ソフトウェアおよびコンフィギュレーション

この章では、ASA ソフトウェアおよびコンフィギュレーションの管理方法について説明します。

ソフトウェアのアップグレード

完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON を使用したイメージのロード（ISA 3000）

TFTP を使用して ROMMON モードから ASA へソフトウェア イメージをロードするには、次の手順を実行します。

手順

ステップ 1 ISA 3000 コンソールへのアクセスに従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMONモードに入るようにプロンプト表示されたら、**Escape**キーを押します。

ステップ 4 ROMMON モードで、IP アドレス、TFTP サーバ アドレス、ゲートウェイ アドレス、ソフトウェア イメージ ファイル、およびポートを含む、ASA に対するインターフェイス設定を次のように定義します。

```
rommon #1> interface gigabitethernet0/0
rommon #2> address 10.86.118.4
rommon #3> server 10.86.118.21
rommon #4> gateway 10.86.118.21
rommon #5> file asa961-smp-k8.bin
```

（注）
ネットワークへの接続がすでに存在することを確認してください。

インターフェイス コマンドは ASA 5506-X、ASA 5508-X、ASA 5516-X、および ISA 3000 プラットフォームで無視されるため、これらのプラットフォームでManagement 1/1 インターフェイスから TFTP リカバリを実行する必要があります。

ステップ 5 設定を検証します。

```
rommon #6> set
ROMMON Variable Settings:
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20
```

ステップ 6 TFTP サーバーに ping を送信します。

```
rommon #7> ping server
Sending 20, 100-byte ICMP Echoes to server 10.86.118.21, timeout is 4 seconds:

Success rate is 100 percent (20/20)
```

ステップ 7 ネットワーク設定を、後で使用できるように保管しておきます。

```
rommon #8> sync
Updating NVRAM Parameters...
```

ステップ 8 システム ソフトウェア イメージをロードします。

```
rommon #9> tftpdnld
ROMMON Variable Settings:
```

```
  ADDRESS=10.86.118.3
  SERVER=10.86.118.21
  GATEWAY=10.86.118.21
  PORT=GigabitEthernet0/0
  VLAN=untagged
  IMAGE=asa961-smp-k8.bin
  CONFIG=
  LINKTIMEOUT=20
  PKTTIMEOUT=4
  RETRY=20

tftp asa961-smp-k8.bin@10.86.118.21 via 10.86.118.21

Received 14450688 bytes

Launching TFTP Image...
Cisco ASA Security Appliance admin loader (3.0) #0: Mon Mar 5 16:00:07 MST 2016

Loading...
```

ソフトウェア イメージが正常にロードされると、ASA は自動的に ROMMON モードを終了します。

ステップ 9 ROMMON モードから ASA を起動する場合、システム イメージはリロード間で保持されないため、やはりイメージをフラッシュ メモリにダウンロードする必要があります。完全なアップグレードの手順については、『Cisco ASA Upgrade Guide』を参照してください。

ROMMON イメージのアップグレード（ISA 3000）

ISA 3000 の ROMMON イメージをアップグレードするには、次の手順に従います。 ASA モデルの場合、システムの ROMMON バージョンは 1.1.8 以上である必要があります。最新バージョンへのアップグレードを推奨します。

新バージョンへのアップグレードのみ可能です。ダウングレードはできません。

⚠

注意 ISA 3000 の ROMMON 1.0.5 へのアップグレードには、以前の ROMMON バージョンの 2 倍の時間がかかります（約 15 分）。アップグレード中はデバイスの電源を**再投入しないでください**。アップグレードが 30 分以内に完了しないか、または失敗した場合は、シスコ テクニカル サポートに連絡してください。デバイスの電源を再投入したり、リセットしたり**しないでください**。

始める前に

Cisco.com から新しい ROMMON イメージを取得して、サーバー上に置いて ASA にコピーします。ASA は、FTP サーバー、TFTP サーバー、SCP サーバー、HTTP（S）サーバー、および SMB サーバーをサポートしています。次の URL からイメージをダウンロードします。

- ISA 3000： https://software.cisco.com/download/home/286288493/type

手順

ステップ 1 ROMMON イメージを ASA フラッシュ メモリにコピーします。この手順では、FTP コピーを表示します。他のサーバータイプのシンタックスの場合は **copy ?** と入力します。

copy ftp://[*username***:***password***@**]*server_ip***/asa5500-firmware-***xxxx***.SPA disk0:asa5500-firmware-***xxxx***.SPA**

ステップ 2 現在のバージョンを確認するには、**show module** コマンドを入力して、MAC アドレス範囲テーブルの Mod 1 の出力で Fw バージョンを調べます。

```
ciscoasa# show module
[...]
Mod  MAC Address Range                 Hw Version   Fw Version   Sw Version
---- --------------------------------- ------------ ------------ ---------------
   1 7426.aceb.ccea to 7426.aceb.ccf2  0.3          1.1.5        9.4(1)
 sfr 7426.aceb.cce9 to 7426.aceb.cce9  N/A          N/A
```

ステップ 3 ROMMON イメージをアップグレードします。

upgrade rommon disk0:asa5500-firmware-*xxxx***.SPA**

例：

```
ciscoasa# upgrade rommon disk0:asa5500-firmware-1108.SPA
Verifying file integrity of disk0:/asa5500-firmware-1108.SPA

Computed Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af

Embedded Hash   SHA2: d824bdeecee1308fc64427367fa559e9
                      eefe8f182491652ee4c05e6e751f7a4f
                      5cdea28540cf60acde3ab9b65ff55a9f
                      4e0cfb84b9e2317a856580576612f4af


Digital signature successfully validated
File Name                     : disk0:/asa5500-firmware-1108.SPA
Image type                    : Release
    Signer Information
        Common Name           : abraxas
        Organization Unit     : NCS_Kenton_ASA
        Organization Name     : CiscoSystems
    Certificate Serial Number : 553156F4
    Hash Algorithm            : SHA2 512
    Signature Algorithm       : 2048-bit RSA
    Key Version               : A
Verification successful.
Proceed with reload? [confirm]
```

ステップ 4 プロンプトが表示されたら、確認して ASA をリロードします。

ASAがROMMONイメージをアップグレードして、その後オペレーティングシステムをリロードします。

ソフトウェアのダウングレード

多くの場合、ASAソフトウェアをダウングレードし、以前のソフトウェアバージョンからバックアップ設定を復元することができます。ダウングレードの方法は、ASAプラットフォームによって異なります。

ダウングレードに関するガイドラインおよび制限事項

ダウングレードする前に、次のガイドラインを参照してください。

- **クラスタリング用の公式のゼロ ダウンタイム ダウングレードのサポートはありません**：ただし場合によっては、ゼロ ダウンタイム ダウングレードが機能します。ダウングレードに関する次の既知の問題を参照してください。この他の問題が原因でクラスタユニットのリロードが必要になることもあり、その場合はダウンタイムが発生します。
  - **クラスタリングを含む9.9(1)より前のリリースへのダウングレード**：9.9(1)以降では、バックアップの配布が改善されています。クラスタに3つ以上のユニットがある場合は、次の手順を実行する必要があります。
    1. クラスタからすべてのセカンダリユニットを削除します（クラスタはプライマリユニットのみで構成されます）。
    2. 1つのセカンダリ ユニットをダウングレードし、クラスタに再参加させます。
    3. プライマリユニットでクラスタリングを無効にします。そのユニットをダウングレードし、クラスタに再参加させます。
    4. 残りのセカンダリ ユニットをダウングレードし、それらを一度に1つずつクラスタに再参加させます。
  - **クラスタサイトの冗長性を有効にする場合は、9.9(1)より前のリリースにダウングレードします**：ダウングレードする場合（または9.9(1)より前のユニットをクラスタに追加する場合）は、サイトの冗長性を無効にする必要があります。そうしないと、古いバージョンを実行しているユニットにダミーの転送フローなどの副作用が発生します。
  - **クラスタリングおよび暗号マップを使用する場合に9.8(1)からダウングレードする**：暗号マップが設定されている場合に9.8(1)からダウングレードすると、ゼロ ダウンタイム ダウングレードはサポートされません。ダウングレード前に暗号マップ設定をクリアし、ダウングレード後に設定をもう一度適用する必要があります。
  - **クラスタリングユニットのヘルスチェックを0.3 ～ 0.7秒に設定した状態で9.8(1)からダウングレードする**：（**health-check holdtime** で）ホールド時間を0.3 ～ 0.7秒に設

定した後で ASA ソフトウェアをダウングレードすると、新しい設定はサポートされないため、設定値はデフォルトの 3 秒に戻ります。

- **クラスタリング（CSCuv82933）を使用している場合に 9.5(2) 以降から 9.5(1) 以前にダウングレードする**：9.5(2) からダウングレードする場合、ゼロ ダウンタイム ダウングレードはサポートされません。ユニットがオンラインに戻ったときに新しいクラスタが形成されるように、すべてのユニットをほぼ同時にリロードする必要があります。ユニットが順番にリロードされるのを待つと、クラスタを形成できなくなります。
- **クラスタリングを使用する場合に 9.2(1) 以降から 9.1 以前にダウングレードする**：ゼロ ダウンタイム ダウングレードはサポートされません。

