

PIX 500 シリーズ セキュリティ アプライアンスから ASA 5500 シリーズ 適応型 セキュリティ アプライアンスへの移行

内容

[概要](#)

[前提条件](#)

[ハードウェアおよびソフトウェアの要件](#)

[使用するコンポーネント](#)

[表記法](#)

[手動による設定の変換](#)

[PIX ソフトウェア バージョンの 7.x へのアップグレード](#)

[copy tftp flash コマンドによる PIX セキュリティ アプライアンスのアップグレード](#)

[モニタ モードからの PIX セキュリティ アプライアンスのアップグレード](#)

[Cisco PIX ソフトウェア 7.0 から Cisco ASA 形式へのインターフェイス名の変換](#)

[PIX から ASA への設定のコピー](#)

[方法1：手動コピー/貼り付け](#)

[方法2:TFTP/FTPからのダウンロード](#)

[PIX ソフトウェア バージョン 6.x 設定の ASA ソフトウェア バージョン 7.x への適用](#)

[トラブルシューティング：手動による設定の変換](#)

[デバイスがリブート ループで停止する](#)

[エラー メッセージ](#)

[設定が正しくない](#)

[FTP などの一部のサービスが機能しない](#)

[Cisco PIX セキュリティ アプライアンスを Cisco Adaptive Security Appliance \(ASA \) に置き換えたときにインターネットにアクセスできない](#)

[関連情報](#)

概要

このドキュメントでは、PIX 500 シリーズ セキュリティ アプライアンスから ASA 5500 シリーズ 適応型セキュリティ アプライアンスへの移行方法について説明しています。

注：PIX 501、PIX 506、およびPIX 506Eは、ソフトウェアバージョン7をサポートしていません。

PIX設定をASA設定に変換するには、次の2つの方法があります。

- Tool-Assisted 変換
- 手動による変換

自動的なツール ベース/Tool-Assisted 変換

シスコでは、PIX 設定を ASA 設定に変換する際、Tool-Assisted 変換を使用することを推奨しています。

Tool-Assisted 変換による方法は、複数の変換を行う場合により高速で、拡張性にも優れています。ただし、中間設定でのプロセスの出力には、古い構文と新しい構文の両方が含まれます。この方法は、変換の完了を、ターゲットとなる適応型セキュリティ アプライアンスへの中間設定のインストールに依存しています。ターゲット デバイスへのインストールが完了するまで、最終的な設定を確認することはできません。

注：シスコは、新しいASAアプライアンスへの移行プロセスを自動化するために、PIXからASAへの移行ツールをリリースしました。このツールは、PIX ソフトウェアのダウンロード サイトからダウンロードできます。詳細は、『[PIX 500 シリーズ セキュリティ アプライアンス設定の ASA 5500 シリーズ適応型セキュリティ アプライアンスへの移行](#)』を参照してください。

前提条件

ハードウェアおよびソフトウェアの要件

PIX 515、515E、525、535 をバージョン 7.0 にアップグレードできます。

シスコでは、バージョン 7.x へのアップグレード プロセスを開始する前は、PIX でバージョン 6.2 以降が実行されていることを推奨します。これによって、現在の設定が正しく変換されるようになります。さらに、これらのハードウェア要件は、次に示す最小限の RAM 要件を満たしている必要があります。

PIX モデル	RAM 要件	
	制限あり (R)	制限なし (UR) / フェールオーバーのみ (FO)
PIX-515	64 MB*	128 MB*
PIX-515 E	64 MB*	128 MB*
PIX-525	128 MB	256 MB
PIX-535	512 MB	1 GB

現在 PIX 上にインストールされているメモリ量を調べるには、show version コマンドを発行します。

注：PIX 515および515Eソフトウェアのアップグレードでは、メモリのアップグレードも必要になる場合があります。

- 制限付きライセンスおよびメモリが 32 MB のアプライアンスは、メモリを 64 MB にアップグレードする必要があります。
- 無制限ライセンスおよびメモリが 64 MB のアプライアンスは、メモリを 128 MB にアップグレードする必要があります。

これらのアプライアンスでメモリをアップグレードするには、次の表で必要な部品番号を確認してください。

現在のアプライアンスの設定		アップグレード ソリューション	
プラットフォームのライセンス	合計メモリ (アップグレード前)	部品番号	合計メモリ (アップグレード後)
制限あり (R)	32 MB	PIX-515-MEM-32=	64 MB
制限なし (UR)	32 MB	PIX-515-MEM-128=	128 MB
フェールオーバーのみ (FO)	64 MB	PIX-515-MEM-128=	128 MB

注：部品番号は、PIXにインストールされているライセンスによって異なります。

ソフトウェアバージョン 6.x から 7.x へのアップグレードはシームレスに実行され、多少の手作業が必要になります。ただし、アップグレードを始める前に、次の手順を実行する必要があります。

