Migración de PIX 500 Series Security Appliances a ASA 5500 Series Adaptive Security Appliances

Contenido

Introducción

Este documento explica cómo migrar de PIX 500 Series Security Appliances a ASA 5500 Series Adaptive Security Appliances.

Nota: Las series PIX 501, PIX 506 y PIX 506E no admiten la versión 7 del software.

Hay dos maneras de convertir una configuración PIX en una configuración ASA:

- Conversión asistida por herramientas
- Conversión manual

Conversión automática basada en herramientas/asistida por herramientas

Cisco recomienda que utilice la conversión asistida por herramientas para convertir las configuraciones PIX a configuraciones ASA.

El método de conversión asistida por herramientas es más rápido y escalable si realiza varias conversiones. Sin embargo, el resultado del proceso en una configuración intermedia contiene tanto la sintaxis antigua como la nueva. Este método se basa en la instalación de la configuración intermedia en el dispositivo de seguridad adaptable de destino para completar la conversión. Hasta que no esté instalado en el dispositivo de destino, no podrá ver la configuración final.

Nota: Cisco ha lanzado la herramienta de migración de PIX a ASA para ayudar a automatizar el proceso de migración a los nuevos dispositivos ASA. Esta herramienta se puede descargar desde el sitio de descarga de software PIX. Consulte Migración de la Configuración de PIX 500 Series Security Appliance a ASA 5500 Series Adaptive Security Appliances para obtener más información.

Prerequisites

Requisitos de hardware y de software

Puede actualizar PIX 515, 515E, 525, 535 a la versión 7.0.

Antes de iniciar el proceso de actualización a la versión 7.x, Cisco recomienda que el PIX ejecute la versión 6.2 o posterior. Esto garantiza que la configuración actual se convierte correctamente. Además, estos requisitos de hardware deben cumplir con los requisitos mínimos de la memoria RAM:

Modelo de PIX	Requisitos de RAM	
	Limitada (R)	Sin restricciones (UR)/Sólo conmutación por fallas (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

Ejecute el comando show version para determinar la cantidad de memoria RAM actualmente instalada en el PIX.

Nota: Las actualizaciones del software PIX 515 y 515E también pueden requerir una actualización de la memoria:

- Aquellos con licencias limitadas y 32 MB de memoria requieren una actualización a una memoria de 64 MB.
- Aquellos con licencias ilimitadas y 64 MB de memoria requieren una actualización a una memoria de 128 MB.

Consulte en esta tabla los números de pieza que necesita para actualizar la memoria de estos

dispositivos.

Configuración del dispositivo actual		Solución de actualización	
Licencia de Plataforma	Memoria Total (antes de la actualización)	Número de Pieza	Memoria Total (después de la actualización)
Limitada (R)	32 MB	PIX-515-MEM-32=	64 MB
Ilimitada (UR)	32 MB	PIX-515-MEM-128=	128 MB
Sólo conmutación por fallas (FO)	64 MB	PIX-515-MEM-128=	128 MB

Nota: El número de pieza depende de la licencia instalada en el PIX.

La actualización del software de la versión 6.x a 7.x es continua y requiere de operaciones manuales, pero antes de comenzar debe seguir los siguientes pasos:

1. Asegúrese de que la configuración actual no incluya los comandos conduit o outbound/apply. Estos comandos ya no se soportan en 7.x y el proceso de upgrade los elimina. Utilice la herramienta Conduit Converter para convertir estos comandos a listas de acceso antes de iniciar la actualización.

2. Asegúrese de que el PIX no finalice las conexiones del Point to Point Tunneling Protocol (PPTP). Actualmente, la versión 7.x del software no admite la terminación del PPTP.

3. Copie todos los certificados digitales para conexiones VPN en el PIX antes de comenzar el proceso de actualización.

4. Lea estos documentos para asegurarse de conocer los comandos nuevos, cambiados o desaprobados:

    - Notas de la versión del software a la que planea actualizar, que se pueden encontrar en "Notas de la versión del dispositivo de seguridad Cisco PIX".