- **ASA 仮想 の場合、9.24 以降のバージョンから 9.24 より前のバージョンにダウングレードすることはできません**。9.24 以降にアップグレードした後、9.24 より前のバージョンにダウングレードすることはできません。
- **9.22 以降からのダウングレードの問題**：usb-port disable コマンドを使用して USB ポートを無効にした後、以前のリリースにダウングレードすると、ポートは無効のままになり、再度有効にするには NVRAM（FXOS local-mgmt **erase secure all** コマンド）を消去する必要があります。
- **9.18 以降からのダウングレードの問題**：9.18 では動作が変更され、**access-group** コマンドがその **access-list** コマンドの前にリストされます。ダウングレードすると、**access-group** コマンドはまだ **access-list** コマンドをロードしていないため拒否されます。以前に **forward-reference enable** コマンドを有効にしていた場合でも、このコマンドは現在削除されているため同じ結果となります。ダウングレードする前にすべての **access-group** コマンドを手動でコピーし、ダウングレード後に再入力してください。
- **スマートライセンスの 9.10(1) からのダウングレード**：スマートエージェントの変更により、ダウングレードする場合、デバイスを Cisco Smart Software Manager に再登録する必要があります。新しいスマートエージェントは暗号化されたファイルを使用するので、古いスマートエージェントが必要とする暗号化されていないファイルを使用するために再登録する必要があります。
- **PBKDF2（パスワードベースのキー派生関数 2）ハッシュをパスワードで使用する場合に 9.5 以前のバージョンにダウングレードする**：9.6 より前のバージョンは PBKDF2 ハッシュをサポートしていません。9.6(1) では、32 文字より長い **enable** パスワードおよび **username** パスワードで PBKDF2 ハッシュを使用します。9.7(1) では、すべての新しいパスワードは、長さに関わらず PBKDF2 ハッシュを使用します（既存のパスワードは引き続き MD5 ハッシュを使用します）。ダウングレードすると、**enable** パスワードがデフォルト（空白）に戻ります。ユーザー名は正しく解析されず、**username** コマンドが削除されます。ローカルユーザーをもう一度作成する必要があります。
- **ASA 仮想 用のバージョン 9.5(2.200) からのダウングレード**：ASA 仮想 はライセンス登録状態を保持しません。**license smart register idtoken id_token force** コマンドで再登録する必要があります（ASDM の場合、[Configuration] > [Device Management] > [Licensing] > [Smart

Licensing] ページで [Force registration] オプションを使用）。Smart Software Manager から ID トークンを取得します。

- **元のトンネルがネゴシエートした暗号スイートをサポートしないソフトウェアバージョンをスタンバイ装置が実行している場合でも、VPN トンネルがスタンバイ装置に複製されます**：このシナリオは、ダウングレード時に発生します。その場合、VPN接続を切断して再接続してください。
- **バージョン 9.20(4) からそれ以前のバージョンへ、永続ライセンス予約が設定された ASA 仮想 をダウングレード**：永続ライセンス予約が登録解除されないようにするため、次の手順を実行することを推奨します。

  1. 永続ライセンス予約を登録解除します。
  2. ASA 仮想 をダウングレードします。
  3. 永続ライセンス予約を再度登録します。

  バージョン 9.20.4 以降では Smart Transport がデフォルトになりますが、バージョン 9.20.3 以前では Smart Call Home がデフォルトとなるため、これらの手順を実行する必要があります。

- **バージョン 9.23(1) から以前のバージョンへの柔軟な永続ライセンス予約を備えた ASA 仮想 のダウングレード**：バージョン 9.23(1) および柔軟な永続ライセンス予約で ASA 仮想 をダウングレードしないことを推奨します。ライセンス登録状態は **[Unregistered]** になります。

ダウングレード後に削除される互換性のない設定

以前のバージョンにダウングレードすると、それ以降のバージョンで導入されたコマンドは設定から削除されます。ダウングレードする前に、ターゲットバージョンに対して設定を自動的にチェックする方法はありません。新しいコマンドが ASA の新しい機能にいつ追加されたかをリリースごとに表示できます。

show startup-config errors コマンドを使用してダウングレードした後、拒否されたコマンドを表示できます。ラボデバイスでダウングレードを実行できる場合は、実稼働デバイスでダウングレードを実行する前にこのコマンドを使用して効果を事前に確認できます。

場合によっては、ASAはアップグレード時にコマンドを新しいフォームに自動的に移行するため、バージョンによっては新しいコマンドを手動で設定しなかった場合でも、設定の移行によってダウングレードが影響を受けることがあります。ダウングレード時に使用できる古い設定のバックアップを保持することを推奨します。8.3 へのアップグレード時には、バックアップが自動的に作成されます（<old_version>_startup_cfg.sav）。他の移行ではバックアップが作成されません。ダウングレードに影響する可能性がある自動コマンド移行の詳細については、『ASAアップグレードガイド』の「バージョン固有のガイドラインと移行」を参照してください。

ダウングレードに関するガイドラインおよび制限事項 （5 ページ）の既知のダウングレードの問題も参照してください。

たとえば、バージョン9.8(2) を実行している ASA には、次のコマンドが含まれています。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0
username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz privilege 15
snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
```

9.0(4) にダウングレードすると、起動時に次のエラーが表示されます。

```
access-list acl1 extended permit sctp 192.0.2.0 255.255.255.0 198.51.100.0 255.255.255.0

                                    ^
ERROR: % Invalid input detected at '^' marker.

username test1 password $sha512$1234$abcdefghijklmnopqrstuvwxyz pbkdf2 privilege 15
                                                                 ^
ERROR: % Invalid input detected at '^' marker.

snmp-server user snmpuser1 snmpgroup1 v3 engineID abcdefghijklmnopqrstuvwxyz encrypted
auth md5 12:ab:34 priv aes 128 12:ab:34
                                          ^
ERROR: % Invalid input detected at '^' marker.
```

この例では、**access-list extended** コマンドでの **sctp** のサポートがバージョン 9.5(2) で、**username** コマンドでの **pbkdf2** のサポートがバージョン 9.6(1) で、**snmp-server user** コマンドでの **engineID** のサポートがバージョン9.5(3) で追加されました。

Cisco ASA アプライアンスのダウングレード

ASA のバージョンを古いバージョンに設定し、バックアップ設定をスタートアップ コンフィギュレーションに復元してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。この手順は、次のモデルに適用されます。

- Firewall 200
- Firepower 1000
- Cisco Secure Firewall 1200
- Firepower 2100
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Firewall 6100

始める前に

この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。

手順

ステップ 1 スタンドアロン、フェールオーバー、またはクラスタリング展開のために、『ASA Upgrade Guide』のアップグレード手順を使用して、ASA ソフトウェアの古いバージョンをロードします。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。**重要**：まだ ASAをリロードしないでください。

ステップ 2 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーの場合は、アクティブユニットでこの手順を実行します。この手順では、コマンドをスタンバイ装置に複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.13.1_cfg.sav startup-config
```

ステップ 3 ASA をリロードします。

ASA CLI

reload

ASDM

[Tools] > **[System Reload]** を選択します。

Firepower 4100/9300 のダウングレード

バックアップ設定をスタートアップ コンフィギュレーションに復元し、ASA のバージョンを古いバージョンに設定してからリロードすることによって、ASA ソフトウェアのバージョンをダウングレードすることができます。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。古い設定を復元しない場合は、新規または変更された機能を表す互換性のないコマンドが存在する可能性があります。新しいコマンドは、ソフトウェアの古いバージョンをロードすると拒否されます。
- ASA の古いバージョンが、FXOS の現在のバージョンと互換性があることを確認します。互換性がない場合は、古い ASA 設定を復元する前に最初の手順として FXOS をダウングレードします。ダウングレードされた FXOS も、（ダウングレードする前に）ASA の現

在のバージョンと互換性があることを確認してください。互換性を実現できない場合は、ダウングレードを実行しないことをお勧めします。

手順

ステップ 1 ASA CLI で、バックアップの ASA 設定をスタートアップ コンフィギュレーションにコピーします。フェールオーバーまたはクラスタリングの場合は、アクティブ/制御ユニットでこの手順を実行します。この手順では、コマンドをスタンバイ/データユニットに複製します。

copy *old_config_url* **startup-config**

write memory を使用して実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存しないことが重要です。このコマンドは、バックアップ設定を上書きします。

例：

```
ciscoasa# copy disk0:/9.8.4_cfg.sav startup-config
```

ステップ 2 FXOS では、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Firewall Chassis Manager または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って ASA ソフトウェアの古いバージョンを使います。この場合は、ASA の新しいバージョンではなく、古いバージョンを指定します。

ステップ 3 また、FXOS をダウングレードする場合は、スタンドアロン、フェールオーバー、あるいはクラスタリング展開のために、Firewall Chassis Manager または FXOS CLI を使用し、『ASA Upgrade Guide』のアップグレード手順に従って FXOS ソフトウェアの古いバージョンを最新のバージョンに設定します。

ISA 3000 のダウングレード

ダウングレードでは、ISA 3000 モデルで以下の機能を完了するためのショートカットが存在します。

- ブート イメージ コンフィギュレーションのクリア（**clear configure boot**）。
- 古いイメージへのブート イメージの設定（**boot system**）。
- （オプション）新たなアクティベーション キーの入力（**activation-key**）。
- 実行コンフィギュレーションのスタートアップへの保存（**write memory**）。これにより、BOOT 環境変数を古いイメージに設定します。このため、リロードすると古いイメージがロードされます。
- 古いコンフィギュレーションのバックアップをスタートアップ コンフィギュレーションにコピーします（**copy** *old_config_ur* **startup-config**）。
- リロード（**reload**）。

始める前に

- この手順ではアップグレードする前に ASA のバックアップ設定を行う必要があるため、古い設定を復元することができます。

手順

ソフトウェアをダウングレードし、古いコンフィギュレーションを復元します。

downgrade [**/noconfirm**] *old_image_url old_config_url* [**activation-key** *old_key*]

例：

```
ciscoasa(config)# downgrade /noconfirm disk0:/asa821-k8.bin disk0:/8_2_1_0_startup_cfg.sav
```

/noconfirm オプションを指定すると、プロンプトが表示されずにダウングレードされます。*image_url* は、disk0、disk1、tftp、ftp、または smb 上の古いイメージへのパスです。*old_config_url* は、保存された移行前の設定へのパスです。8.3 よりも前のアクティベーション キーに戻る必要がある場合は、そのアクティベーション キーを入力できます。