1. 現在の設定に conduit コマンドまたは outbound/apply コマンドがないことを確認します。これらのコマンドは、7.x ではサポートされていないため、アップグレードプロセスによって削除されます。アップグレードを実行する前にこれらのコマンドをアクセスリストに変換するには、[Conduit Converter](#) ツールを使用します。
2. PIX が Point to Point Tunneling Protocol (PPTP) 接続を終端していないことを確認します。ソフトウェアバージョン 7.x は、現在 PPTP 終端をサポートしていません。
3. アップグレードプロセスを開始する前に、VPN 接続用のデジタル証明書をすべて PIX にコピーします。
4. 新しいコマンド、変更されたコマンド、廃止されたコマンドを把握するには、次のドキュメントを参照してください。
 - アップグレードを予定しているソフトウェアバージョンのリリースノートは、『Cisco PIXセキュリティアプライアンスリリースノート』を参照してください。
 - [『Cisco PIX 6.2 および 6.3 ユーザ用 Cisco PIX ソフトウェアバージョン 7.0 アップグレードガイド』](#)
5. ダウンタイム中に移行を実施するようにします。移行は 2 つの手順によるシンプルなプロセスですが、PIX セキュリティ アプライアンスの 7.x へのアップグレードは大きな変更であり、ダウンタイムが必要になります。
6. 7.x ソフトウェアを『[Cisco Software Center](#)』（[登録](#)ユーザ専用）からダウンロードします。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ASA 5500 シリーズ セキュリティ アプライアンス
- PIX セキュリティ アプライアンス 515、515E、525、および 535
- PIX ソフトウェア バージョン 6.3、7.0

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメント表記の詳細については、『[シスコテクニカルティップスの表記法](#)』を参照してください。

手動による設定の変換

手動による変換プロセスでは、テキスト エディタを使用して設定を 1 行ずつ確認し、PIX 固有のコマンドを ASA コマンドに変換します。

PIX 設定を ASA 設定に手動で変換することにより、変換プロセスを非常に詳細に制御できます。ただし、プロセスには時間がかかり、複数の変換を行う必要がある場合に拡張性がありません。

PIX から ASA に移行するには、次の 3 つの手順を実行する必要があります。

1. PIX ソフトウェア バージョンを 7.x にアップグレードします。
2. Cisco PIX ソフトウェア 7.0 から Cisco ASA 形式にインターフェイス名を変換します。
3. PIX ソフトウェア 7.0 の設定を Cisco ASA 5500 にコピーします。

PIX ソフトウェア バージョンの 7.x へのアップグレード

実際にアップグレード プロセスを開始する前に、次の手順を実行します。

1. show running-config コマンドまたは write net コマンドを発行して、PIX の現在の設定をテキスト ファイルまたは TFTP サーバに保存します。
2. RAM などの要件を確認するには、show version コマンドを発行します。また、このコマンドの出力をテキスト ファイルに保存します。前のバージョンのコードへ戻す場合は、元のアクティベーション キーが必要になる場合があります。

PIX が 4.2 よりも前の Basic Input Output System (BIOS) バージョンを搭載している場合や、PIX 515 または PIX 535 を PDM がすでにインストールされている状態でアップグレードする場合は、copy tftp flash による方法ではなく、モニタ モードでアップグレード手順を実行する必要があります。BIOS バージョンを確認するには、PIX を再ブートし、コンソール ケーブルを接続

した状態で、ブート時のメッセージを読み取ります。

BIOS バージョンは、メッセージに次のように表示されています。

```
<#root>
```

```
Rebooting....
```

```
CISCO SYSTEMS PIX FIREWALL
```

```
Embedded BIOS Version 4.3.207
```

```
01/02/02 16:12:22.73
```

```
Compiled by morlee
```

```
64 MB RAM
```

注：6.xコマンドは、アップグレード中に自動的に7.xコマンドに変換されます。コマンドの自動変換により、設定が変更されます。自動変換が要件を満たしていることを確認するには、7.xソフトウェアのブート後に、設定の変更を確認する必要があります。続いて、次回のセキュリティアプライアンスのブート時にシステムが設定を再変換しないように、設定をフラッシュメモリに保存します。

注：システムを7.xにアップグレードした後は、7.xソフトウェアイメージを破損し、モニタモードからシステムを再起動する必要があるため、パスワード回復などのソフトウェアバージョン6.x npディスクユーティリティを使用しないことが重要です。また、以前の設定、セキュリティカーネル、およびキー情報が失われる可能性もあります。

copy tftp flash コマンドによる PIX セキュリティ アプライアンスのアップグレード

copy tftp flash コマンドを使用して PIX をアップグレードするには、次のステップを実行します。

1. PIX アプライアンスのバイナリ イメージ (たとえば pix701.bin) を TFTP サーバのルート ディレクトリにコピーします。
2. イネーブル プロンプトから、copy tftp flash コマンドを発行します。

```
<#root>
```

```
pixfirewall>
```

```
enable
```

```
Password:
```


!!

Image installed
pixfirewall#
pixfirewall#

reload

Proceed with reload? [confirm]

Rebooting...

CISCO SYSTEMS PIX FIREWALL
Embedded BIOS Version 4.3.207 01/02/02 16:12:22.73
Compiled by morlee
128 MB RAM

PCI Device Table.
Bus Dev Func VendID DevID Class Irq
00 00 00 8086 7192 Host Bridge
00 07 00 8086 7110 ISA Bridge
00 07 01 8086 7111 IDE Controller
00 07 02 8086 7112 Serial Bus 9
00 07 03 8086 7113 PCI Bridge
00 0D 00 8086 1209 Ethernet 11
00 0E 00 8086 1209 Ethernet 10
00 13 00 11D4 2F44 Unknown Device 5

Cisco Secure PIX Firewall BIOS (4.2) #0: Mon Dec 31 08:34:35 PST 2001
Platform PIX-515E
System Flash=E28F128J3 @ 0xffff00000

Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 5063168 bytes of image from flash.

