



Migration Guide for Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations

July 2008

Contents

- [Overview, page 1](#)
- [Tool Assisted Configuration Conversion, page 2](#)
- [Manual Configuration Conversion, page 18](#)
- [Related Documentation, page 24](#)
- [Obtaining Documentation, Obtaining Support, and Security Guidelines, page 24](#)

Overview

Although the Cisco PIX 500 Series Security Appliances share a common software foundation with the Cisco ASA 5500 Series Adaptive Security Appliances, you cannot directly use a PIX configuration on an ASA security appliance. Differences between the platforms, such as physical interface names and the use of **outbound** and **conduit** commands, prevent PIX configurations from being used unmodified on ASA security appliances. However, if you are migrating from PIX security appliances to ASA security appliances in your network, you can convert the PIX configuration to an ASA configuration.

There are two ways to convert a PIX configuration to an ASA configuration:

- manual conversion
- tool-assisted conversion

Both methods have their own benefits and weaknesses. Both methods also allow you to perform the configuration conversion offline while your source PIX device remains in service on your network.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2008 Cisco Systems, Inc. All rights reserved.

Manual Conversion Overview

With the manual conversion process, you use a text editor to go through your configuration line-by-line and convert PIX-specific commands to ASA commands.

Manual conversion of the PIX configuration to an ASA configuration gives you the most control over the conversion process. However, the process is time consuming and does not scale well if you must make more than one conversion.

Tool-Assisted Conversion Overview

We recommend that you use the tool-assisted conversion for converting PIX configurations to ASA configurations. This method uses two tools, the Outbound Conduit Conversion Tool and the Cisco PIX-to-ASA migration tool, to convert Cisco PIX Software version 6.3(x), 7.x, or 8.0 configurations to configurations that are usable on a Cisco ASA 5500 Series Adaptive Security Appliance.

The Outbound Conduit Conversion Tool (or optionally the Output Interpreter) converts the **outbound** and **conduit** commands to the equivalent access lists. The Cisco PIX-to-ASA migration tool converts the rest of the configuration to an intermediate configuration that can be processed by the adaptive security appliance.

The tool-assisted conversion method is faster and more scalable if you make multiple conversions. However, the output of the process is an intermediate configuration that contains both old syntax and new syntax. This method relies on installing the intermediate configuration on the target adaptive security appliance to complete the conversion. Until it is installed on the target device, you cannot view the final configuration.

Tool Assisted Configuration Conversion

This section contains the following topics:

- [Before You Begin, page 2](#)
- [Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations, page 7](#)

Before You Begin

Before you begin the conversion process you must familiarize yourself with the important notes, verify the source and target platforms, and install the conversion utilities on your local computer.

This section contains the following topics:

- [Important Notes, page 3](#)
- [Verifying the Source Platform, page 3](#)
- [Verifying the Target Platform, page 3](#)
- [Installing the PIX-to-ASA Migration Tool, page 4](#)
- [Installing the OCC Tool \(Optional\), page 6](#)

Important Notes

- If your Cisco PIX 500 Series Security Appliance is running software version 6.2(x) or earlier you must upgrade to 6.3(x) before starting the conversion process. Converting configurations from software versions earlier than 6.3(x) is not supported.
- PPTP VPN is not supported on software versions 7.x. PPTP commands in the source configuration are marked as comments in the converted configuration with a note that they are not supported.
- Exporting certificates is not supported in PIX 6.3. If you have certificates in your PIX configuration, you must either upgrade to PIX version 8.0 and export the certificates first, or you must obtain a new certificate after the conversion process.
- Serial cable failover is not supported in the ASA platform. Therefore, you must add LAN failover on the ASA after the migration process.
- Physical interface exhaustion—A physical interface must always be mapped one-to-one to a destination physical interface. If interfaces in the source platform exceed the number of available interfaces available in the destination platform, such as migrating from a fully equipped Cisco PIX 535 to an Cisco ASA 5540, those interfaces will be converted to the 7.x syntax but will keep their original interface names.
- Multiple Context Mode—You must manually convert multiple context mode configurations. See [Manual Configuration Conversion, page 18](#).
- VLANs on the Cisco ASA 5505—On an Cisco ASA 5505, the migration tool assigns VLAN 2 to Ethernet 0/0 and VLAN 1 to all other physical interfaces. Typically, VLAN 1 and VLAN 2 provide access to inside and outside interfaces. If you do not assign source interfaces to these VLANs, then the ASA will not have access to the inside and the outside interfaces.

Verifying the Source Platform

The source platform should meet the following requirements:

- Run Cisco PIX Software Version 6.3(x) or later. Use the **show version** command to determine the software version on the device. If the device is running an earlier version of the software, you must upgrade to version 6.3(x) before continuing.
- Run in single mode. If the device is in multiple mode, you must manually convert the configuration. See [Manual Configuration Conversion, page 18](#).

Verifying the Target Platform

To perform the migration, you must have an Cisco ASA 5500 Series Adaptive Security Appliance running Cisco ASA Software Version 7.2. Use the **show version** command or ASDM to determine the software version on the device.



Note

Cisco ASA Software versions earlier than 7.2(2) may also be specified as a target, but features of later versions that are available on some Cisco PIX Software platforms, such as PPPoE, are not supported by earlier Cisco ASA Software versions.

The following hardware platforms are supported:

- ASA-5505
- ASA-5510
- ASA-5520
- ASA-5540
- ASA-5550
- ASA-5580

Installing the PIX-to-ASA Migration Tool

The PIX-to-ASA migration tool is supported on Microsoft Windows 2000 or later, Red Hat Linux dated 2003 or later, or Mac OS X 1.4 or later. You must have Java Runtime Environment version 1.4.2 or later installed. We recommend that you use the latest version of either Java 1.4.2, Java 5 (1.5), or Java 6 (1.6). Java downloads may be obtained from <http://www.java.com/downloads>.



Note

Although the PIX-to-ASA migration tool is supported on Microsoft Windows, Red Hat Linux, and Mac OS X only, it may run on other platforms that support the required versions of Java.