ファイルの管理

フラッシュ メモリ内のファイルの表示

フラッシュ メモリ内のファイルを表示して、そのファイルに関する情報を参照できます。

手順

ステップ 1 フラッシュ メモリ内のファイルを表示します。

dir [**disk***n***:**]

disk0: は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。

例：

```
hostname# dir

Directory of disk0:/
500    -rw-  4958208     22:56:20 Nov 29 2004  cdisk.bin
2513   -rw-  4634        19:32:48 Sep 17 2004  first-backup
```

```
2788   -rw-  21601       20:51:46 Nov 23 2004  backup.cfg
2927   -rw-  8670632     20:42:48 Dec 08 2004  asdmfile.bin
```

ステップ 2 特定のファイルに関する追加情報を表示します。

show file information [path:/]*filename*

例：

```
hostname# show file information cdisk.bin

disk0:/cdisk.bin:
  type is image (XXX) []
  file size is 4976640 bytes version 7.0(1)
```

示されているファイル サイズは例にすぎません。

デフォルト パスは、内部フラッシュ メモリのルート ディレクトリ（disk0:/）です。

フラッシュ メモリからのファイルの削除

不要になったファイルはフラッシュ メモリから削除できます。

手順

フラッシュ メモリからファイルを削除します。

delete disk*n***:** *filename*

disk0: は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。

パスを指定しないと、デフォルトにより、ファイルは現在の作業ディレクトリから削除されます。ファイルを削除するときは、ワイルドカードを使用できます。削除するファイル名を求めるプロンプトが表示されます。その後、削除を確認する必要があります。

フラッシュ ファイル システムの削除

フラッシュ ファイル システムを消去するには、次の手順を実行します。

手順

ステップ 1 ISA 3000 コンソールへのアクセスの手順に従って、ASA のコンソール ポートに接続します。

ステップ 2 ASA の電源を切ってから、再び電源をオンにします。

ステップ 3 スタートアップの間に、ROMMON モードに入るようにプロンプト表示されたら、**Escape** キーを押します。

ステップ 4 **erase** コマンドを入力します。これにより、すべてのファイルが上書きされてファイル システムが消去されます（非表示のシステム ファイルを含む）。

rommon #1> **erase** [**disk0:** | **disk***n***:** | **usb:**]

disk0: は内部メモリです。その他のドライブ番号は外部ストレージを表します。新しいモデルでは、外部 USB ドライブに **usb:** を使用しています。

ファイル アクセスの設定

ASA では、FTP クライアント、セキュア コピー クライアント、または TFTP クライアントを使用できます。また、ASA をセキュア コピー サーバーとして設定することもできるため、コンピュータでセキュア コピー クライアントを使用できます。

FTP クライアント モードの設定

ASA では、FTP サーバーとの間で、イメージ ファイルやコンフィギュレーション ファイルのアップロードおよびダウンロードを実行できます。パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバーは、今回の特定の接続においてリッスンするポート番号を応答として返します。

手順

FTP モードをパッシブに設定します。

ftp mode passive

例：

```
ciscoasa(config)# ftp mode passive
```

ASA セキュアコピークライアントの設定

ASA が SCP クライアントとして動作する場合は、**copy** コマンドを使用して SCP を設定できます。

SCP のパフォーマンスは、使用する暗号化アルゴリズムにある程度依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマン

スが低下します。提示された暗号方式を変更するには、**ssh cipher encryption** コマンド。たとえば、**ssh cipher encryption custom aes128-cbc**

始める前に

- SSH バージョン 2 接続をサポートするには、ASA のライセンスに強力な暗号化（3DES/AES）ライセンスが必要です。
- 特に指定されていないかぎり、マルチ コンテキスト モードでは、システム実行スペースで次の手順を実行します。コンテキストからシステム実行スペースに切り替えるには、**changeto system** コマンドを入力します。
- SCP サーバーの場合は、「SSH アクセスの設定」に従って Cisco ASA で SSH を有効にします。

手順

ステップ 1 （オプション）ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、手動でキーを管理できます。

ssh pubkey-chain [**no**] **server** *ip_address* {**key-string** *key_string* **exit**| **key-hash** {**md5** | **sha256**} *fingerprint*}

例：

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
ciscoasa(config-ssh-pubkey-server)# show running-config ssh pubkey-chain
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256 f1:22:49:47:b6:76:74:b2:db:26:fb:13:65:d8:99:19:
e7:9e:24:46:59:be:13:7f:25:27:70:9b:0e:d2:86:12
```

各サーバーについて、SSH ホストの **key-string**（公開キー） または **key-hash**（ハッシュ値）を指定できます。

key_string はリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

key-hash {**md5** | **sha256**} *fingerprint* では、たとえば、**show** コマンドの出力からコピーしたキーなどの、すでにハッシュされているキー（MD5 または SHA-256 キーを使用）が入力されます。

ステップ 2 （任意） SSH ホスト キー チェックを有効または無効にします。マルチ コンテキスト モードでは、管理コンテキストでこのコマンドを入力します。

[**no**] **ssh stricthostkeycheck**

例：

```
ciscoasa# ssh stricthostkeycheck
ciscoasa# copy x scp://cisco@10.86.95.9/x
The authenticity of host '10.86.95.9 (10.86.95.9)' can't be established.
RSA key fingerprint is dc:2e:b3:e4:e1:b7:21:eb:24:e9:37:81:cf:bb:c3:2a.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.86.95.9' (RSA) to the list of known hosts.
Source filename [x]?

Address or name of remote host [10.86.95.9]?

Destination username [cisco]?

Destination password []? cisco123

Destination filename [x]?
```

デフォルトで、このオプションは有効になっています。このオプションがイネーブルになっている場合、ASA にまだ格納されていないホストキーを許可または拒否するように求められます。このオプションがディセーブルになっている場合、ASA は過去に保存されたことがないホストキーを自動的に許可します。

例

次に、10.86.94.170 にあるサーバーのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256 65:d9:9d:fe:1a:bc:61:aa:
64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

次に、10.7.8.9 にあるサーバーのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:
46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

ASA TFTP クライアントのパス設定

TFTP は、単純なクライアント/サーバー ファイル転送プロトコルで、RFC 783 および RFC 1350 Rev. 2 で規定されています。TFTP サーバーとの間でファイルをコピーできるように、ASA を TFTP クライアントとして設定できます。これにより、コンフィギュレーション ファイルをバックアップし、それらを複数の ASA にプロパゲートできます。

ここでは、TFTP サーバーへのパスを事前定義できるため、**copy** および **configure net** などのコマンドで入力する必要がなくなります。

手順

configure net および **copy** コマンドで使用するために、TFTP サーバーのアドレスおよびファイル名を事前定義します。

tftp-server *interface_name server_ip filename*

例：

```
ciscoasa(config)# tftp-server inside 10.1.4.7 files/config1.cfg
ciscoasa(config)# copy tftp: test.cfg

Address or name of remote host [10.1.4.7]?

Source filename [files/config1.cfg]?config2.cfg

Destination filename [test.cfg]?

Accessing tftp://10.1.4.7/files/config2.cfg;int=outside...
```

コマンドを入力するとファイル名を上書きできます。たとえば、**copy** コマンドを使用するときに事前定義された TFTP サーバーのアドレスを利用できますが、インタラクティブプロンプトでファイル名を入力することもできます。

copy コマンドに、**tftp://***url* ではなく **tftp:** を入力して tftp-server の値を使用します。

ASA へのファイルのコピー

このセクションでは、アプリケーションイメージ、ASDM ソフトウェア、構成ファイル、その他内部または外部のフラッシュメモリにダウンロードする必要があるファイルを TFTP、FTP、SMB、HTTP、HTTPS、SCP サーバー、または USB ドライブなどのデバイスからコピーする方法について説明します。

ガイドライン

- **disk0:** は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。
- USB ドライブが EXT2/3/4 または VFAT/FAT32 としてフォーマットされていることを確認します。
- 文字の大文字と小文字が異なっていても、同じ名前の 2 つのファイルをフラッシュ メモリの同じディレクトリに保存できません。たとえば、config.cfg というファイルが存在する場所に Config.cfg というファイルをダウンロードしようとすると、次のエラー メッセージが表示されます。

```
%Error opening disk0:/Config.cfg (File exists)
```

- マルチコンテキストモードの場合は、プライベートストレージ（**storage-url private**）を構成しない限りシステム実行スペース内にいる必要があります。コンテキスト内では、実行コンフィギュレーションまたはスタートアップコンフィギュレーション（プライベートストレージがある場合は「スタートアップ コンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー （19 ページ）」および「コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ （36 ページ）」を参照）、またはキャプチャをコピーすることもできます。SCP は、コンテキスト内ではサポートされません。

始める前に

- Cisco ASA **copy** コマンドを使用して SCP サーバーとの間でファイルをコピーするには、次の手順を実行する必要があります。
  - **ssh** コマンドを使用して、Cisco ASA で SCP サーバーサブネット/ホストの SSH アクセスを有効にします。
  - **crypto key generate** コマンドを使用してキーペアを生成します（物理 Cisco ASA の場合のみ）。

手順

次のサーバー タイプの 1 つを使用してファイルをコピーします。

- TFTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy tftp://10.1.1.67/files/context1.cfg disk0:/context1.cfg

Address or name of remote host [10.1.1.67]?

Source filename [files/context1.cfg]?

Destination filename [context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- FTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/context1.cfg
disk0:/contexts/context1.cfg

Address or name of remote host [10.1.1.67]?

Source username [jcrichton]?

Source password [aeryn]?

Source filename [files/context1.cfg]?

Destination filename [contexts/context1.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- HTTP（S） サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[**:***port*][*/path*]*/src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy https://asun:john@10.1.1.67/files/moya.cfg disk0:/contexts/moya.cfg

Address or name of remote host [10.1.1.67]?

Source username [asun]?

Source password [john]?

Source filename [files/moya.cfg]?

Destination filename [contexts/moya.cfg]?
Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SMB サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **smb:**//[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename* **disk***n***:/**[*path*/]*dest_filename*

  例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

- SCP サーバーからコピーします。

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

copy [**/noconfirm**] [*interface_name*]
scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] **disk***n***:**/[*path/*]*dest_filename*

例：

```
ciscoasa# copy scp://pilot@10.86.94.170/test.cfg disk0:/test.cfg

Address or name of remote host [10.86.94.170]?