128MB RAM

Total NICs found: 2
mcwa i82559 Ethernet at irq 11 MAC: 0009.4360.ed44
mcwa i82559 Ethernet at irq 10 MAC: 0009.4360.ed43
BIOS Flash=am29f400b @ 0xd8000
Old file system detected. Attempting to save data in flash

*!--- This output indicates that the Flash file
!--- system is formatted. The messages are normal.*

Initializing flashfs...
flashfs[7]: Checking block 0...block number was (-27642)
flashfs[7]: erasing block 0...done.
flashfs[7]: Checking block 1...block number was (-30053)
flashfs[7]: erasing block 1...done.
flashfs[7]: Checking block 2...block number was (-1220)

flashfs[7]: erasing block 2...done.
flashfs[7]: Checking block 3...block number was (-22934)
flashfs[7]: erasing block 3...done.
flashfs[7]: Checking block 4...block number was (2502)
flashfs[7]: erasing block 4...done.
flashfs[7]: Checking block 5...block number was (29877)
flashfs[7]: erasing block 5...done.
flashfs[7]: Checking block 6...block number was (-13768)
flashfs[7]: erasing block 6...done.
flashfs[7]: Checking block 7...block number was (9350)
flashfs[7]: erasing block 7...done.
flashfs[7]: Checking block 8...block number was (-18268)
flashfs[7]: erasing block 8...done.
flashfs[7]: Checking block 9...block number was (7921)
flashfs[7]: erasing block 9...done.
flashfs[7]: Checking block 10...block number was (22821)
flashfs[7]: erasing block 10...done.
flashfs[7]: Checking block 11...block number was (7787)
flashfs[7]: erasing block 11...done.
flashfs[7]: Checking block 12...block number was (15515)
flashfs[7]: erasing block 12...done.
flashfs[7]: Checking block 13...block number was (20019)
flashfs[7]: erasing block 13...done.
flashfs[7]: Checking block 14...block number was (-25094)
flashfs[7]: erasing block 14...done.
flashfs[7]: Checking block 15...block number was (-7515)
flashfs[7]: erasing block 15...done.
flashfs[7]: Checking block 16...block number was (-10699)
flashfs[7]: erasing block 16...done.
flashfs[7]: Checking block 17...block number was (6652)
flashfs[7]: erasing block 17...done.
flashfs[7]: Checking block 18...block number was (-23640)
flashfs[7]: erasing block 18...done.
flashfs[7]: Checking block 19...block number was (23698)
flashfs[7]: erasing block 19...done.
flashfs[7]: Checking block 20...block number was (-28882)
flashfs[7]: erasing block 20...done.
flashfs[7]: Checking block 21...block number was (2533)
flashfs[7]: erasing block 21...done.
flashfs[7]: Checking block 22...block number was (-966)
flashfs[7]: erasing block 22...done.
flashfs[7]: Checking block 23...block number was (-22888)
flashfs[7]: erasing block 23...done.
flashfs[7]: Checking block 24...block number was (-9762)
flashfs[7]: erasing block 24...done.
flashfs[7]: Checking block 25...block number was (9747)
flashfs[7]: erasing block 25...done.
flashfs[7]: Checking block 26...block number was (-22855)
flashfs[7]: erasing block 26...done.
flashfs[7]: Checking block 27...block number was (-32551)
flashfs[7]: erasing block 27...done.
flashfs[7]: Checking block 28...block number was (-13355)
flashfs[7]: erasing block 28...done.
flashfs[7]: Checking block 29...block number was (-29894)
flashfs[7]: erasing block 29...done.
flashfs[7]: Checking block 30...block number was (-18595)
flashfs[7]: erasing block 30...done.
flashfs[7]: Checking block 31...block number was (22095)
flashfs[7]: erasing block 31...done.
flashfs[7]: Checking block 32...block number was (1486)
flashfs[7]: erasing block 32...done.
flashfs[7]: Checking block 33...block number was (13559)

flashfs[7]: erasing block 33...done.
flashfs[7]: Checking block 34...block number was (24215)
flashfs[7]: erasing block 34...done.
flashfs[7]: Checking block 35...block number was (21670)
flashfs[7]: erasing block 35...done.
flashfs[7]: Checking block 36...block number was (-24316)
flashfs[7]: erasing block 36...done.
flashfs[7]: Checking block 37...block number was (29271)
flashfs[7]: erasing block 37...done.
flashfs[7]: Checking block 125...block number was (0)
flashfs[7]: erasing block 125...done.
flashfs[7]: inconsistent sector list, fileid 7, parent_fileid 0
flashfs[7]: inconsistent sector list, fileid 12, parent_fileid 0
flashfs[7]: 5 files, 3 directories
flashfs[7]: 0 orphaned files, 0 orphaned directories
flashfs[7]: Total bytes: 16128000
flashfs[7]: Bytes used: 5128192
flashfs[7]: Bytes available: 10999808
flashfs[7]: flashfs fsck took 59 seconds.
flashfs[7]: Initialization complete.