Note

When you download the installation files shown in these instructions, the names of the downloaded installation files may include a version number. For example, you may download and use `PIXtoASASetup_1_0.exe` in the place of the `PIXtoASASetup.exe` file.

Installing on Microsoft Windows

To install the PIX-to-ASA migration tool on Windows, perform the following steps:

-
- Step 1** Download the `PIXtoASASetup.exe` file from the Cisco Software Center at the following URL:
<http://www.cisco.com/public/sw-center/index.shtml>
- Step 2** Double-click the `PIXtoASASetup.exe` file.
The PIX-to-ASA migration tool installation wizard opens.
- Step 3** Click **Next**.
The Destination Folder screen appears. (Optional) To change the install location, perform the following steps:
- a. Click **Change**.
 - b. Browse to the desired install location.
 - c. Click **OK**.
- Step 4** Click **Next**.
The Setup Type screen appears. Select the setup type you prefer, and click **Next**.
You can choose between a complete installation and a custom installation:
- Complete Installation—Installs all components. After clicking next, the Ready to Install Program screen appears. Go to step [Step 6](#).

- Custom Installation—You can choose the components you want installed. After clicking Next, the Custom Setup screen appears. Go to step [Step 5](#).

Step 5 (Optional) Select which components that you do not want installed by clicking the disk icon next to the component, selecting **This feature will not be available**, and then clicking **Next**. Click on a component name to see a description of the component.



Note By default, all features are selected to be installed.

The Ready to Install the Program screen appears.

Step 6 Click **Install**.

Step 7 When the installation is complete, click **Finish** to close the Install Wizard.



Tip To launch the PIX-to-ASA migration tool when you close the wizard, check the Launch PIX-to-ASA migration tool checkbox.

The Install Wizard adds a Cisco PIX-to-ASA migration tool folder to your Start menu. The folder contains shortcuts to the *Migration Guide for Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations* document, the PIX-to-ASA migration tool, and the PIX-to-ASA migration tool uninstaller.

Installing on MAC OS X

To install the PIX-to-ASA migration tool on MAC OS X, perform the following steps:

Step 1 Download the `PIX_to_ASA.dmg` disk image file from the Cisco Software Center.

Step 2 Double-click the `PIX_to_ASA.dmg` disk image file to mount it.

A PIX to ASA folder opens on your desktop. If the folder does not open, double-click the **PIX to ASA** virtual disk icon that is on the desktop.

Step 3 (Optional) Create a directory in which to store a permanent copy of the folder contents.

Although you do not need to keep a copy of the extracted files on your system, keeping a copy of the files may be useful if you plan to use the scripting tools.

Step 4 (Optional) Drag the contents of the folder into the folder you created. You can drag the `PIXtoASA.app` file to the Macintosh Applications folder to install the application.



Note The `.app` and `.dmg` suffixes may not appear with the default system settings.

The archive contains `PIXtoASA.app` (a Macintosh GUI application), an executable JAR for scripts, a Bourne shell script, and the user documentation in PDF format.

Installing on Linux

To install the PIX-to-ASA migration tool on Red Hat Linux, perform the following steps:

-
- Step 1** Download the `PIXtoASA.zip` file from the Cisco Software Center.
 - Step 2** Unpack the file with either the `unzip` or the `gunzip` application to the desired location.
The file contains a PDF file of the user documentation, a Bourne shell script that can be used to launch the application, and an executable JAR file.
-

Installing the OCC Tool (Optional)

The OCC Tool is supported on Microsoft Windows and Sun Solaris only. The OCC tool runs on Windows 95, Windows 98, Windows 2000, Windows XP, and Solaris 2.8 (SunOS 5.8).

If you must convert the **outbound** and **conduit** commands on a Linux or Macintosh workstation, you must use the Output Interpreter. See [Converting the conduit and outbound Commands, page 8](#).

Installing the OCC Tool on Microsoft Windows

To install the OCC tool on Microsoft Windows, perform the following steps:

-
- Step 1** Download the `occ-121.zip` file from the Cisco Software Center.
 - Step 2** Unpack the archive to the desired location on your system.
The archive contains the `occ-121.exe` Windows binary file.
-

Installing the OCC Tool on SUN Solaris

To install the OCC tool on SUN Solaris, perform the following steps:

-
- Step 1** Download the `occ-121.gz` file from the Cisco Software Center.
 - Step 2** Unpack the archive to the desired location on your system.
The archive contains the `occ-121` Solaris binary file.
-

Converting Cisco PIX Configurations to Cisco ASA 5500 Series Configurations

Table 1 provides a summary of the steps necessary to convert your PIX configuration to an ASA configuration.

Table 1 Conversion Process Summary

	Task	See
Step 1	Retrieve the PIX configuration from the device.	Retrieving the PIX Configuration, page 7
Step 2	Convert the PIX conduit and outbound commands.	Converting the conduit and outbound Commands, page 8
Step 3	Convert the PIX configuration to an ASA configuration.	Converting a Cisco PIX Configuration to a Cisco ASA 5500 Series Configuration, page 9
Step 4	View the converted, intermediate configuration.	Viewing the Intermediate Configuration, page 16
Step 5	Complete the conversion process by installing the converted configuration on an ASA 5500 Series Adaptive Security Appliance running 7.0(x), 7.2(x), or 8.x software.	Installing the Intermediate ASA Configuration, page 16
Step 6	(Optional) Configure LAN-based failover (if converting from a serial cable failover configuration).	Configuring LAN-based Failover, page 17
Step 7	Verify the final, converted configuration.	Verifying the ASA Configuration, page 18
Step 8	Deploy your new device.	Deploying the New Device, page 18

Retrieving the PIX Configuration

Retrieve the PIX configuration from the source device, and store it on your local file system. You can retrieve a PIX configuration in the following ways:

- Enter the URL **https://ip_address/config** into the address field of a web browser, and copy the displayed PIX configuration into a plain text file. The *ip_address* is the IP address of a PIX security appliance that is reachable by PDM or Cisco ASDM.
- Use the **write net** or **copy running-config [tftp/ftp]** command (which requires an available server to receive the configuration). These commands transfer information in cleartext. Do not use them over insecure networks.
- Begin with Cisco ASDM Version 5.0, ASDM may transfer a copy of the startup config to the local computer through the menu item **Tools > File Management > File Transfer**.