Source username [pilot]?

Destination filename [test.cfg]?

The authenticity of host '10.86.94.170 (10.86.94.170)' can't be established.
RSA key fingerprint is
<65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19>(SHA256).
Are you sure you want to continue connecting (yes/no)? yes

Please use the following commands to add the hash key to the configuration:
  ssh pubkey-chain
    server 10.86.94.170
      key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19


Password: <type in password>
!!!!!!
6006 bytes copied in 8.160 secs (750 bytes/sec)
```

- USB または内蔵または外付けドライブからコピーします。

  copy [**/noconfirm**] **disk***n***:**/[*path*]*/src_filename* **disk***n***:**/[*path*/]*dest_filename*

  例：

```
ciscoasa# copy /noconfirm disk1:/test.xml disk0:/test.xml

Cryptochecksum: db8ba196 9ad189a8 7f5f501f 1bec469b
!!!!!!!!!!!
11143 bytes copied in 5.710 secs (2228 bytes/sec)
```

スタートアップコンフィギュレーションまたは実行コンフィギュレーションへのファイルのコピー

テキスト ファイルは、TFTP、FTP、SMB、HTTP（S）、または SCP サーバーから、またはフラッシュ メモリから、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションにダウンロードできます。

コンフィギュレーションを実行コンフィギュレーションにコピーするには、2つのコンフィギュレーションをマージします。マージによって、新しいコンフィギュレーションから実行コンフィギュレーションに新しいコマンドが追加されます。コンフィギュレーションが同じ場合、変更は発生しません。コマンドが競合する場合、またはコマンドが Cisco ASA の実行に影響を

与える場合、マージの結果はコマンドによって異なります。エラーが発生することも、予期できない結果が生じることもあります。

（オプション）ASAがサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

マルチコンテキストモードのコンテキスト内で、プライベートストレージ（**storage-url private**）を有効にする場合は、この手順を使用できます。プライベートストレージなしで、TFTP サーバーから実行コンテキスト コンフィギュレーションにダウンロードするには、**configure net** コマンドを使用します。SCP は、コンテキスト内でサポートされません

手順

スタートアップ コンフィギュレーションまたは実行コンフィギュレーションにファイルをコピーするには、適切なダウンロード サーバーに対して次のコマンドのいずれかを入力します。

- TFTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **tftp:**//*server*[/*path*]/*src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy tftp://10.1.1.67/files/old-running.cfg running-config
  ```

- FTP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **ftp:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy ftp://jcrichton:aeryn@10.1.1.67/files/old-startup.cfg startup-config
  ```

- HTTP（S） サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **http**[**s**]**:**//[*user*[**:***password*]**@**]*server*[**:***port*][/*path*]/*src_filename* {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy https://asun:john@10.1.1.67/files/new-running.cfg running-config
  ```

- SMB サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*] **smb:**//[*user*[**:***password*]**@**]*server*[/*path*]/*src_filename* {**startup-config** | **running-config**}

  例：

```
ciscoasa# copy /noconfirm smb://chiana:dargo@10.1.1.67/new-running.cfg running-config
```

- SCP サーバーからコピーします。

  copy [**/noconfirm**] [*interface_name*]
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/src_filename*[**;int=***interface_name*] {**startup-config** | **running-config**}

  例：

  ```
  ciscoasa# copy scp://pilot:moya@10.86.94.170/new-startup.cfg startup-config
  ```

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

例

たとえば、TFTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy tftp://209.165.200.226/configs/startup.cfg startup-config
```

FTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy ftp://admin:letmein@209.165.200.227/configs/startup.cfg startup-config
```

HTTP サーバーからコンフィギュレーションをコピーするには、次のコマンドを入力します。

```
ciscoasa# copy http://209.165.200.228/configs/startup.cfg startup-config
```

ASA イメージ、ASDM、およびスタートアップ コンフィギュレーションの設定

複数の ASA または ASDM イメージがある場合は、ブートするイメージを指定する必要があります。イメージを設定しない場合はデフォルトのブートイメージが使用され、そのイメージは意図されたものではない可能性があります。スタートアップ コンフィギュレーションでは、必要に応じて、隠しディレクトリではなく表示されるファイルシステム内のファイルを指定できます。

次のモデルのガイドラインを参照してください。

- Firepower 4100/9300 シャーシ：ASA のアップグレードは FXOS によって管理されます。ASA オペレーティング システム内で ASA をアップグレードすることはできないため、ASA イメージに対してこの手順を使用しないでください。ASA と FXOS は個別にアップグレードでき、FXOSディレクトリリストに別々に表示されます。ASAパッケージには必ず ASDM が含まれています。
- Firepower 1000Cisco Secure Firewall 1200/3100/4200：ASA、ASDM、および FXOS のイメージは1つのパッケージに一緒にバンドルされています。パッケージの更新は、次の手順を使用してASAによって管理されます。これらのプラットフォームでは、ブートするイメージを識別するために ASA が使用されますが、基盤となるメカニズムはレガシー ASA とは異なります。詳細については、以下のコマンドの説明を参照してください。
- モデルの ASDM：ASDM は ASA オペレーティングシステム内からアップグレードできるため、バンドルされた ASDM イメージのみを使用する必要はありません。Firepower 4100/9300 では、手動でアップロードする ASDM イメージは FXOS イメージリストに表示されません。ASA から ASDM イメージを管理する必要があります。

（注） ASAバンドルをアップグレードすると、同じ名前（**asdm.bin**）であるため、バンドル内の ASDM イメージが ASA 上の前の ASDM バンドルイメージに置き換わります。ただし、アップロードした別の ASDMイメージ（たとえば**asdm-782.bin**）を手動で選択すると、バンドルアップグレード後も引き続き同じイメージが使用されます。互換性のある ASDMバージョンを実行していることを確認するには、バンドルをアップグレードする前にASDMをアップグレードするか、または ASA バンドルをアップグレードする直前に、バンドルされた ASDMイメージ（**asdm.bin**）を使用するように ASA を再設定する必要があります。

- ASA 仮想：初期導入時の ASA 仮想 パッケージでは、ASA イメージが読み取り専用 boot:/ パーティションに配置されます。ASA 仮想 をアップグレードする際は、フラッシュメモリ内の別のイメージを指定します。後でコンフィギュレーションをクリアすると（**clear configure all**）、ASA 仮想 は元の展開のイメージをロードするようになることに注意してください。初期導入時のASA仮想パッケージには、フラッシュメモリに配置されるASDMイメージも含まれています。ASDM イメージを個別にアップグレードできます。
- **disk0:** は内部メモリです。その他のドライブ番号は、USB ドライブ、SSD、SD カードなどの外部ストレージを表します。

次のデフォルト設定を参照してください。

- ASA イメージ：
  - Firepower 1000Cisco Secure Firewall 1200/3100/4200：以前実行していたブートイメージをブートします。

- ISA 3000：内部フラッシュメモリ内で見つかった最初のアプリケーションイメージをブートします。
- ASA 仮想：最初に展開したときに作成された、読み取り専用の boot:/ パーティションにあるイメージをブートします。
- Firepower 4100/9300 シャーシ：どの ASA イメージをブートするかは FXOS システムによって決定されます。この手順を使用して ASA イメージを設定することはできません。

- すべての ASA 上の ASDM イメージ：内部フラッシュ メモリ内で見つかった（この場所にイメージがない場合は外部フラッシュ メモリ内で見つかった）最初の ASDM イメージをブートします。
- スタートアップ コンフィギュレーション：デフォルトで、ASA は、隠しファイルであるスタートアップ コンフィギュレーションからブートします。

手順

ステップ 1 ASA ブート イメージの場所を設定します。

boot system *url*

例：

```
ciscoasa(config)# boot system disk0:/images/asa921.bin
```

URL は次のようになります。

- **disk** *n*:/[*path*/]*filename*
- **tftp:**//[*user*[**:***password*]**@**]*server*[**:***port*]/[*path*/]*filename*

  TFTP オプションは、すべてのモデルでサポートされるわけではありません。

Firepower 1000 Secure Firewall 1200/3100/4200：1 つの **boot system** コマンドのみ入力できます。新しいイメージにアップグレードする場合は、**no boot system** を入力して、以前に設定したイメージを削除する必要があります。設定に **boot system** コマンドが存在しない場合があることに注意してください。たとえば、ROMMON からイメージをインストールした場合、新しいデバイスがある場合、またはコマンドを手動で削除した場合などです。**boot system** コマンドは、入力時にアクションを実行します。システムはイメージを検証して解凍し、ブート場所（FXOS によって管理される disk0 の内部ロケーション）にコピーします。ASA をリロードすると、新しいイメージがロードされます。リロードの前に気が変わった場合は、**no boot system** コマンドを入力してブート場所から新しいイメージを削除し、現在のイメージを引き続き実行することができます。このコマンドを入力した後、ASA フラッシュメモリから元のイメージファイルを削除することもできます。すると、ASA はブート場所から正しく起動します。ただし、**boot system** コマンドはフラッシュメモリ内のイメージでのみ動作するため、フラッシュメモリで使用するイメージを保持することをお勧めします。他のモデルとは異なり、スタートアップ コン