Saving the configuration

!
Saving a copy of old configuration as downgrade.cfg
!
Saved the activation key from the flash image
Saved the default firewall mode (single) to flash
Saving image file as image.bin
!!
!!
Upgrade process complete
Need to burn loader....
Erasing sector 0...[OK]
Burning sector 0...[OK]

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs : 25
Inside Hosts : Unlimited
Failover : Active/Active
VPN-DES : Enabled
VPN-3DES-AES : Enabled
Cut-through Proxy : Enabled
Guards : Enabled
URL Filtering : Enabled
Security Contexts : 2
GTP/GPRS : Disabled
VPN Peers : Unlimited

This platform has an Unrestricted (UR) license.

Encryption hardware device : VAC (IRE2141 with 2048KB, HW:1.0, CGXROM:1.9, FW:6.5)

.
| |
|| |
.|| ||. .|| ||.
.:|| | ||:..:|| | ||:.
C i s c o S y s t e m s

***** Warning *****

This product contains cryptographic features and is subject to United States and local country laws governing, import, export, transfer, and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute, or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning *****

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

!--- These messages are printed for any deprecated commands.

ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 50, "aaa-server LOCAL protoco..."
ERROR: This command is no longer needed. The 'floodguard' feature is always enabled.
*** Output from config line 55, "floodguard enable"

Cryptochecksum(unchanged): 9fa48219 950977b6 dbf6bea9 4dc97255

!--- All current fixups are converted to the new Modular Policy Framework.

INFO: converting 'fixup protocol dns maximum-length 512' to MPF commands
INFO: converting 'fixup protocol ftp 21' to MPF commands
INFO: converting 'fixup protocol h323_h225 1720' to MPF commands
INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands
INFO: converting 'fixup protocol http 80' to MPF commands
INFO: converting 'fixup protocol netbios 137-138' to MPF commands
INFO: converting 'fixup protocol rsh 514' to MPF commands
INFO: converting 'fixup protocol rtsp 554' to MPF commands
INFO: converting 'fixup protocol sip 5060' to MPF commands
INFO: converting 'fixup protocol skinny 2000' to MPF commands
INFO: converting 'fixup protocol smtp 25' to MPF commands
INFO: converting 'fixup protocol sqlnet 1521' to MPF commands
INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands
INFO: converting 'fixup protocol tftp 69' to MPF commands

```
INFO: converting 'fixup protocol sip udp 5060' to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to MPF commands
Type help or '?' for a list of available commands.
pixfirewall>
```

注：PIXが現在7.xソフトウェアバージョンを実行していることを確認するには、show versionコマンドを発行します。

注：設定の移行中に発生したエラーを調べるには、show startup-config errorsコマンドを発行します。エラーはPIXを初めてブートした後にこの出力に表示されます。

モニタ モードからの PIX セキュリティ アプライアンスのアップグレード

モニタ モードに入る

PIX でモニタ モードに入るには、次のステップを実行してください。

1. 次の通信設定を使用して、コンソール ケーブルを PIX のコンソール ポートに接続します。
 - 9600 ビット/秒
 - 8 データ ビット
 - パリティなし
 - 1 ストップ ビット
 - フロー制御なし
2. 電源をオフにしてからオンにするか、PIX をリロードします。起動時に、フラッシュ ブートを中断するには Break キーまたは Esc キーを使用するように指示するプロンプトが表示されます。通常のブート プロセスを中断するための時間は、10 秒あります。
3. ESC キーを押すか、Break 文字を送信すると、モニタ モードに入ります。
 - Windows Hyper Terminal を使用している場合は、ESC キーか、Ctrl+Break キーを押すことで、Break 文字を送信できます。
 - PIX のコンソール ポートにアクセスするために、ターミナル サーバ経由で Telnet を行っている場合は、Telnet のコマンド プロンプトを得るために Ctrl+] (Control + 右角カッコ) を押す必要があります。その後、send break コマンドを発行します。
4. monitor> プロンプトが表示されます。
5. 「モニタ モードからの PIX のアップグレード」セクションに進みます。

モニタ モードからの PIX のアップグレード

モニタ モードから PIX をアップグレードするには、次のステップを実行します。

1. PIX アプライアンスのバイナリ イメージ (たとえば pix701.bin) を TFTP サーバのルート ディレクトリにコピーします。
2. PIX でモニタ モードに入ります。操作方法がわからない場合は、「[モニタ モードに入る](#)」を参照してください。

注：モニタモードに入ったら、「?」キーを使用して使用可能なオプションのリストを表示できます。

3. TFTP サーバが接続されているインターフェイス番号か、TFTP サーバに最も近いインターフェイスを入力します。デフォルトはインターフェイス 1 (内部) です。

```
<#root>  
monitor>  
interface
```

注：モニタモードでは、インターフェイスは常に速度とデュプレックスを自動ネゴシエートします。インターフェイスの設定をハード コードすることはできません。したがって、PIX インターフェイスを速度やデュプレックスがハード コードされているスイッチに接続する場合は、モニタ モードに入っている間に、オート ネゴシエートするようにスイッチを再設定します。また、PIX アプライアンスでは、モニタ モードからギガビット イーサネット インターフェイスを初期化できないことに注意してください。代わりに、ファスト イーサネット インターフェイスを使用する必要があります。