Note

The conversion process does not modify the configuration on the source device. The source device can remain in operation on your network while you convert the configuration and apply the configuration to the target device.

Do not use the **show config**, **show running-config**, or **show running-config all** commands to retrieve the configuration. These commands obscure passwords with asterisks (*) and may not display information that PDM or Cisco ASDM uses to maintain network object and group names. Using those commands may also display the configuration with unwanted line wrapping or the --- MORE --- prompt embedded in the output, both of which can introduce errors in the converted configuration.

Converting the conduit and outbound Commands

The recommended method for converting **conduit** and **outbound** commands is to use the OCC tool. However, the OCC tool is only supported on Windows and Solaris. To convert **conduit** and **outbound** commands on Linux or Macintosh, you must use the online Output Interpreter tool. See <https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl>.



Note

Using the Output Interpreter requires you to upload your configuration to a Cisco server.

A conduit permits connections from one network interface to access hosts on another. The OCC tool checks for overlaps between the global address of the conduit and each of the following:

- Global address in statics on the interface.
- Pool address(es) in globals on the interface.
- Local address in nat 0s or nat 0 access-lists on higher security-level interfaces.
- Interface address.



Note

When a **nat 0** command exists on an interface, any conduits matching the **nat 0** are converted to ACL entries. These ACL entries are then applied to all interfaces that have a lower security level, unless a **global** or **static** command matches the local addresses in the **nat 0** or **nat 0 access-list** command or it can be determined from the available routing information that the traffic belongs to a particular interface.



Note

When **dhcp setroute** or **pppoe setroute** is applied to the outside interface, a default route to the outside interface is added to the routing information.

If no overlaps apply, the OCC tool does not create an ACL entry for the conduit on that particular interface.

An outbound list is based on the source IP address, the destination IP address, and the destination port or protocol, as specified by the access rules. Outbound lists control Internet use by specifying the following:

- If inside users can create outbound connections
- If inside users can access specific outside servers
- What services are available to inside users for outbound connections and for accessing outside servers

The PIX security appliance uses an algorithm to determine which outbound command to apply to a given incoming packet. Packets are denied by either the `outgoing_src` list or the `outgoing_dst` list. The OCC tool considers an outbound command with a narrower address mask to be a better match, regardless of the service. If the address masks are equal, a more specific service is a better match.

To convert conduit and outbound commands using the OCC tool, perform the following steps:

-
- Step 1** Open a command prompt (Windows) or xterm (Solaris) window.
- Step 2** Change directory to the path from which you extracted the OCC tool.
- Step 3** Enter the following command:

```
occ old_config new_config
```

The *old_config* argument is the configuration file retrieved from the PIX security appliance. The *new_config* argument is the name you want the tool to use when it generates the changed configuration file.

The tool creates a new configuration file with the **outbound** and **conduit** commands converted to the appropriate ACL configurations. Use this new configuration file for the rest of the conversion process.

Converting a Cisco PIX Configuration to a Cisco ASA 5500 Series Configuration

The Cisco PIX to ASA migration tool supports both GUI and CLI-based operation, giving administrators flexibility in how they use this tool. The graphical interface guides administrators through the entire process, from selecting input/output files, to selecting the migration target platform, to mapping network interfaces, and then to generating the newly migrated configuration. The CLI enables the same capabilities, but it gives administrators the ability to create scripts to easily perform bulk migrations. This tool helps to expedite the migration process and to prevent administrators from making common mistakes when performing manual migrations.

The following methods can be used to convert the configuration from PIX to ASA:

- [Using the GUI](#)—Recommended for a smaller number of devices.
- [Using the CLI Syntax](#)—Recommended for a larger number of devices.

Using the GUI

We recommend that you use the GUI for converting the PIX configuration to ASA. The GUI provides all of the capabilities of the CLI. Unlike the command line tool, all GUI interface configuration input and output occurs through files, rather than process standard input, output, and error output.

To migrate a PIX security appliance to an ASA security appliance using the GUI, perform the following steps:

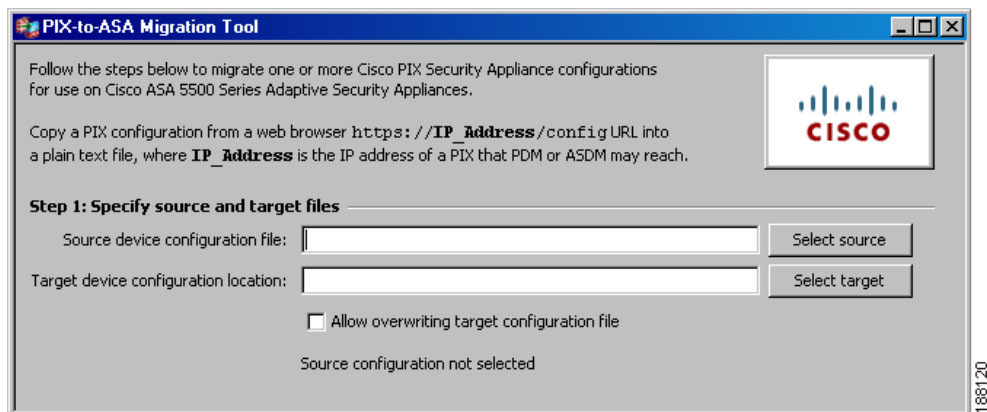
-
- Step 1** Launch the GUI:
- On Windows, click **Start > All Programs > Cisco ASA-to-PIX Migration Tool > PIX-to-ASA Migration Tool**, or double-click the desktop icon, if it is installed. You can also double-click the file **PIXtoASA.exe** file.
 - On MAC OS X, double-click **PIXtoASA.app**.
 - On all platforms, enter the following command from a terminal session or command line prompt:
java -jar PIXtoASA.jar -gui



Note You can use additional CLI parameters to pre-populate the GUI interface when launching the GUI from the command line. See [Populating the GUI Using CLI Options](#), page 13.