フィギュレーション内のこのコマンドは、ブートイメージに影響しません（本質的に表面的なものです）。リロード時には、最後にロードされたブートイメージが常に実行されます。このコマンドを入力した後で設定を保存しない場合、リロードすると、新しいイメージが起動された場合でも、古いコマンドが設定に出現します。設定を保存することにより、設定の同期を維持する必要があります。Cisco ダウンロード サイトからロードできるのは、元のファイル名のイメージのみです。ファイル名を変更した場合はロードされません。また、Firewall Threat Defense イメージをロードして Firewall Threat Defense に再イメージ化できます。この場合は、すぐにリロードするように求められます。

ASA 仮想 および ISA 3000：最大 4 つの **boot system** コマンドエントリを入力して、ブートする複数のイメージを順番に指定することができます。ASA は、最初に検出に成功したイメージをブートします。**boot system** コマンドを入力すると、エントリがリストの最後に追加されます。ブートエントリの順序を変更するには、**clear configure boot system** コマンドを使用してすべてのエントリを削除してから、エントリを目的の順序で再入力する必要があります。設定できる **boot system tftp** コマンドは 1 つだけです。これは、最初に設定する必要があります。

（注）
ASA が連続ブートのサイクルから抜け出せない場合は、ASA を ROMMON モードにリブートします。ROMMON モードの詳細については、デバッグ メッセージの表示を参照してください。

例：

```
asa(config)# boot system disk0:/cisco-asa-fp2k.9.13.2.SPA
The system is currently installed with security software package 9.13.1, which has:
   - The platform version:  2.7.1
   - The CSP (asa) version: 9.13.1
Preparing new image for install...
!!!!!!!!!!!!!
Image download complete (Successful unpack the image).
Installation of version 9.13.2 will do the following:
   - upgrade to the new platform version 2.7.2
   - upgrade to the CSP ASA version 9.13.2
After the installation is complete, reload to apply the new image.
Finalizing image install process...

Install_status: ready...........
Install_status: validating-images.....
Install_status: update-software-pack-completed
asa(config)#
```

ステップ 2 ブートする ASDM イメージを設定します。

asdm image disk*n*:/[*path*/]*filename*

例：

```
ciscoasa(config)# asdm image disk0:/images/asdm721.bin
```

ブートするイメージを指定しない場合、インストールされているイメージが 1 つしかなくても、ASA によって **asdm image** コマンドが実行コンフィギュレーションに挿入されます。[自動更新（Auto Update）]（設定されている場合）の問題を避けるため、また起動時ごとのイメー

ジ検索を回避するため、ブートする ASDM イメージをスタートアップ コンフィギュレーションで指定する必要があります。

ステップ 3 （オプション）スタートアップ コンフィギュレーションをデフォルトの隠しファイルではなく既知のファイルになるように設定します。

boot config disk*n***:/**[*path*/]*filename*

この機能は、隠しディレクトリに収まらない大規模な設定を使用する場合に重要です。大規模な設定を保存する場合、次のエラーメッセージが表示されるときは、代わりにこのコマンドを使用して設定を新しいファイルに保存してください。

```
%Error writing. nvram:/startup-config (No space left on device:)
```

例：

```
ciscoasa(config)# boot config disk0:/configs/startup1.cfg
```

コンフィギュレーションまたはその他のファイルのバックアップと復元

システム障害に備えて、コンフィギュレーション ファイルなどのシステム ファイルを定期的にバックアップすることを推奨します。

完全なシステム バックアップまたは復元の実行

次の手順では、コンフィギュレーションおよびイメージの zipバックアップ tar.gz ファイルへのバックアップおよび復元方法と、そのファイルのローカル コンピュータへの転送方法について説明します。

バックアップまた復元を開始する前に

- バックアップまたは復元を開始する前に、バックアップまたは復元場所に使用可能なディスク領域が少なくとも 300 MB ある必要があります。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 一度に開始できるバックアップまたは復元は 1 つだけです。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、

ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。

- クラスタリングを使用する場合、バックアップまたは復元できるのは、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみです。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、マスターパスフレーズの設定を参照して、バックアップを続行する前に、マスター パスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキー ペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キー ペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。
- CLI を使用してバックアップしてから ASDM を使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
  - 実行コンフィギュレーション
  - スタートアップ コンフィギュレーション
  - すべてのセキュリティ イメージ

    Cisco Secure Desktop およびホスト スキャンのイメージ

    Cisco Secure Desktop およびホスト スキャンの設定

    セキュアクライアント（SVC）画像とプロファイル

    セキュアクライアント（SVC）のカスタマイズおよびトランスフォーム
  - アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
  - VPN 事前共有キー
  - SSL VPN コンフィギュレーション
  - アプリケーション プロファイルのカスタム フレームワーク（APCF）

- ブックマーク
- カスタマイゼーション
- ダイナミック アクセス ポリシー（DAP）
- プラグイン
- 接続プロファイル用の事前入力スクリプト
- プロキシ自動設定
- 変換テーブル
- Web コンテンツ
- バージョン情報

システムのバックアップ

この手順では、完全なシステム バックアップを実行する方法について説明します。

手順

ステップ 1 システムをバックアップします。

backup [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# backup location disk0:/sample-backup]
Backup location [disk0:/sample-backup]?
```

interface *name* を指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

システム実行スペースからのマルチ コンテキスト モードで、**context** キーワードを入力して、指定したコンテキストをバックアップします。各コンテキストは個別にバックアップする必要があります。つまり、ファイルごとに **backup** コマンドを再入力する必要があります。

VPN 証明書および事前共有キーのバックアップ中、証明書を符号化するために、**passphrase** キーワードで指定された秘密キーが必要です。PKCS12 形式の証明書を符号化および復号化するために使用するパスフレーズを入力する必要があります。バックアップに含まれるのは証明書に関連する RSA キー ペアだけであり、スタンドアロン証明書は除外されます。

バックアップの **location** にはローカル ディスクまたはリモート URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。

- シングル モード：disk0:*hostname*.backup.*timestamp*.tar.gz
- マルチ モード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# backup location disk0:/sample-backup
Backup location [disk0:/sample-backup]?

Begin backup…
Backing up [ASA version] … Done!
Backing up [Running Config] … Done!
Backing up [Startup Config]  … Done!

Enter a passphrase to encrypt identity certificates. The default is cisco.
You will be required to enter the same passphrase while doing a restore: cisco
Backing up [Identity Certificates] … Done!

IMPORTANT: This device uses master passphrase encryption. If this backup file
is used to restore to a device with a different master passphrase,
you will need to provide the current master passphrase during restore.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Compressing the backup directory ... Done!
Copying Backup ... Done!
Cleaning up ... Done!
Backup finished!
```

バックアップの復元

zip tar.gz ファイルからローカル PC に復元するコンフィギュレーションやイメージを指定します。

手順

ステップ 1 バックアップ ファイルからシステムを復元します。

restore [**/noconfirm**] [**context** *ctx-name*] [**passphrase** *value*] [**location** *path*]

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
```

context キーワードを使用して複数のコンテキストを復元する場合、バック アップされた各コンテキスト ファイルは個別に復元する必要があります。つまり、**restore** コマンドをファイルごとに再入力する必要があります。

ステップ 2 プロンプトに従います。

例：

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?

Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version,
some configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption.
Master passphrase is required to restore running configuration,
startup configuration and VPN pre-shared keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to
this device, please note them for future reference.

ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside,
the IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside,
the IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations.
Do not overwrite configuration file if you want to preserve the old http-
and https-proxy configurations.

Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates.
The default is cisco. If the passphrase is not correct, certificates will not be restored.

No passphrase was provided for identity certificates.
Using the default value: cisco. If the passphrase is not correct,
```

```
certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

自動バックアップおよび復元の設定（ISA 3000）

ISA 3000 では、**write memory** を使用して設定を保存するたびに、特定の場所への自動バックアップを設定できます。

自動復元では、完全な設定を SD フラッシュメモリカードにロードして、新しいデバイスを簡単に設定できます。工場出荷時のデフォルト設定では、自動復元が有効になっています。

自動バックアップの設定（ISA 3000）

ISA 3000 では、**write memory** を使用して設定を保存するたびに、特定の場所への自動バックアップを設定できます。

始める前に

この機能は、ISA 3000 のみで使用できます。

手順

ステップ 1 パッケージのバックアップ パラメータを設定します。

backup-package backup [**interface** *name*] **location** {**disk***n***:** | *url*} [**passphrase** *string*]

- **interface** *name*：オフデバイスストレージを指定した場合に、バックアップ URL に到達するためのインターフェイスを指定します。interface name を指定しない場合、ASA は管理専用のルーティングテーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。
- **location** {**disk***n***:** | *url*}：データのバックアップに使用するストレージメディアを指定します。URL またはローカルストレージを指定できます。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。自動復元のデフォルト設定では disk3 が使用されます。
- **passphrase** *string*：バックアップデータを保護するためのパスフレーズを設定します。自動復元のデフォルト設定では、パスフレーズとして「cisco」が使用されます。

これらの設定は、手動の **backup** コマンドでもデフォルトで使用されます。システムのバックアップ （27 ページ）を参照してください。自動バックアップまたは復元を有効にしている場

合に手動の**backup**コマンドを使用すると、指定した名前のバックアップファイルと、自動バックアップおよび復元で使用される「auto-backup-asa.tgz」という名前のファイルが保存されます。

例：

```
ciscoasa(config)# backup-package backup location disk3: passphrase cisco
```

ステップ 2 バックアップおよび復元の自動モードを有効にします。

backup-package backup auto

write memory を使用して設定を保存すると、設定は自動的にバックアップ場所とスタートアップ コンフィギュレーションに保存されます。バックアップファイルの名前は「auto-backup-asa.tgz」です。自動バックアップを無効にするには、このコマンドの **no** 形式を使用します。

例：