4. 手順 3 で入力したインターフェイスの IP アドレスを入力します。

```
<#root>  
monitor>  
address
```

5. TFTP サーバの IP アドレスを入力します。

```
<#root>
```

```
monitor>
```

```
server
```

6. (オプション) ゲートウェイの IP アドレスを入力します。ゲートウェイ アドレスは、PIX のインターフェイスが TFTP サーバと同じネットワーク上にない場合に必要です。

```
<#root>
```

```
monitor>
```

```
gateway
```

7. ロードする TFTP サーバ上のファイルの名前を入力します。これは PIX のバイナリ イメージのファイル名です。

```
<#root>
```

```
monitor>
```

```
file
```

8. PIX から TFTP サーバに対して ping を実行し、IP の接続性を確認します。

ping に失敗した場合は、ケーブル、PIX インターフェイスと TFTP サーバの IP アドレス、およびゲートウェイの IP アドレス (必要な場合) を再度チェックしてください。以降の手順に進むには、ping が成功する必要があります。

```
<#root>
```

```
monitor>
```

```
ping
```

9. TFTP のダウンロードを開始するには、tftp と入力します。

```
<#root>  
monitor>  
tftp
```

10. PIX によってイメージが RAM にダウンロードされ、RAM が自動的にブートされます。

ブートプロセスの間、ファイルシステムが現在の設定と一緒に変換されます。ただし、作業はまだ完了していません。ブートした後、手順 11 に進む前に、次の警告メッセージに注意してください。

```
*****  
**                                                                 **  
**   *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING *** **  
**                                                                 **  
**           ----> Current image running from RAM only! <---- **  
**                                                                 **  
** When the PIX was upgraded in Monitor mode the boot image was not **  
** written to Flash. Please issue "copy tftp: flash:" to load and **  
** save a bootable image to Flash. Failure to do so will result in **  
** a boot loop the next time the PIX is reloaded. **  
**                                                                 **  
*****
```

11. ブートが完了したら、イネーブル モードに入り、同じイメージを PIX に再度コピーします。今回は copy tftp flash コマンドを発行します。

この操作によって、イメージがフラッシュ ファイル システムに保存されます。この手順を実行しないと、次に PIX がリロードしたときに、ブート時にループに陥ります。

```
<#root>  
pixfirewall>  
enable  
pixfirewall#  
copy tftp flash
```

注：copy tftp flashコマンドを使用してイメージをコピーする方法の詳細については、「copy tftp flashコマンドによるPIXセキュリティアプライアンスのアップグレード」セクションを参照してください。

12. copy tftp flash コマンドを使用してイメージをコピーすれば、アップグレード プロセスは完了です。

設定例：モニタ モードからの PIX セキュリティ アプライアンスのアップグレード

```
<#root>
```

```
monitor>
```

```
interface 1
```

```
0: i8255X @ PCI(bus:0 dev:13 irq:10)
```

```
1: i8255X @ PCI(bus:0 dev:14 irq:7 )
```

```
2: i8255X @ PCI(bus:1 dev:0 irq:11)
```

```
3: i8255X @ PCI(bus:1 dev:1 irq:11)
```

```
4: i8255X @ PCI(bus:1 dev:2 irq:11)
```

```
5: i8255X @ PCI(bus:1 dev:3 irq:11)
```

```
Using 1: i82559 @ PCI(bus:0 dev:14 irq:7 ), MAC: 0050.54ff.4d81
```

```
monitor>
```

```
address 10.1.1.2
```

```
address 10.1.1.2
```

```
monitor>
```

```
server 172.18.173.123
```

```
server 172.18.173.123
```

```
monitor>
```

```
gateway 10.1.1.1
```

```
gateway 10.1.1.1
```

```
monitor>
```

```
file pix701.bin
```

```
file pix701.bin
```

```
monitor>
```

```
ping 172.18.173.123
```

```
Sending 5, 100-byte 0xa014 ICMP Echoes to 172.18.173.123, timeout is 4 seconds:
```

```
!!!!
```

```
Success rate is 100 percent (5/5)
```

```
monitor>
```

```
tftp
```

```
tftp pix701.bin@172.18.173.123.....
```

```
Received 5124096 bytes
```

Cisco PIX Security Appliance admin loader (3.0) #0: Mon Mar 7 17:39:03 PST 2005

#####

128MB RAM

Total NICs found: 6

mcwa i82559 Ethernet at irq 10 MAC: 0050.54ff.4d80

mcwa i82559 Ethernet at irq 7 MAC: 0050.54ff.4d81

mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2014

mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2015

mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2016

mcwa i82558 Ethernet at irq 11 MAC: 00e0.b600.2017

BIOS Flash=AT29C257 @ 0xffffd8000

Old file system detected. Attempting to save data in flash

*!--- This output indicates that the Flash file
!--- system is formatted. The messages are normal.*

Initializing flashfs...

flashfs[7]: Checking block 0...block number was (-10627)

flashfs[7]: erasing block 0...done.

flashfs[7]: Checking block 1...block number was (-14252)

flashfs[7]: erasing block 1...done.

flashfs[7]: Checking block 2...block number was (-15586)

flashfs[7]: erasing block 2...done.

flashfs[7]: Checking block 3...block number was (5589)

flashfs[7]: erasing block 3...done.

flashfs[7]: Checking block 4...block number was (4680)

flashfs[7]: erasing block 4...done.