Step 2 Specify the location of the input and output files. (See [Figure 1.](#))

Figure 1 Specify Source and Target Files



- a. Click the **Select source** button to choose the source PIX configuration file, or type the full path to the file in the source field. After a source configuration file is specified, the content of the file is scanned.



Note If you change the source configuration file, you must click the **Rescan source configuration** button so that the new file is scanned.

- b. Click the **Select target** button to choose the target device configuration filename or directory. Use a different filename for the target from the source. When specifying a folder for the target location, the filename of the converted configuration will be the same as the source filename unless it resides in the same folder as the source file. In that case, an error message will be shown. After a target is specified, the target filename is verified to be different from the source name.



Note The **Allow overwriting target configuration file** check box allows the target configuration file to be overwritten if it exists. This check box is disabled by default to prevent the overwriting of an existing target file.

If the results of the source configuration file scan contain warnings for unsupported commands, you are not permitted to proceed unless you check the **Allow unsupported apply, conduit, and outbound commands** button.



Caution Enabling the Allow unsupported apply, conduit, and outbound commands option overrides the protection. You should only override the protection if there are very few conduits, such as ICMP. If there are a significant number of conduits and outbound commands, do not proceed. Instead, use the OCC tool to convert the Outbound/Conduit statements into ACLs, and then migrate your PIX configuration. See [Converting the conduit and outbound Commands, page 8.](#)

Step 3 Specify a target device type from the list box. (See [Figure 2.](#))

Figure 2 Specify Target Device Type

Step 2: Specify target device type

Target device type:

No target device type selected

188121

Target device types are specified because of the differences in the number of available interfaces.

You may choose from the following list of target device types:

- ASA 5505 with base license
- ASA 5505 with plus license
- ASA 5510 with base license before 7.2(2)
- ASA 5510 with plus license before 7.2(2)
- ASA 5510 7.2(2) or after
- ASA 5520 before 7.2(2)
- ASA 5520 7.2(2) or after
- ASA 5540 before 7.2(2)
- ASA 5540 7.2(2) or after
- ASA 5550
- ASA 5580

Step 4 Select the interface modules or cards that are installed in each slot. (See [Figure 3](#).)

Figure 3 Specify Interface Cards in Device Slots

Step 3: Specify any interface cards in device slots of target ASA 5510 with plus license before 7.2(2)

SSM slot 1:

188117

For each available slot of the device type, the potential interface card names are listed, if any. Cards without external interfaces are not listed.



Note You cannot configure interface cards for certain devices that do not apply. The Cisco ASA 5505 has a slot, but no card. The Cisco ASA 5550 has a card, but it cannot be changed.

Step 5 Specify interface mappings. (See [Figure 4](#).)

Figure 4 Specify Interface Mappings

Step 4: Specify interface mappings from PIX version 6.3(5) to ASA 5510 with plus license before 7.2(2)

Source interfaces:	Target interfaces
ethernet0: (outside)	<input type="text" value="Ethernet0/0"/>
ethernet1: (inside)	<input type="text" value="Ethernet0/1"/>

188118

Each interface found in the source configuration file is shown with a drop-down list of the target device type interfaces and its interface cards in slots. An attempt is made to match the fastest source interfaces with the fastest target interfaces in the expected order by listing the potentially fastest interfaces with the lowest port number first.

Except for the Cisco ASA 5580, which may be specified only with Management interfaces, Management interfaces are not initially selected because they are not intended for ordinary use for through-the-box traffic. If the target device does not have enough interfaces to be matched uniquely with source interfaces, any remaining source interfaces are mapped to the last acceptable target interface. In this case, you must explicitly specify which source interfaces will map to either a Management interface or to no target interface. To avoid possible misconfiguration, an alert appears for duplicate mappings.



Caution

Be careful to verify whether or not an interface is being used before you specify that it is not used.

Step 6 (Optional) Specify a boot path for an ASA image. (See [Figure 5](#).)

Figure 5 Specify Path to Preferred Boot Image



Even through the configuration file may not specify a boot image, the ASA ROM configuration may specify a boot image from a previous **write memory** operation.

If the ASA configuration specifies no boot images, the first image found is used while reloading.

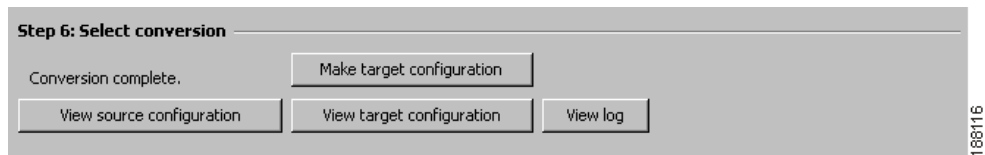
Step 7 Convert a PIX configuration into an ASA configuration by clicking **Make target configuration**. The log file appears.



Note

If this is your first conversion, all of the buttons might not be available for you to select. The View target configuration and View log buttons are available only when the corresponding file exists. Upon your first conversion the buttons are enabled if the files already exist; however, all buttons should be available upon subsequent conversions. (See [Figure 6](#).)

Figure 6 Initiate Conversion



During the conversion a status bar shows the percentage of the configuration that has completed. When conversion has finished, a message appears to inform you that the conversion has completed or has failed with an exception. If the conversion fails, the exception information is appended to the log.

You can view the source configuration, target configuration, and log files if they exist. When the viewing files are opened or reopened, the contents are refreshed from the corresponding file.

If you want to convert more than one source configuration file during a session, return to the step that specifies the source file and input a new file.