```
ciscoasa(config)# backup-package backup auto
```

自動復元の設定（ISA 3000）

自動復元モードは、ユーザの操作なしでデバイスのシステム設定を復元します。たとえば、保存したバックアップ設定を含む SD メモリカードを新しいデバイスに挿入し、デバイスの電源をオンにします。デバイスが起動すると、システム設定を復元する必要があるかどうかを判断するために SD カードがチェックされます。（復元は、バックアップファイルに別のデバイスの「フィンガープリント」がある場合にのみ開始されます。バックアップファイルのフィンガープリントは、バックアップまたは復元操作中に現在のデバイスに一致するように更新されます。そのため、デバイスがすでに復元を完了している場合、またはデバイスが独自のバックアップを作成している場合は、自動復元はスキップされます。）フィンガープリントに復元が必要であることが示されている場合、デバイスはシステム設定を置き換えます（startup-config、running-config、SSL VPN 設定など。バックアップの内容の詳細については、システムのバックアップ （27 ページ）を参照してください）。デバイスの起動が完了すると、保存された設定が実行されます。

工場出荷時のデフォルト設定では自動復元が有効になっているため、デバイスの事前設定を実行しなくても、SD メモリカードにロードされた完全な設定で新しいデバイスを簡単に設定できます。

デバイスは、システム設定を復元する必要があるかどうかをブートプロセスの早い段階で決定する必要があるため、ROMMON 変数をチェックして、デバイスが自動復元モードかどうかを判断し、バックアップ設定の場所を取得します。次の ROMMON 変数が使用されます。

- **RESTORE_MODE =** {**auto** | **manual**}

  デフォルトは **auto** です。

- **RESTORE_LOCATION** = {**disk0:** | **disk1:** | **disk2:** | **disk3:**}

  デフォルトは **disk3:** です。

- **RESTORE_PASSPHRASE** = *key*

  デフォルトは **cisco** です。

自動復元設定を変更するには、次の手順を実行します。

始める前に

- この機能は、ISA 3000 のみで使用できます。
- デフォルトの復元設定を使用する場合は、SD メモリカード（部品番号 SD-IE-1GB=）を取り付ける必要があります。
- 自動復元を有効にするためにデフォルト設定を復元する必要がある場合は、**configure factory default** コマンドを使用します。このコマンドは、トランスペアレント ファイアウォール モードでのみ使用できます。そのため、ルーテッド ファイアウォール モードの場合は、最初に **firewall transparent** コマンドを使用します。

手順

ステップ 1 パッケージの復元のパラメータを設定します。

backup-package restore location {**disk***n***:** | *url*} [**passphrase** *string*]

- **location disk***n***:**：データの復元に使用するストレージメディアを指定します。disk0 は内部フラッシュドライブです。disk1 は USB 1 のオプションの USB メモリスティックです。disk2 は USB 2 のオプションの USB メモリスティックです。disk3 は SD メモリカードです。デフォルトは disk3 です。
- **passphrase** *string*：バックアップデータを読み取るパスフレーズを設定します。デフォルトは「cisco」です。

これらの設定は、手動の **restore** コマンドでもデフォルトで使用されます。システムのバックアップ （27 ページ）を参照してください。

例：

```
ciscoasa(config)# backup-package restore location disk1: passphrase $upe3rnatural
```

ステップ 2 復元の自動モードを有効または無効にします。

[**no**] **backup-package restore auto**

復元されるファイルの名前は「auto-backup-asa.tgz」です。

例：

```
ciscoasa(config)# no backup-package restore auto
```

シングル モード コンフィギュレーションまたはマルチ モード システム コンフィギュレーションのバックアップ

シングルコンテキスト モードで、またはマルチモードのシステム コンフィギュレーションから、スタートアップ コンフィギュレーションまたは実行コンフィギュレーションを外部サーバーまたはローカル フラッシュ メモリにコピーできます。

始める前に

（オプション）ASAがサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

手順

次のサーバー タイプの 1 つを使用してコンフィギュレーションをバックアップします。

- TFTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **tftp://***server*[*/path*]*/dst_filename*

  例：

  ```
  ciscoasa# copy running-config tftp://10.1.1.67/files/new-running.cfg
  ```

- FTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **ftp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

  ```
  ciscoasa# copy startup-config ftp://jcrichton:aeryn@10.1.1.67/files/new-startup.cfg
  ```

- SMB サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **smb://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy /noconfirm running-config smb://chiana:dargo@10.1.1.67/new-running.cfg
```

- SCP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**startup-config** | **running-config**} **scp://**[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  例：

  ```
  ciscoasa# copy startup-config
  scp://pilot:moya@10.86.94.170/new-startup.cfg
  ```

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

- ローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**startup-config** | **running-config**} {**disk0**|**disk1**}**:/**[*path/*]*dst_filename*

  例：

  ```
  ciscoasa# copy /noconfirm running-config disk0:/new-running.cfg
  ```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず**mkdir** コマンドを使用してディレクトリを作成します。

フラッシュ メモリ内のコンテキスト コンフィギュレーションまたはその他のファイルのバック アップ

システム実行スペースで次のいずれかのコマンドを入力することによって、ローカル フラッシュ メモリにあるコンテキスト コンフィギュレーションまたは他のファイルをコピーします。

始める前に

（オプション）ASA がサーバーとの通信に使用するインターフェイスを指定します。インターフェイスを指定しない場合、ASA は管理専用のルーティング テーブルをチェックします。ここで一致が見つからない場合はデータのルーティング テーブルをチェックします。

手順

次のサーバー タイプの 1 つを使用してコンテキスト コンフィギュレーションバックアップをバックアップします。

- フラッシュから TFTP サーバーにコピーします。

copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
tftp://*server*[*/path*]*/dst_filename*

例：

```
ciscoasa# copy disk0:/asa-os.bin tftp://10.1.1.67/files/asa-os.bin
```

- フラッシュから FTP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  ftp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy disk0:/asa-os.bin ftp://jcrichton:aeryn@10.1.1.67/files/asa-os.bin
```

- フラッシュから SMB サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  smb://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*

  例：

```
ciscoasa# copy /noconfirm copy disk0:/asdm.bin
smb://chiana:dargo@10.1.1.67/asdm.bin
```

- フラッシュから SCP サーバーにコピーします。

  copy [**/noconfirm**] [*interface_name*] {**disk0**|**disk1**}**:/**[*path*/]*src_filename*
  scp://[*user*[**:***password*]**@**]*server*[*/path*]*/dst_filename*[**;int=***interface_name*]

  例：

```
ciscoasa# copy disk0:/context1.cfg
scp://pilot:moya@10.86.94.170/context1.cfg
```

  ;int=*interface* オプションは、ルート ルックアップをバイパスして、常に指定されたインターフェイスを使用して SCP サーバーに到達します。

- フラッシュからローカル フラッシュ メモリにコピーします。

  copy [**/noconfirm**] {**disk0**|**disk1**}**:/**[*path*/]*src_filename* {**disk0**|**disk1**}**:/**[*path*/]*dst_filename*

  例：

```
ciscoasa# copy /noconfirm disk1:/file1.cfg disk0:/file1.cfgnew-running.cfg
```

  宛先ディレクトリが存在することを確認してください。存在しない場合は、まず**mkdir** コマンドを使用してディレクトリを作成します。

コンテキスト内でのコンテキスト コンフィギュレーションのバックアップ

マルチ コンテキスト モードでは、コンテキスト内から次のバックアップを実行できます。

手順

ステップ 1 （リモートサーバーの場合、admin コンテキストに接続された）スタートアップ構成サーバーに実行コンフィギュレーションをコピーします。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。

copy running-config startup-config

例：

```
ciscoasa/contexta# copy running-config startup-config
```

ステップ 2 コンテキストネットワークに接続された FTP または TFTP サーバーに実行構成をコピーします。

copy running-config {**ftp** | **tftp**}**:**//*url*/*dest_filename*

正確な URL オプションについては、**copy** コマンドのヘルプを参照してください。

プライベートストレージ（**storage-url private**）を有効にすると、他のサーバーオプションも使用できます。 ただし、コンテキスト内では SCP はサポートされません。

例：

```
ciscoasa/contexta# copy running-config tftp:/10.89.6.8/configs/1010-1.cfg
```

端末ディスプレイからのコンフィギュレーションのコピー

手順

ステップ 1 コンフィギュレーションを端末に表示します。

more system:running-config

ステップ 2 コマンドから出力をコピーして、コンフィギュレーションをテキスト ファイルに貼り付けます。

export および import コマンドを使用した追加ファイルのバックアップ

コンフィギュレーションに欠かせない追加ファイルは次のとおりです。

- **import webvpn** コマンドを使用してインポートするファイル。現在これらのファイルには、カスタマイゼーション、URL リスト、Web コンテンツ、プラグイン、および言語翻訳などがあります。
- DAP ポリシー（dap.xml）。
- CSD コンフィギュレーション（data.xml）。
- デジタル キーおよびデジタル証明書。
- ローカル CA ユーザー データベース ファイルと証明書ステータス ファイル。

CLI では、**export** コマンドと **import** コマンドを使用して、コンフィギュレーションの個々の要素をバックアップおよび復元できます。

これらのファイル（たとえば、**import webvpn** コマンドを使用してインポートしたこれらのファイルや証明書など）をバックアップするには、次の手順を実行します。

手順

ステップ 1 次のように、適用可能な **show** コマンドを実行します。

```
ciscoasa # show import webvpn plug-in
ica
rdp
ssh, telnet
vnc
```

ステップ 2 バックアップするファイルに対して **export** コマンドを発行します（この例では rdp ファイルです）。