flashfs[7]: Checking block 5...block number was (-21657)

flashfs[7]: erasing block 5...done.

flashfs[7]: Checking block 6...block number was (-28397)

flashfs[7]: erasing block 6...done.

flashfs[7]: Checking block 7...block number was (2198)

flashfs[7]: erasing block 7...done.

flashfs[7]: Checking block 8...block number was (-26577)

flashfs[7]: erasing block 8...done.

flashfs[7]: Checking block 9...block number was (30139)

flashfs[7]: erasing block 9...done.

flashfs[7]: Checking block 10...block number was (-17027)

flashfs[7]: erasing block 10...done.

flashfs[7]: Checking block 11...block number was (-2608)

flashfs[7]: erasing block 11...done.

flashfs[7]: Checking block 12...block number was (18180)

flashfs[7]: erasing block 12...done.

flashfs[7]: Checking block 13...block number was (0)

flashfs[7]: erasing block 13...done.

flashfs[7]: Checking block 14...block number was (29271)

flashfs[7]: erasing block 14...done.

flashfs[7]: Checking block 15...block number was (0)

flashfs[7]: erasing block 15...done.

flashfs[7]: Checking block 61...block number was (0)

flashfs[7]: erasing block 61...done.

flashfs[7]: inconsistent sector list, fileid 9, parent_fileid 0

flashfs[7]: inconsistent sector list, fileid 10, parent_fileid 0

flashfs[7]: 9 files, 3 directories

flashfs[7]: 0 orphaned files, 0 orphaned directories

flashfs[7]: Total bytes: 15998976

flashfs[7]: Bytes used: 10240

flashfs[7]: Bytes available: 15988736

flashfs[7]: flashfs fsck took 58 seconds.

flashfs[7]: Initialization complete.

product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return the enclosed items immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
<http://www.cisco.com/wwl/export/crypto/tool/stqrg.html>

If you require further assistance please contact us by sending email to export@cisco.com.

***** Warning *****

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

!--- These messages are printed for any deprecated commands.

.ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 71, "aaa-server LOCAL protoco..."
ERROR: This command is no longer needed. The 'floodguard' feature is always enabled.
*** Output from config line 76, "floodguard enable"

Cryptochecksum(unchanged): 8c224e32 c17352ad 6f2586c4 6ed92303

*!--- All current fixups are converted to the
!--- new Modular Policy Framework.*

INFO: converting 'fixup protocol dns maximum-length 512' to MPF commands
INFO: converting 'fixup protocol ftp 21' to MPF commands
INFO: converting 'fixup protocol h323_h225 1720' to MPF commands
INFO: converting 'fixup protocol h323_ras 1718-1719' to MPF commands
INFO: converting 'fixup protocol http 80' to MPF commands
INFO: converting 'fixup protocol ils 389' to MPF commands
INFO: converting 'fixup protocol netbios 137-138' to MPF commands
INFO: converting 'fixup protocol rsh 514' to MPF commands
INFO: converting 'fixup protocol rtsp 554' to MPF commands
INFO: converting 'fixup protocol sip 5060' to MPF commands
INFO: converting 'fixup protocol skinny 2000' to MPF commands
INFO: converting 'fixup protocol smtp 25' to MPF commands
INFO: converting 'fixup protocol sqlnet 1521' to MPF commands
INFO: converting 'fixup protocol sunrpc_udp 111' to MPF commands
INFO: converting 'fixup protocol tftp 69' to MPF commands
INFO: converting 'fixup protocol sip udp 5060' to MPF commands
INFO: converting 'fixup protocol xdmcp 177' to MPF commands

**
** *** WARNING *** WARNING *** WARNING *** WARNING *** WARNING *** **
**
**
** ----> Current image running from RAM only! <---- **

```

**
** When the PIX was upgraded in Monitor mode the boot image was not
** written to Flash. Please issue "copy tftp: flash:" to load and
** save a bootable image to Flash. Failure to do so will result in
** a boot loop the next time the PIX is reloaded.
**
*****
Type help or '?' for a list of available commands.
pixfirewall>
pixfirewall>

enable

Password:

pixfirewall#
pixfirewall#

copy tftp flash

Address or name of remote host []?
172.18.173.123

Source filename []?
pix701.bin

Destination filename [pix701.bin]?

Accessing tftp://172.18.173.123/pix701.bin...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file flash:/pix701.bin...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
5124096 bytes copied in 139.790 secs (36864 bytes/sec)
pixfirewall#

```

Cisco PIX ソフトウェア 7.0 から Cisco ASA 形式へのインターフェイス名の変換

プロセスの次の手順は、新たに変換された Cisco PIX ソフトウェア 7.0 ベースの設定をオフラインで編集することです。

Cisco ASA インターフェイスの命名規則は Cisco PIX セキュリティ アプライアンスとは異なるた

め、Cisco ASA 5500 シリーズ セキュリティ アプライアンスに Cisco PIX 設定をコピー/アップロードする前に、Cisco PIX 設定に変更を加える必要があります。

PIX 設定のインターフェイス名を変更するには、次の手順を実行します。

1. 新しい Cisco PIX ソフトウェア 7.0 ベースの設定をオフラインでコピーします。このためには、設定を TFTP/FTP サーバにアップロードするか、設定をコンソール セッションからテキスト エディタにコピーします。