Populating the GUI Using CLI Options

When launching the GUI from the CLI, you may use the following optional parameters to prepopulate the GUI:

- To force the GUI interface to appear (if other command line arguments are used when executing the PIXtoASA.jar):
[-gui]
- To specify the source filename:
[-f *input_file* | --input-file=*input_file*]
- To specify the target filename:
[-o *output_file* | --output-file=*output_file*]
- To specify the log filename:
[-l *log_file* | --log-file=*log_file*]
- To append the log file:
[-a *log_file* | --append-log-file=*log_file*]
- To select the check box that allows the target file to be overwritten:
[-overwrite]
- To specify the console, which is used for troubleshooting purposes:
[-console]

Using the CLI Syntax

To migrate a PIX security appliance to an ASA security appliance using the command line interface, use the following command at the command prompt:



```
java -jar PIXtoASA.jar [options]
```



Note

If the directory where the command is being entered does not contain the PIXtoASA.jar file, then you must enter the full path to the file. If the path contains spaces, enclose the path name in double quotation marks (“”).

Optional Parameter	Description
[-7]	Specifies that your source PIX configuration is 7.x or later. This information is useful when only interface mapping conversion is necessary.
[-f <i>input_file</i> --input-file= <i>input_file</i>]	Specifies the input file.
[-o <i>output_file</i> --output-file= <i>output_file</i>]	Specifies the output file to which the converted output is saved. If the output files already exists, it will be overwritten.

Optional Parameter	Description
<code>[-l log_file --log-file=log_file]</code>	Specifies the log file to which errors and warnings are redirected. Warnings are generated as inline comments in the converted configuration, as well as in the log file, if specified, for example, if a feature is not supported on the new platform or if functionality has been retired. If a log file already exists, it will be overwritten or extended according to the use of the -l or -a keywords.
<code>[-a log_file --append-log-file=log_file]</code>	Specifies that new output to the log file is appended to the end of the existing log file.
<code>[-v --version]</code>	Specifies the version of the migration tool engine.
<code>[-t platform --target-platform=platform]</code>	Specifies either asa-5505 , asa-5510 , asa-5520 , asa-5540 , asa-5550 , or asa-5580 target platform values. The configuration is converted to the specified bundled default platform. If target platform is specified, then you cannot specify explicit interface mappings using the -m keyword.  Note If a bundled default platform is specified with an explicit interface mapping, the application is terminated and an error message appears, stating that the -t target-platform and the -m map-interface specifications are mutually exclusive.
<code>[-T 7.0 --target-version=7.0]</code>	Specifies the version of the ASA software running on the target platform.
<code>[-m src_int@dst_int --map-interface=src_int@dst_int]</code>	Specifies explicit interface mappings. Source interface values include ethernet [0-9] or gb-ethernet[0-9] . If explicit interface mappings are specified, then you cannot specify a bundled target platform using the -t keyword. It is necessary to specify the complete list of interface mappings needed to be mapped. Existing interface mappings that are not specified are converted into new syntax only and are not mapped.  Note Mapping a physical source interface to a logical or sub interface is not supported. If this is performed, you need to complete the mapping manually.
<code>[-5]</code>	Specifies to produce an ASA 5505 switchport configuration.
<code>[-b boot_system_file]</code>	Specifies the image file the ASA should boot, disk0:/path/filename , disk1:/path/filename , flash:/path/filename , or tftp://url .
<code>[-h --help]</code>	Shows all command parameters available.

Example

The following example shows how to run the Java, non-GUI mode, of the tool, specifying the target platform as an ASA-5540 and redirecting the source PIX configuration into the tool:

```
java -jar PIXtoASA.jar -t asa-5540 < PIX501config.txt
```

```
INFO: PIX to ASA conversion tool $Revision: 1.9 $
INFO: PIX Version 6.3(4) Removed from config
INFO: fixup protocol sip udp 5060 Removed from config
WARNING: The configuration is NOT supported - floodguard enable
WARNING: Your password is set to all STARS(*) Please Correct before deploying to the new
device! 'vpdn username cisco password ***** '
INFO: Cryptochecksum:e136533e23231c5bfff4088cee75a5a Removed from config
INFO: : end Removed from config
INFO: The destination platform is: asa-5540

INFO: Interface Mapping:
'ethernet0'->'GigabitEthernet0/0'
'ethernet1'->'GigabitEthernet0/1'
```

Additional Files Provided

Two additional files are provided for your convenience. Each contains the `java -jar PIXtoASA.jar` command and can be used to invoke scripts.

- `PIXtoASA.bat`—For Windows platforms
- `pixtoasa.sh`—For Red Hat Linux and Macintosh platforms

These files must be in the same directory as the `PIXtoASA.jar` file in order to call the file correctly.

Bundled Platforms

When using bundled platforms with fixed configurations to map interfaces, the source platform interface is automatically mapped to the next available destination platform interface on a first-come first-served basis. The target platform is specified using the keyword `-t` in the CLI syntax.

[Table 2](#) lists the ASA platform interface mappings.

Table 2 ASA Platform Interface Mappings

ASA Model	Interface Mapping
ASA-5505	<ul style="list-style-type: none"> • VLAN2 (outside) • VLAN1(inside) • VLAN3-8
ASA-5510	<ul style="list-style-type: none"> • Ethernet0/0-4 • GigabitEthernet1/0-3
ASA-5520	<ul style="list-style-type: none"> • GigabitEthernet0/0-3
ASA-5540	<ul style="list-style-type: none"> • GigabitEthernet1/0-3
ASA-5550	
ASA-5580	<ul style="list-style-type: none"> • GigabitEthernet3/0-3 • GigabitEthernet4/0-3 • GigabitEthernet6/0-3

Explicit Interface Mapping

When using explicit interface mapping to map interfaces, you must specify a complete interface mapping scheme, including the full names of all interfaces involved. Explicit interface mapping is specified using the keyword **-m** in the CLI syntax.