```
ciscoasa # export webvpn plug-in protocol rdp tftp://tftpserver/backupfilename
```

スクリプトを使用したファイルのバックアップおよび復元

スクリプトを使用して、ASA のコンフィギュレーション ファイルをバックアップおよび復元できます。これには、**import webvpn** CLI によってインポートする拡張機能のすべて、CSD コンフィギュレーションの XML ファイル、および DAP コンフィギュレーションの XML ファイルが含まれます。セキュリティ上の理由により、デジタル キーと証明書、またはローカル CA キーの自動バックアップを実行することはお勧めしません。

この項では、自動バックアップの手順について説明します。また、そのまま使用することも、環境要件に合わせて修正することもできるサンプル スクリプトを示します。サンプル スクリプトはLinuxシステムに固有のスクリプトです。Microsoft Windowsシステムで使用するには、サンプルのロジックを使用して修正する必要があります。

（注） 代わりに、**backup** コマンドと **restore** コマンドを使用することもできます。詳細については、完全なシステム バックアップまたは復元の実行 （25 ページ）を参照してください。

バックアップおよび復元スクリプトを使用する前に

スクリプトを使用して ASA コンフィギュレーションをバックアップおよび復元するには、まず次の作業を実行します。

- Expect モジュールとともに Perl をインストールする。
- ASA に到達可能な SSH クライアントをインストールする。
- TFTP サーバーをインストールして、ASA からバックアップ サイトにファイルを送信する。

別の選択肢としては、市販のツールを使用します。このスクリプトのロジックをそれらのツールに取り入れることができます。

スクリプトを実行する

バックアップおよび復元のスクリプトを実行するには、次の手順を実行します。

手順

ステップ 1 システムの任意の場所に、スクリプトファイルをダウンロードまたはカットアンドペーストします。

ステップ 2 コマンド ラインで、**Perl***scriptname* と入力します。*scriptname* はスクリプト ファイルの名前です。

ステップ 3 Enter を押します。

ステップ 4 オプションごとに値を入力するように、プロンプトが表示されます。あるいは、**Perl***scriptname* コマンドを入力するときにオプションの値を入力してから、**Enter** を押すこともできます。どちらの方法でも、スクリプトによりオプションごとに値を入力するよう求められます。

ステップ 5 このスクリプトが実行され、発行されるコマンドが出力されます。この出力はCLIの記録となります。これらの CLI は後で行われる復元に使用できます。特に、ファイルを 1 つまたは 2 つだけ復元する場合に便利です。

サンプルスクリプト

```
#!/usr/bin/perl
#Description: The objective of this script is to show how to back up
configurations/extensions.
# It currently backs up the running configuration, all extensions imported via "import
webvpn" command, the CSD configuration XML file, and the DAP configuration XML file.
#Requirements: Perl with Expect, SSH to the ASA, and a TFTP server.
#Usage: backupasa -option option_value
#       -h: ASA hostname or IP address
#       -u: User name to log in via SSH
#       -w: Password to log in via SSH
#       -e: The Enable password on the security appliance
#       -p: Global configuration mode prompt
#       -s: Host name or IP address of the TFTP server to store the configurations
#      -r: Restore with an argument that specifies the file name. This file is produced
 during backup.
#If you don't enter an option, the script will prompt for it prior to backup.
#
#Make sure that you can SSH to the ASA.

use Expect;
use Getopt::Std;

#global variables
%options=();
$restore = 0; #does backup by default
$restore_file = '';
$asa = '';
$storage = '';
$user = '';
$password = '';
$enable = '';
$prompt = '';
$date = `date +%F`;
chop($date);
my $exp = new Expect();

getopts("h:u:p:w:e:s:r:",\%options);
do process_options();

do login($exp);
do enable($exp);
if ($restore) {
   do restore($exp,$restore_file);
}
else {
   $restore_file = "$prompt-restore-$date.cli";
   open(OUT,">$restore_file") or die "Can't open $restore_file\n";
   do running_config($exp);
   do lang_trans($exp);
   do customization($exp);
   do plugin($exp);
   do url_list($exp);
   do webcontent($exp);
   do dap($exp);
   do csd($exp);
   close(OUT);
}
do finish($exp);

sub enable {
   $obj = shift;
```

```
   $obj->send("enable\n");
   unless ($obj->expect(15, 'Password:')) {
      print "timed out waiting for Password:\n";
   }
   $obj->send("$enable\n");
   unless ($obj->expect(15, "$prompt#")) {
      print "timed out waiting for $prompt#\n";
   }
}

sub lang_trans {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn translation-table\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     s/^\s+//;
     s/\s+$//;
     next if /show import/ or /Translation Tables/;
     next unless (/^.+\s+.+$/);
     ($lang, $transtable) = split(/\s+/,$_);
     $cli = "export webvpn translation-table $transtable language $lang
$storage/$prompt-$date-$transtable-$lang.po";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub running_config {
  $obj = shift;
  $obj->clear_accum();
  $cli ="copy /noconfirm running-config $storage/$prompt-$date.cfg";
  print "$cli\n";
  $obj->send("$cli\n");
  $obj->expect(15, "$prompt#" );
}


sub customization {
  $obj = shift;
  $obj->clear_accum();
  $obj->send("show import webvpn customization\n");
  $obj->expect(15, "$prompt#" );
  $output = $obj->before();
  @items = split(/\n+/, $output);

  for (@items) {
    chop;
    next if /^Template/ or /show import/ or /^\s*$/;
    $cli = "export webvpn customization $_ $storage/$prompt-$date-cust-$_.xml";
    $ocli = $cli;
    $ocli =~ s/^export/import/;
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
  }
```

```
}

sub plugin {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn plug-in\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/;
     $cli = "export webvpn plug-in protocol $_ $storage/$prompt-$date-plugin-$_.jar";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub url_list {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("show import webvpn url-list\n");
   $obj->expect(15, "$prompt#" );
   $output = $obj->before();
   @items = split(/\n+/, $output);

   for (@items) {
     chop;
     next if /^Template/ or /show import/ or /^\s*$/ or /No bookmarks/;
     $cli="export webvpn url-list $_ $storage/$prompt-$date-urllist-$_.xml";
     $ocli = $cli;
     $ocli =~ s/^export/import/;
     print "$cli\n";
     print OUT "$ocli\n";
     $obj->send("$cli\n");
     $obj->expect(15, "$prompt#" );
   }
}

sub dap {
   $obj = shift;
   $obj->clear_accum();
   $obj->send("dir dap.xml\n");
   $obj->expect(15, "$prompt#" );

   $output = $obj->before();
   return 0 if($output =~ /Error/);

   $cli="copy /noconfirm dap.xml $storage/$prompt-$date-dap.xml";
   $ocli="copy /noconfirm $storage/$prompt-$date-dap.xml disk0:/dap.xml";
   print "$cli\n";
   print OUT "$ocli\n";
   $obj->send("$cli\n");
   $obj->expect(15, "$prompt#" );
}

sub csd {
   $obj = shift;
   $obj->clear_accum();
```

```
    $obj->send("dir sdesktop\n");
    $obj->expect(15, "$prompt#" );

    $output = $obj->before();
    return 0 if($output =~ /Error/);

    $cli="copy /noconfirm sdesktop/data.xml $storage/$prompt-$date-data.xml";
    $ocli="copy /noconfirm $storage/$prompt-$date-data.xml disk0:/sdesktop/data.xml";
    print "$cli\n";
    print OUT "$ocli\n";
    $obj->send("$cli\n");
    $obj->expect(15, "$prompt#" );
}

sub webcontent {
    $obj = shift;
    $obj->clear_accum();
    $obj->send("show import webvpn webcontent\n");
    $obj->expect(15, "$prompt#" );
    $output = $obj->before();
    @items = split(/\n+/, $output);

    for (@items) {
      s/^\s+//;
      s/\s+$//;
      next if /show import/ or /No custom/;
      next unless (/^.+\s+.+$/);
      ($url, $type) = split(/\s+/,$_);
      $turl = $url;
      $turl =~ s/\//\+//;
      $turl =~ s/\+\//-/;
      $cli = "export webvpn webcontent $url $storage/$prompt-$date-$turl";
      $ocli = $cli;
      $ocli =~ s/^export/import/;
      print "$cli\n";
      print OUT "$ocli\n";
      $obj->send("$cli\n");
      $obj->expect(15, "$prompt#" );
    }
}

sub login {
    $obj = shift;
    $obj->raw_pty(1);
    $obj->log_stdout(0); #turn off console logging.
    $obj->spawn("/usr/bin/ssh $user\@$asa") or die "can't spawn ssh\n";
    unless ($obj->expect(15, "password:" )) {
        die "timeout waiting for password:\n";
    }

    $obj->send("$password\n");

    unless ($obj->expect(15, "$prompt>" )) {
        die "timeout waiting for $prompt>\n";
    }
}

sub finish {
    $obj = shift;
    $obj->hard_close();
    print "\n\n";