PIX 設定を TFTP/FTP サーバにアップロードするには、コンソールから次のコマンドを発行します。

```
copy startup^'config tftp://n.n.n.n/PIX7cfg.txt
or
copy startup^'config ftp://n.n.n.n/PIX7cfg.txt
```

2. Cisco PIX ソフトウェア 7.0 ベースの設定ファイルが正常に TFTP/FTP サーバにアップロードされると (または、テキスト エディタにペースト/コピーされると)、メモ帳、ワードパッド、または他のお好みのテキスト エディタを開いて、PIX 設定のインターフェイス名を変更できます。

Cisco PIX セキュリティ アプライアンスのインターフェイス番号は 0 ~ n です。Cisco ASA 5500 シリーズ セキュリティ アプライアンスのインターフェイス番号は、その場所およびスロットに基づいています。組み込みインターフェイスは 0/0 ~ 0/3 であり、管理インターフェイスは Management 0/0 です。4GE SSM モジュールのインターフェイス番号は 1/0 ~ 1/3 です。

7.0 が動作している Base ライセンス付きの Cisco ASA 5510 では、3 個のファスト イーサネット ポート (0/0 ~ 0/2) と Management 0/0 インターフェイスが利用できます。Security Plus ライセンス付きの Cisco ASA 5510 では、5 個のポートすべてでファスト イーサネット インターフェイスが利用できます。Cisco ASA 5520 および 5540 には、4 個のギガビット イーサネット ポートと 1 個のファスト イーサネット管理ポートが搭載されています。Cisco ASA 5550 には、8 個のギガビット イーサネット ポートと 1 個のファスト イーサネット ポートが搭載されています。

PIX 設定のインターフェイス名を ASA インターフェイス形式に変更します。

例 :

```
<#root>
```

```
Ethernet0 ==> Ethernet
```

```
0/0
```

```
Ethernet1 ==> Ethernet
```

0/1

```
GigabitEthernet0 ==> GigabitEthernet
```

0/0

詳細は、『[Ciscoセキュリティアプライアンスコマンドラインコンフィギュレーションガイド、バージョン7.0](#)』の「インターフェイスパラメータの設定」セクションを参照してください。

PIX から ASA への設定のコピー

この時点で、Cisco PIX ソフトウェア 7.0 ベースの設定は、インターフェイス名が変更され、Cisco ASA 5500 シリーズにコピーまたはアップロードできるようになっています。Cisco PIX ソフトウェア 7.0 ベースの設定を Cisco ASA 5500 シリーズ アプライアンスにロードするには、2 つの方法があります。

「[方法1：手動コピー/貼り付け](#)」または「[方法2: TFTP/FTPからのダウンロード](#)」の手順を実行します。

方法1：手動コピー/貼り付け

PIX コンソールからのコピー/ペーストにより、設定をコピーします。

1. 変更した Cisco PIX ソフトウェア 7.0 設定をペーストする前に、コンソールを通じて Cisco ASA 5500 シリーズにログインし、clear config all コマンドを発行して設定をクリアします。

```
<#root>
```

```
ASA#config t
ASA(config)#clear config all
```

2. 設定を ASA コンソールにコピー アンド ペーストし、設定を保存します。

注：テストを開始する前に、すべてのインターフェイスが no shutdown 状態であることを確認してください。

方法2:TFTP/FTPからのダウンロード

2 つ目の方法は、Cisco PIX ソフトウェア 7.0 ベースの設定を TFTP/FTP サーバからダウンロードする方法です。この手順の場合、Cisco ASA 5500 シリーズ アプライアンスの管理インターフェイスを、TFTP/FTP ダウンロード用に設定する必要があります。

1. ASA コンソールから、次のコマンドを発行します。

<#root>

```
ASA#config t
ASA(config)#interface management 0
ASA(config)#nameif management
ASA(config)#ip add
```

```
ASA(config)#no shut
```

注： (オプション) route management <ip> <mask> <next-hop>

2. 管理インターフェイスが設定されたら、PIX 設定を ASA にダウンロードできます。

<#root>

```
ASA(Config)#copy tftp://
```

```
/PIX7cfg.txt running-config
```

3. 設定を保存します。

PIX ソフトウェア バージョン 6.x 設定の ASA ソフトウェア バージョン 7.x への適用

PIX 6.2 または 6.3 設定の新たな ASA セキュリティ アプライアンスへの変換は、手動によるプロセスです。ASA/PIX 管理者は、PIX 6.x 構文を ASA 構文に適合するように変換し、ASA 設定にコマンドを入力する必要があります。access-list コマンドなど、一部のコマンドをカット アンドペーストしてもかまいません。PIX 6.2 または 6.3 設定と新たな ASA 設定を念入りに比較し、変換に間違いがないようにします。

注：[Cisco CLI Analyzer\(登録ユーザ専用\)](#)を使用すると、`apply`、`outbound`、`conduit`などの古いサポート対象外のコマンドを適切なアクセスリストに変換できます。変換された設定文は、十分に確認する必要があります。変換がセキュリティ ポリシーに適合することを確認する必要があります。

注：新しいASAアプライアンスへのアップグレード手順は、新しいPIXアプライアンスへのアップグレード手順とは異なります。ASA へのアップグレードを PIX のプロセスで実行しようとすると、ASA 上で多くの設定エラーが発生します。