In the following example, ethernet0 is mapped to gigabitethernet0/0, and ethernet1 is mapped to gigabitethernet0/1:

```
java -jar PIXtoASA.jar -t asa-5540 -m ethernet0@gigabitethernet0/0 -m
ethernet2@gigabitethernet0/1
```



Note

The above example appears on the screen as a single line with a space between the **-m** and the ethernet2@gigabitethernet0/1.

Viewing the Intermediate Configuration

You can view the intermediate configuration in two ways:

- Using the GUI interface—View the source configuration file, view the target configuration file, then compare the two.
- Using the CLI—Use a text application tool to view the differences between the files. This method is preferred for large configuration files.



Note

The intermediate configuration is a hybrid configuration that contains elements of the old configuration and the new configuration. The conversion to an ASA configuration is not completed until it is installed on an ASA security appliance.

Warnings are generated as inline comments in the converted configuration. You receive warnings if the following apply:

- The new platform contains features that are not supported.
- The new platform contains features that have been deprecated.
- A configuration contains a password that is blanked out with stars (*), which may occur if an administrator copied the configuration from a PIX security appliance using the **show running-configuration** command.

Installing the Intermediate ASA Configuration

The intermediate configuration generated by the tool must be loaded into the startup configuration on an ASA device for final conversion by the platform. (If loaded into the running configuration, some intermediate CLI might not be correctly converted.) It can also be imported into Cisco Security Manager (CSM) or the Cisco Adaptive Security Device Manager (ASDM).

See the *Command Line Configuration Guide* for your target version of ASA software for more information about configuring your device for CLI or ASDM access:

http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html

To install the intermediate ASA configuration and complete the conversion process, perform the following steps:

-
- Step 1** Transfer the configuration file to the ASA.
- Using ASDM, select the **File Management** option in the **Tools** menu.
 - Using the CLI, use the **copy** command to the TFTP or FTP server.
- Step 2** Copy the configuration file into the startup-config.
- Using ASDM, select the **File Management** option in the **Tools** menu. Be sure to specify the **no confirm** option.
 - Using the CLI, use the **copy** command:
- ```
copy disk0:/startupconfigfilename startup-config
```




---

**Note** The conversion of the configuration occurs when the configuration is loaded during startup.

---



**Caution**

Do not use the **write memory** command or, if prompted during the next step, overwrite the startup configuration with the running configuration. Doing so will overwrite the newly installed configuration.

---

- Step 3** Reload the ASA.
- Using ASDM, select the **Reload** option in the Tools menu. When prompted, do **not** save the configuration and reload.
  - Using the CLI, **reload** and then specify that you do **not** want to save the configuration.
- 

## Configuring LAN-based Failover

If you converted from a PIX security appliance that used serial cable failover, you will need to add LAN-based failover commands to the configuration.

To enable LAN-based failover, perform the following steps:

- 
- Step 1** Specify the interface to be used as the failover interface:

```
hostname(config)# failover lan interface if_name phy_if
```

The *if\_name* argument assigns a name to the interface specified by the *phy\_if* argument. The *phy\_if* argument can be the physical port name, such as Ethernet0/1, or a previously created subinterface, such as Ethernet0/2.3. On the Cisco ASA 5505 Adaptive Security Appliance, the *phy\_if* specifies a VLAN.

- Step 2** Assign the active and standby IP address to the failover link:

```
hostname(config)# failover interface ip if_name ip_addr mask standby ip_addr
```

The standby IP address must be in the same subnet as the active IP address. You do not need to identify the standby address subnet mask.

The failover link IP address and MAC address do not change at failover. The active IP address for the failover link always stays with the primary unit, while the standby IP address stays with the secondary unit.

**Step 3** Enable the interface:

```
hostname(config)# interface phy_if
hostname(config-if)# no shutdown
```

See the *Command Line Configuration Guide* for your target version of Cisco ASA Software for more information about configuring LAN-based failover:

[http://www.cisco.com/en/US/products/ps6120/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html)

## Verifying the ASA Configuration

There are several ways that you can confirm the accuracy of the new ASA configuration. Use the command **show startup-config errors** to view any errors the ASA detected as it booted. The command **show running-config tech** is also useful for confirming your ASA configuration.

You may also view the new configuration in ASDM. In ASDM, you should verify the access lists, configured hardware ports, interfaces, and inspections. From the CLI, you should use the commands **show run interface**, **show access lists**, and check the inspections to verify they have been configured correctly.

Finally, you should test the configuration for the desired behavior. You can use the **packet-tracer** command, or you can use the Packet Tracer utility in the ASDM **Tools** Menu.

## Deploying the New Device

Once you have verified the new configuration, put the new device into production. The new device should have the same IP addresses as the PIX security appliance being replaced. You should remove the PIX security appliance from the network before bring the new device online to avoid address conflicts.

# Manual Configuration Conversion

Table 3 provides a summary of the steps needed to convert your PIX configuration to an ASA configuration.

**Table 3** Manual Conversion Process Summary

|               | Task                                                                               | See                                                       |
|---------------|------------------------------------------------------------------------------------|-----------------------------------------------------------|
| <b>Step 1</b> | Retrieve the PIX configuration from the device.                                    | <a href="#">Retrieving the PIX Configuration, page 19</a> |
| <b>Step 2</b> | Open the configuration in a text editor and manually change the required commands. | <a href="#">Mapping Commands Manually, page 19</a>        |
| <b>Step 3</b> | Deploy your new device.                                                            | <a href="#">Deploying the New Device, page 24</a>         |

## Retrieving the PIX Configuration

Retrieve the PIX configuration from the source device and store it on your local file system. You can retrieve a PIX configuration in the following ways:

- Using a web browser, enter the URL **https://ip\_address/config** into the address field, and copy the displayed PIX configuration into a plain text file. The *ip\_address* is the IP address of a PIX that is reachable by PDM or ASDM.
- Using the **write net** or **copy running-config [tftp/ftp]** command (which requires an available server to receive the configuration). These commands transfer information in cleartext. Do not use them over insecure networks.
- Beginning with ASDM version 5.0, ASDM may transfer a copy of the startup config to the local computer through the menu item **Tools > File Management > File Transfer**.