}
```

```
sub restore {
   $obj = shift;
   my $file = shift;
   my $output;
   open(IN,"$file") or die "can't open $file\n";
   while (<IN>) {
      $obj->send("$_");
      $obj->expect(15, "$prompt#" );
      $output = $obj->before();
      print "$output\n";
   }
   close(IN);
}

sub process_options {
  if (defined($options{s})) {
      $tstr= $options{s};
      $storage = "tftp://$tstr";
  }
  else {
      print "Enter TFTP host name or IP address:";
      chop($tstr=<>);
      $storage = "tftp://$tstr";
  }
  if (defined($options{h})) {
      $asa = $options{h};
  }
  else {
      print "Enter ASA host name or IP address:";
      chop($asa=<>);
  }

  if (defined ($options{u})) {
      $user= $options{u};
  }
  else {
      print "Enter user name:";
      chop($user=<>);
  }

  if (defined ($options{w})) {
      $password= $options{w};
  }
  else {
      print "Enter password:";
      chop($password=<>);
  }
  if (defined ($options{p})) {
      $prompt= $options{p};
  }
  else {
      print "Enter ASA prompt:";
      chop($prompt=<>);
  }
  if (defined ($options{e})) {
      $enable = $options{e};
  }
  else {
      print "Enter enable password:";
      chop($enable=<>);
  }

  if (defined ($options{r})) {
     $restore = 1;
```

```
        $restore_file = $options{r};
    }
}
```

Cisco Secure Firewall 3100/4200/6100 での SSD のホットスワップ

SSD が 2 つある場合、起動時に RAID が形成されます。ファイアウォールの電源が入っている状態で CLI で次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

  Cisco Secure Firewall デバイスで SSD を 1 つだけ使用する場合、[ドライブの状態（Drive State）] に [劣化（degraded）] と表示されます。

⚠

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

手順

ステップ 1 SSD の 1 つを取り外します。

a) SSD を RAID から取り外します。

raid remove-secure local-disk {**1** | **2**}

remove-secure キーワードは SSD を RAID から削除し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。SSD を RAID から削除するだけでデータをそのまま維持する場合は、**remove** キーワードを使用できます。

例：

```
ciscoasa(config)# raid remove-secure local-disk 2
```

b) SSD がインベントリに表示されなくなるまで、RAID ステータスを監視します。

show raid

SSD が RAID から削除されると、**操作性**と**ドライブの状態**が**劣化**として表示されます。2 つ目のドライブは、メンバーディスクとして表示されなくなります。

例：

```
ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                operable
Presence:                   equipped
Lifecycle:                  available
Drive State:                optimal
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   0
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

Device Name:                nvme1n1
Disk State:                 in-sync
Disk Slot:                  2
Read Errors:                0
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:

ciscoasa# show raid
Virtual Drive
ID:                         1
Size (MB):                  858306
Operability:                degraded
Presence:                   equipped
Lifecycle:                  available
Drive State:                degraded
Type:                       raid
Level:                      raid1
Max Disks:                  2
Meta Version:               1.0
Array State:                active
Sync Action:                idle
Sync Completed:             unknown
Degraded:                   1
Sync Speed:                 none

RAID member Disk:
Device Name:                nvme0n1
Disk State:                 in-sync
Disk Slot:                  1
Read Errors:                0
```

```
Recovery Start:             none
Bad Blocks:
Unacknowledged Bad Blocks:
```

c) SSD をシャーシから物理的に取り外します。

ステップ 2 SSD を追加します。

a) SSD を空のスロットに物理的に追加します。

b) SSD を RAID に追加します。

raid add local-disk {**1** | **2**}

新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。ステータスを表示するには、**show raid** コマンドを使用します。

以前に別のシステムで使用されており、まだロックされている SSD を取り付ける場合は、次のコマンドを入力します。

raid add local-disk {**1** | **2**} *psid*

psid は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。

USB ポートの無効化

デフォルトでは、タイプ A USB ポートは有効になっています。セキュリティ上の理由から、USB ポートへのアクセスを無効にする必要がある場合があります。USB の無効化は、次のモデルでサポートされています。

- Firepower 1000 シリーズ
- Cisco Secure Firewall 200 シリーズ
- Cisco Secure Firewall 3100
- Cisco Secure Firewall 4200
- Cisco Secure Firewall 6100 シリーズ

ガイドライン

- USB ポートを有効または無効にするにはリロードが必要です。
- USB ポートが無効で、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効のままになります。NVRAM を消去（FXOS local-mgmt **erase secure all** コマンド）せずに再度有効にすることはできません。
- ROMMON **factory-reset** または FXOS local-mgmt **erase secure** を実行すると、USB ポートが再度有効になります。

- アクティブユニットまたは制御ノードの USB ポートを無効または有効にし、高可用性またはクラスタリングを設定します。コマンドが他のノードに複製されます。ただし、変更を有効にするには、各ユニットをリロードする必要があります。

（注） この機能は、USB コンソールポート（存在する場合）には影響しません。

手順

ステップ 1 USB ポートを無効化します。

usb-port disable

write memory

reload

USB ポートを再度有効にするには、**no usb-port disable** と入力します。

例：

```
ciscoasa(config)# usb-port disable
Requesting USB disable. This may take 30 seconds to complete.
Please execute 'write memory' and reboot the system to apply
any operational state changes.

ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 19d02ee0 671dbe24 88193adb bccb8147

12382 bytes copied in 0.530 secs
[OK]

ciscoasa(config)# reload
Proceed with reload? [confirm]
```

ステップ 2 ポートステータスを表示します。

show usb-port

[管理ステータス（Admin State）] には、USB ポートの設定が表示されます。[動作ステータス（Oper State）] には、現在の動作が表示されます。たとえば、USB ポートを無効化してリロードしていない場合、[管理ステータス（Admin State）] には無効と表示され、[動作ステータス（Oper State）] は有効になります。

例：

```
ciscoasa(config)# show usb-port
USB Port info
---------------
Admin State: disabled
```

```
Oper State: disabled
```

ソフトウェアとコンフィギュレーションの履歴

機能名	プラットフォームリリース	機能情報
セキュアコピークライアントおよびサーバ	9.1(5)/9.2(1)	SCP サーバとの間でファイルを転送するため、ASA は Secure Copy（SCP）クライアントおよびサーバをサポートするようになりました。 **ssh pubkey-chain**、**server (ssh pubkey-chain)**、**key-string**、**key-hash**、**ssh stricthostkeycheck** の各コマンドが導入されました。 **copy scp** コマンドが変更されました。
設定可能な SSH 暗号機能と整合性アルゴリズム	9.1(7)/9.4(3)/9.5(3)/9.6(1)	ユーザーは SSH 暗号化を管理するときに暗号化モードを選択し、さまざまなキー交換アルゴリズムに対して HMAC と暗号化を設定できます。アプリケーションに応じて、暗号の強度を強くしたり弱くする必要がある場合があります。セキュアなコピーのパフォーマンスは暗号化アルゴリズムに一部依存します。デフォルトで、ASA は 3des-cbc aes128-cbc aes192-cbc aes256-cbc aes128-ctr aes192-ctr aes256-ctr の順にアルゴリズムをネゴシエートします。提示された最初のアルゴリズム（3des-cbc）が選択された場合、aes128-cbc などの一層効率的なアルゴリズムが選択された場合よりも大幅にパフォーマンスが低下します。たとえば、提示された暗号方式に変更するには、**ssh cipher encryption custom aes128-cbc** を使用します。 次のコマンドが導入されました。**ssh cipher encryption**、**ssh cipher integrity**

機能名	プラットフォームリリース	機能情報
デフォルトでイネーブルになっている Auto Update サーバー証明書の検証	9.2(1)	Auto Update サーバ証明書の検証がデフォルトでイネーブルになりました。新しいコンフィギュレーションでは証明書の検証を明示的にディセーブルにする必要があります。証明書の確認をイネーブルにしていなかった場合に、以前のリリースからアップグレードしようとすると、証明書の確認はイネーブルではなく、次の警告が表示されます。 `WARNING: The certificate provided by the auto-update servers will not be verified. In order to verify this certificate please use the verify-certificate option.` 設定を移行する場合は、次のように確認なしを明示的に設定します。 **auto-update server no-verification** **auto-update server** {**verify-certificate** | **no-verification**} コマンドが変更されました。
CLIを使用したシステムのバックアップと復元	9.3(2)	CLIを使用してイメージや証明書を含む完全なシステムコンフィギュレーションをバックアップおよび復元できるようになりました。 **backup** および **restore** の各コマンドが導入されました。
新しいASA 5506W-Xイメージの回復およびロード	9.4(1)	新しいASA 5506W-Xイメージのリカバリおよびロードがサポートされています。 **hw-module module wlan recover image** コマンドが導入されました。
ISA 3000 の自動バックアップと復元	9.7(1)	バックアップ コマンドと復元コマンドのプリセット パラメータを使用して、自動バックアップ機能や自動復元機能を有効にできます。これらの機能は、外部メディアからの初期設定、デバイス交換、作動可能状態へのロールバックなどで使用されます。 次のコマンドが導入されました。**backup-package location**、**backup-package auto**、**show backup-package status**、**show backup-package summary**

機能名	プラットフォームリリース	機能情報
SCP クライアントを使用する場合、CiscoSSH スタックには SSH アクセスが必要です	9.17(1)	CiscoSSH スタックを使用する場合、ASA **copy** コマンドを使用して SCP サーバとの間でファイルをコピーするには、**ssh** コマンドを使用して SCP サーバサブネット/ホストの SSH アクセスを ASA で有効にする必要があります。
Cisco Secure Firewall 3100 での SSD の RAID サポート	9.17(1)	SSD は自己暗号化ドライブ（SED）です。SSD が 2 つある場合、ソフトウェア RAID を形成します。 新規/変更されたコマンド：**raid**、**show raid**、**show ssd**
USB ポートの無効化	9.22(1)	デフォルトでは、タイプ A USB ポートは有効になっていて、無効にできません。次のモデルで、セキュリティ上の目的で USB ポートアクセスを無効にできるようになりました。 • Firepower 1000 • Cisco Secure Firewall 1200 • Cisco Secure Firewall 3100 • Cisco Secure Firewall 4200 この設定はファームウェアに保存され、リロードが必要です。USB ポートが無効で、この機能をサポートしていないバージョンにダウングレードすると、ポートは無効のままになります。NVRAM を消去せずに再度有効にすることはできません。 （注） この機能は、USB コンソールポート（存在する場合）には影響しません。 新規/変更されたコマンド：**usb-port disable**、**show usb-port**

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。

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。