level for "management" set to 0 by default.
Executing command: ip address 10.86.203.151 255.255.254.0
Executing command: security-level 100
Executing command: no shutdown
Executing command: exit
Executing command: http server enable
Executing command: http 10.86.202.0 255.255.254.0 management
Executing command: dhcpd address 10.86.203.152-10.86.203.254 management
Executing command: dhcpd enable management
Executing command: logging asdm informational
Factory-default configuration is completed
ciscoasa(config)#
```

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 1000、およびCisco Secure Firewall 1200、3100、4200/6100 の場合：このコマンドは、残りの設定とともにブートイメージの場所をクリアします（存在する場合）。この設定変更は、ブートアップ時のイメージには影響を与えず、現在ロードされているイメージが引き続き使用されます。

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 仮想 導入設定の復元

この項では、ASA 仮想 の導入（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 仮想 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 仮想 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。

Firepower 1010 のデフォルト設定

Firepower 1010 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェア スイッチ**：イーサネット 1/2 ～ 1/8 は VLAN 1 に属しています。
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）

- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
```

```
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 200 のデフォルト設定

Cisco Secure Firewall 200 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェアスイッチ**：イーサネット 1/2 ー 1/5 は VLAN 1 に属します
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Vlan1
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
interface Ethernet1/1
 no switchport
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet1/2
 switchport
 no security-level
!
interface Ethernet1/3
 switchport
 no security-level
!
interface Ethernet1/4
 switchport
 no security-level
!
interface Ethernet1/5
 switchport
 speed sfp-detect
 no security-level
!
interface Management1/1
 management-only
 nameif management
 security-level 100
 ip address 192.168.45.1 255.255.255.0
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
!
object network obj_any
 nat (any,outside) dynamic interface
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 208.67.222.222 outside
 name-server 208.67.220.220 outside
!
dhcpd auto_config outside
!
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable management
!
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
```

Firepower 1100 のデフォルト設定

Firepower 1100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 1210/1220 のデフォルト設定

Cisco Secure Firewall 1210/1220 の工場出荷時のデフォルト設定は、次のとおりです。

- **ハードウェアスイッチ**：イーサネット 1/2 ～ 1/8（1210）または 1/2 ～ 1/10（1220）は VLAN 1 に属しています
- **内部から外部**へのトラフィック フロー：イーサネット 1/1（外部）、VLAN 1（内部）
- **管理**：管理 1/1（管理）、IP アドレス：192.168.45.1
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- 内部インターフェイスの **DHCP サーバー**、管理インターフェイス
- 外部 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。管理ホストは 192.168.45.0/24 ネットワークに限定され、内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Vlan1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
no shutdown
!
interface Management1/1
managment-only
nameif management
no shutdown
security-level 100
ip address 192.168.45.1 255.255.255.0
!
interface Ethernet1/1
nameif outside
ip address dhcp setroute
no shutdown
!
interface Ethernet1/2
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/3
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/4
no shutdown
switchport
```

```
switchport mode access
switchport access vlan 1
!
interface Ethernet1/5
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/6
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/7
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
interface Ethernet1/8
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/9
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
! 1220
interface Ethernet1/10
no shutdown
switchport
switchport mode access
switchport access vlan 1
!
object network obj_any
   subnet 0.0.0.0 0.0.0.0
   nat (any,outside) dynamic interface
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd address 192.168.45.10-192.168.45.12 management
dhcpd enable inside
dhcpd enable management
!
http server enable
http 192.168.45.0 255.255.255.0 management
http 192.168.1.0 255.255.255.0 inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 1230/1240/1250 のデフォルト設定

Cisco Secure Firewall 1230/1240/1250 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 3100 デフォルト設定

Cisco Secure Firewall 3100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 4200 のデフォルト設定

Cisco Secure Firewall 4200 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Management1/1
  management-only
  nameif management
  security-level 100
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/1
  nameif outside
  security-level 0
  ip address dhcp setroute
  no shutdown
!
interface Ethernet1/2
  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 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
   name-server 208.67.222.222 outside
   name-server 208.67.220.220 outside
!
```

Cisco Secure Firewall 6100 のデフォルト設定

Cisco Secure Firewall 6100 の工場出荷時のデフォルト設定は、次のとおりです。

- **内部から外部へのトラフィック フロー**：Ethernet 1/1（外部）、Ethernet 1/2（内部）
- DHCP の**外部 IP アドレス**、**内部 IP アドレス**：192.168.1.1
- **管理**：Management 1/1（管理）、DHCP からの IP アドレス
- 内部インターフェイスの **DHCP サーバー**
- 外部 DHCP、管理 DHCP からの**デフォルト ルート**
- **ASDM** アクセス：管理ホストと内部ホストに許可されます。内部ホストは 192.168.1.0/24 ネットワークに限定されます。
- **NAT**：内部から外部へのすべてのトラフィック用のインターフェイス PAT。
- **DNS** サーバー：OpenDNS サーバーはあらかじめ構成されています。

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 Management1/1
 speed sfp-detect
 management-only
 nameif management
 security-level 100
 ip address dhcp setroute
!
interface Ethernet1/1
 speed sfp-detect
 nameif outside
 security-level 0
 ip address dhcp setroute
!
interface Ethernet1/2
 speed sfp-detect
 nameif inside
 security-level 100
 ip address 192.168.1.1 255.255.255.0
!
object network obj_any
 subnet 0.0.0.0 0.0.0.0
!
object network obj_any
 nat (any,outside) dynamic interface
!
http server enable
http 0.0.0.0 0.0.0.0 management
http 192.168.1.0 255.255.255.0 inside
!
dhcpd auto_config outside
!
dhcpd address 192.168.1.20-192.168.1.254 inside
dhcpd enable inside
!
dns domain-lookup outside
dns server-group DefaultDNS
 name-server 208.67.220.220
```

```
name-server 208.67.222.222
!
```

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ァルト 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。

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
```

ASA 仮想 による展開の設定

ASA 仮想 を導入すると、ASDM を使用して、Management 0/0 インターフェイスへの接続を可能にする多数のパラメータをプリセットできます。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 サーバーの有効または無効
- 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 サーバー
- 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Essentials機能階層
- Smart Transport URL（https://smartreceiver.cisco.com/licservice/license）およびポート 80。
- （オプション）Smart Transport 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 ユーザー名とパスワード
- 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 Licensing Authority に ASA 仮想 を正常に登録するには、ASA 仮想 にインターネットアクセスが必要です。インターネットに接続してライセンス登録を完了させるには、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 managemment_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
```

（注） Essentials ライセンスは、以前は「標準」ライセンスと呼ばれていました。

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 managemment_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 を設定してモニターするには、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 （13 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 をモニターするには、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、ユーザー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：複数の管理ユーザーが 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。複数のユーザーが同時に 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。既存の接続では、その接続が確立された時点で設定されていたポリシーの使用が続行されます。古い接続に対する **show** コマンドの

出力は古いコンフィギュレーションを反映しており、場合によっては古い接続に関するデータが含まれないことがあります。

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、次のコマンドを入力します。

- **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。

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。

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。