### Note

The conversion process does not modify the configuration on the source device. The source device can remain in operation on your network while you convert the configuration and apply the configuration to the target device.

Do not use the **show config**, **show running-config**, or **show running-config all** commands to retrieve the configuration. These commands obscure passwords with asterisks (\*) and may not display information that PDM or ASDM uses to maintain network object and group names. Using those commands may also display the configuration with unwanted line wrapping or the --- MORE --- prompt embedded in the output, both of which can introduce errors in the converted configuration.

## Mapping Commands Manually

Performing a manual conversion is the most time-consuming method, yet it allows for the most control over the conversion. The manual conversion includes following sections:

- [Interface Mapping, page 19](#)
- [FIXUP Conversion, page 21](#)
- [LAN-Based Failover, page 21](#)
- [Dynamic Interface Addressing, page 23](#)
- [Multiple Context Mode Configuration Conversion, page 23](#)

## Interface Mapping

One of the major functions of the conversion is to map the interface names of the PIX security appliance, which are ethernet0 and gb-ethernet0, to the ASA security appliance naming that is based on chassis slot number and interface number such as: Ethernet0/0, GigabitEthernet0/0, GigabitEthernet1/0, for example.

Remapping of interfaces can be performed manually, but the task can be time consuming and prone to error. The Cisco PIX to ASA migration tool automates this process.

There are two ways of mapping interfaces using the PIX to ASA migration tool:

- Bundled platforms with fixed configurations
- Explicit interface mapping scheme

**Note**

The Cisco ASA 5505 is unique in that the source interfaces are mapped into VLAN interfaces on the built-in switch. The same interface naming convention is used as the default Cisco ASA 5505, where the outside interface is named VLAN2 and the inside is named VLAN1.

By default, switch interface Ethernet0/0 is mapped as an access port in VLAN2. The rest of the interfaces on the switch are access ports in VLAN1. If the source platform has more interfaces than that, it is necessary to manually change the switch configuration to reflect the proper VLAN-to-switch port mapping.

The ASA platform, and all PIX 7.x and higher, define interface characteristics via sub commands under the interface as known from IOS. The source platform interface characteristics are automatically represented as the proper interface sub commands.

In pre 7.0 software interfaces names, logical names, ip addresses, network masks failover ip addresses are all configured as separate commands scattered throughout the configuration. In 7.x and forward all this information is configured in the IOS way of interface and sub commands under the interface.

[Table 1](#) lists the sample converted interface constructs from PIX/ASA version 6.3 to PIX/ASA version 7.2(2).

**Table 4**      **Interface Constructs**

| <b>PIX 6.3 interface configuration<br/>(before conversion)</b>                                                                                                                                                                                                                                           | <b>ASA 7.2(2) interface configuration<br/>(after conversion)</b>                                                                                                                                                                                                                                                             |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Static IP and failover:<br><br><pre>interface ethernet0 auto nameif ethernet0 outside security0 ip address outside 192.168.2.1 255.255.255.0 failover ip address outside 192.168.2.2</pre>                                                                                                               | <pre>interface GigabitEthernet0/0   ip address 192.168.2.1 255.255.255.0 standby 192.168.2.2   nameif outside   security-level 0</pre>                                                                                                                                                                                       |
| VLAN:<br><br><pre>interface gb-ethernet2 1000auto interface gb-ethernet2 vlan50 logical nameif vlan50 vlan50 security10 ip address vlan50 50.1.1.1 255.0.0.0</pre>                                                                                                                                       | <pre>interface GigabitEthernet0/0   no shutdown interface GigabitEthernet0/0.50   vlan 50   ip address 50.1.1.1 255.0.0.0   nameif vlan50   security-level 10</pre>                                                                                                                                                          |
| Dynamic IP address through DHCP:<br><br><pre>interface ethernet0 10baset nameif ethernet0 outside security0 ip address outside dhcp setroute</pre>                                                                                                                                                       | <pre>interface GigabitEthernet0/0   no ip address   no shutdown   ip address dhcp setroute   nameif outside   security-level 0</pre>                                                                                                                                                                                         |
| Dynamic IP address through PPPOE:<br><br><pre>interface ethernet0 10baset nameif ethernet0 outside security0 ip address outside pppoe setroute vpdn group pppoex request dialout pppoe vpdn group pppoex localname cisco vpdn group pppoex ppp authentication pap vpdn username cisco password xxx</pre> | <pre>interface GigabitEthernet0/0   ip address pppoe setroute   pppoe client route distance 2   pppoe client vpdn group pppoex   nameif outside   security-level 0 vpdn group pppoex request dialout pppoe vpdn group pppoex localname cisco vpdn group pppoex ppp authentication pap vpdn username cisco password xxx</pre> |

## FIXUP Conversion

In ASA 7.x, application inspection was introduced as inspection maps and the inspect syntax; this is defined in software versions prior to 7.0 as fixups.

FIXUPs for standard ports are converted into the global inspection policy, as shown in [Table 5](#). FIXUPs on other ports are retained in their FIXUP format and left to be converted by the platform or CSM. Those platforms will create separate class maps and inspection-maps for their corresponding FIXUP.

[Table 5](#) lists sample FIXUP conversion commands from PIX/ASA version 6.3 to PIX/ASA version 7.2(2).