トラブルシューティング：手動による設定の変換

デバイスがリブート ループで停止する

- PIX のアップグレードに `copy tftp flash` 方式を使用した後リブートすると、次のようなリブートのループ状態になる。

```
<#root>
```

```
Cisco Secure PIX Firewall BIOS (4.0)
```

```
#0:
```

```
Thu Mar 2 22:59:20 PST 2000
```

```
Platform PIX-515
```

```
Flash=i28F640J5 @ 0x300
```

```
Use BREAK or ESC to interrupt flash boot.
```

```
Use SPACE to begin flash boot immediately.
```

```
Reading 5063168 bytes of image from flash.
```

BIOS バージョンが 4.2 よりも前の PIX アプライアンスは、`copy tftp flash` コマンドを使用する方法でアップグレードすることはできません。モニタ モードによる方法でアップグレードする必要があります。

- PIX で 7.x を実行した後、リブートすると、次のようなリブートのループの状態になる。

```
<#root>
```

```
Rebooting....
```

```
Cisco Secure PIX Firewall BIOS (4.0) #0: Thu Mar 2 22:59:20 PST 2000
```

```
Platform PIX-515
```

```
Flash=i28F640J5 @ 0x300
```

```
Use BREAK or ESC to interrupt flash boot.
Use SPACE to begin flash boot immediately.
Reading 115200 bytes of image from flash.
```

```
PIX Flash Load Helper
```

```
Initializing flashfs...
flashfs[0]: 10 files, 4 directories
flashfs[0]: 0 orphaned files, 0 orphaned directories
flashfs[0]: Total bytes: 15998976
flashfs[0]: Bytes used: 1975808
flashfs[0]: Bytes available: 14023168
flashfs[0]: Initialization complete.
```

```
Unable to locate boot image configuration
```

```
Booting first image in flash
```

```
No bootable image in flash. Please download
an image from a network server in the monitor mode
```

```
Failed to find an image to boot
```

PIX をモニタ モードから 7.0 へアップグレードしたものの、7.0 の初回ブート後に 7.0 のイメージがフラッシュに再コピーされなかった場合は、PIX がリロードされたときにリブートのループ状態になります。

解決策は、モニタ モードからイメージを再ロードすることです。ブート後、copy tftp flash コマンドを使用して、イメージをもう一度コピーする必要があります。

エラー メッセージ

copy tftp flash コマンドを使用する方法でアップグレードすると、次のエラー メッセージが表示される。

```
<#root>
```

```
pixfirewall#
```

```
copy tftp flash
```

```
Address or name of remote host [0.0.0.0]? 172.18.173.123
```

```
Source file name [cdisk]? pix701.bin
```

```
copying tftp://172.18.173.123/pix701.bin to flash:image
```

```
[yes|no|again]? y
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Received 5124096 bytes
```

```
Erasing current image
```

```
Insufficient flash space available for this request:
```

```
Size info: request:5066808 current:1966136 delta:3100672 free:2752512
```

```
Image not installed
```

```
pixfirewall#
```

このメッセージは通常、PDM がすでにインストールされている PIX 515 または PIX 535 を copy tftp flash による方法でアップグレードしたときに表示されます。

モニタ モードによる方法でアップグレードすることで、この問題は解決されます。

設定が正しくない

PIX を 6.x から 7.x へアップグレードした後、一部の設定が正しく移行されない。

show startup-config errors コマンドの出力には、設定の移行中に発生したエラーが表示されます。エラーは PIX を初めてブートした後にこの出力に表示されます。これらのエラーを調べて、解決を試みてください。

FTP などの一部のサービスが機能しない

FTP などの一部のサービスがアップグレード後に機能しないことがあります。

これらのサービスの検査が、アップグレード後に有効化されていません。適切なサービスの検査を有効化します。このためには、これらのサービスをデフォルトのグローバル検査ポリシーに追加するか、対象のサービスについて個別の検査ポリシーを作成します。

検査ポリシーの詳細については、『[Ciscoセキュリティアプライアンスコマンドラインコンフィギュレーションガイド、バージョン7.0](#)』の「アプリケーション層プロトコル検査の適用」セクションを参照してください。

Cisco PIX セキュリティ アプライアンスを Cisco Adaptive Security Appliance (ASA) に置き換えたときにインターネットにアクセスできない

Cisco PIX セキュリティ アプライアンスを Cisco Adaptive Security Appliance (ASA) に置き換えた後にインターネットにアクセスできない場合は、このセクションを使用します。

PIX をネットワークから切断し、PIX の Outside インターフェイスと同じ IP アドレスの Outside インターフェイスを使用して ASA をネットワーク上に接続すると、アップストリーム ルータには Outside インターフェイスの IP アドレスに対応した PIX 用の MAC アドレスがまだ保持されています。結果として、応答パケットを ASA に戻すことができません。ASA を正常に動作させるには、アップストリーム ルータの ARP エントリをクリアし、新しい (正しい) MAC アドレス エントリを学習させる必要があります。PIX を ASA に置き換える際に ARP エントリをフラッシュすることで、インターネット接続の問題は解決されます。ARP エントリのフラッシュは ISP 側で実行する必要があります。

関連情報

- [Cisco PIX 500 シリーズ セキュリティ アプライアンス : 概要](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。