**Table 5**      *FIXUP Conversion*

| <b>PIX/ASA 6.3 commands<br/>(before conversion)</b> | <b>PIX/ASA 7.2(2) commands<br/>(after conversion)</b> |
|-----------------------------------------------------|-------------------------------------------------------|
| fixup protocol dns maximum-length 512               | policy-map type inspect dns preset_dns_map            |
| fixup protocol ftp 21                               | parameters                                            |
| fixup protocol h323 h225 1720                       | message-length maximum 512                            |
| fixup protocol h323 ras 1718-1719                   | policy-map global_policy                              |
| fixup protocol http 80                              | class inspection_default                              |
| fixup protocol rsh 514                              | inspect dns preset_dns_map                            |
| fixup protocol rtsp 554                             | inspect ftp                                           |
| fixup protocol sip 5060                             | inspect h323 h225                                     |
| fixup protocol sip udp 5060                         | inspect h323 ras                                      |
| fixup protocol skinny 2000                          | inspect http                                          |
| fixup protocol smtp 25                              | inspect rsh                                           |
| fixup protocol sqlnet 1521                          | inspect rtsp                                          |
| fixup protocol tftp 69                              | inspect sip                                           |
|                                                     | inspect skinny                                        |
|                                                     | inspect smtp                                          |
|                                                     | inspect sqlnet                                        |
|                                                     | inspect tftp                                          |

## LAN-Based Failover

PIX failover configuration is converted to ASA failover syntax. Failover IP address section (standby IP addresses) are also converted.



**Note**

Serial failover is not supported on the ASA platform, nor is it automatically converted to LAN failover by the PIX to ASA migration tool. Therefore, you should manually convert serial failover to LAN failover on the source platform before starting the conversion process.

**Example**

The following example is a PIX LAN Failover Configuration Conversion.

PIX 6.3(5) configuration (before conversion):

```
interface gb-ethernet0 1000auto
interface gb-ethernet1 1000auto
interface gb-ethernet2 1000auto
interface gb-ethernet2 vlan50 logical
interface gb-ethernet2 vlan55 logical
interface ethernet0 100full
interface ethernet1 100full
nameif gb-ethernet0 outside security0
nameif gb-ethernet1 inside security100
nameif gb-ethernet2 dmz security8
nameif ethernet0 eng security4
nameif ethernet1 mkt security4
nameif vlan50 vlan50 security10
nameif vlan55 vlan55 security12
ip address outside 5.5.5.45 255.255.255.0
ip address inside 14.36.8.48 255.255.0.0
ip address dmz 1.1.1.6 255.255.255.0
ip address mkt 2.2.2.2 255.255.255.0
ip address vlan50 50.1.1.1 255.0.0.0
failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 5.5.5.68
failover ip address inside 14.36.199.34
failover ip address mkt 2.2.2.4
failover ip address vlan50 50.1.1.2
failover lan unit primary
failover lan interface mkt
failover link vlan55
failover lan enable
```

Converted ASA configuration:

```
interface GigabitEthernet0/0
 ip address 5.5.5.45 255.255.255.0 standby 5.5.5.68
 nameif outside
 security-level 0
: Original Interface id gb-ethernet1
interface GigabitEthernet0/1
 ip address 14.36.8.48 255.255.0.0 standby 14.36.199.34
 nameif inside
 security-level 100
: Original Interface id gb-ethernet2
interface GigabitEthernet0/2
 ip address 1.1.1.6 255.255.255.0
 nameif dmz
 security-level 8
: Original Interface id gb-ethernet2_50
interface GigabitEthernet0/2.50
 vlan 50
 ip address 50.1.1.1 255.0.0.0 standby 50.1.1.2
 nameif vlan50
 security-level 10
: Original Interface id gb-ethernet2_55
interface GigabitEthernet0/2.55
 vlan 55
 no ip address
 no shutdown
: Original Interface id ethernet0
```

```

interface GigabitEthernet0/3
 no ip address
 no shutdown
 nameif eng
: Original Interface id ethernet1
: Failover
interface GigabitEthernet1/0
 security-level 4
failover
failover timeout 0:00:00
::: your failover poll timer syntax has been corrected from 'failover poll 15' to
'failover polltime 15'
failover polltime 15
failover lan unit primary
:::failover lan interface mkt -> failover lan interface mkt GigabitEthernet1/0
failover lan interface mkt GigabitEthernet1/0
failover interface ip mkt 2.2.2.2 255.255.255.0 standby 2.2.2.4
:::failover link vlan55 -> failover link vlan55 GigabitEthernet0/2.55
failover link vlan55 GigabitEthernet0/2.55
failover interface ip vlan55 0.0.0.0 0.0.0.0 standby 0.0.0.0
::: Not supported - failover lan enable

```

## Dynamic Interface Addressing

Interface IP addressing is supported on the PIX platform as static address assignment and as dynamic addressing for DHCP and PPPOE.

## Multiple Context Mode Configuration Conversion

When converting a multiple context mode configuration from PIX to ASA, you only need to convert the system context configuration. You use the **allocate-interface** command in the system context to map the ASA physical interface names to the corresponding PIX interface names, which are then used by the individual security contexts.

To convert the system context, perform the following steps:

---

**Step 1** Map how each interface on the target ASA device will correspond to the interfaces on the source PIX device. For example, you might map GigabitEthernet0/0 to the original ethernet0 on the PIX security appliance.

**Step 2** Update the **allocate-interface** commands in the system context configuration to map the original PIX interface names to the physical ASA interfaces.

```
hostname(config-ctx)# allocate-interface physical_interface [mapped_interface_name]
```

For example, the command **allocate-interface ethernet0** could become **allocate-interface GigabitEthernet0/0 ethernet0**



### Note

If an **allocate-interface** command already includes a mapped interface name, then you only need to update the physical interface name from the PIX name to the ASA name. For example, **allocate-interface ethernet0 alias0** would become **allocate-interface GigabitEthernet0/0 alias0**.

---

## Deploying the New Device

Once you have verified the new configuration, put the new device into production. The new device will have the same IP addresses as the PIX security appliance being replaced. You should remove the PIX security appliance from the network before bring the new device online to avoid address conflicts.

## Related Documentation

For additional information on the adaptive security appliance, go to:

[http://www.cisco.com/en/US/products/ps6120/tsd\\_products\\_support\\_series\\_home.html](http://www.cisco.com/en/US/products/ps6120/tsd_products_support_series_home.html)

## Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, *Packet*, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0705R)

© 2008 Cisco Systems, Inc.

All rights reserved.

---