    - Guía para usuarios de Cisco PIX 6.2 y 6.3 que actualizan a la versión 7.0 del software Cisco PIX

5. Planee realizar la migración durante el tiempo de inactividad. Si bien la migración es un proceso simple de dos pasos, la actualización del PIX Security Appliance a 7.x es un cambio importante que requiere suspender el funcionamiento por un tiempo.

6. Descargue el software 7.x de Descargas de Cisco (sólo para clientes registrados).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- ASA 5500 Series Security Appliances
- PIX Security Appliance 515, 515E, 525 y 535
- PIX Software versiones 6.3, 7.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Conversión de configuración manual

Con el proceso de conversión manual, usted utiliza un editor de texto para ir a través de su configuración línea por línea y convertir comandos específicos de PIX a comandos ASA.

La conversión manual de la configuración PIX a una configuración ASA le brinda el mayor control sobre el proceso de conversión. Sin embargo, el proceso lleva mucho tiempo y no se amplía bien si debe realizar más de una conversión.

Para migrar de PIX a ASA debe seguir estos tres pasos:

1. Actualizar el software PIX a la versión 7.x.
2. Convertir los Nombres de Interfaz de Cisco PIX Software 7.0 al Formato de Cisco ASA.
3. Copie la configuración del software PIX 7.0 en Cisco ASA 5500.

Actualización del Software PIX a la Versión 7.x

Antes de comenzar el proceso de actualización, siga estos pasos:

1. Ejecute el comando show running-config o write net para guardar la configuración actual de PIX en un archivo de texto o un servidor TFTP.
2. Ejecute el comando show version para verificar los requisitos, como el de la memoria RAM. Además, guarde la salida de este comando en un archivo de texto. Si debe restaurar el código a una versión más antigua, es posible que necesite la clave de activación original.

Si el PIX tiene una versión básica del sistema de entrada y salida (BIOS) anterior a la 4.2 o si planea actualizar un PIX 515 o un PIX 535 con un PDM ya instalado, debe completar el procedimiento de actualización en el Modo Monitor en lugar de con el método copy tftp flash. Para ver la versión del BIOS, reinicie el PIX y, con un cable de consola conectado, lea los mensajes en el arranque.

La versión del BIOS aparece en un mensaje, como:

<#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
```

Nota: Los comandos de 6.x cambian por los comandos de 7.x automáticamente durante la actualización. La conversión automática de los comandos provoca un cambio en la configuración. Debe revisar los cambios de configuración luego de iniciar el software 7.x para verificar que los cambios automáticos sean correctos. Luego guarde la configuración en la memoria flash para asegurarse de que el sistema no cambie la configuración nuevamente la próxima vez que se inicie el dispositivo de seguridad.

Nota: Una vez actualizado el sistema a la versión 7.x, es importante que no emplee la utilidad npdisk de la versión 6.x, como la recuperación de contraseñas, ya que corrompe la imagen del software 7.x y deberá reiniciar el sistema en el Modo Monitor. También puede perder la configuración anterior, el núcleo de seguridad e información esencial.

Actualice el PIX Security Appliance con el comando copy tftp flash

Siga estos pasos para actualizar el software PIX con el comando copy tftp flash.

1. Copie la imagen binaria del dispositivo PIX, por ejemplo, pix701.bin, al directorio raíz del servidor TFTP.
2. Desde el mensaje de activación, ejecute el comando copy tftp flash.

<#root>

```
pixfirewall>

enable

Password:
```

```
pixfirewall#

copy tftp flash
```

3. Introduzca la dirección IP del servidor TFTP.

```
<#root>

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

4. Introduzca el nombre del archivo en el servidor TFTP que desea cargar. Este es el nombre del archivo de imagen binaria de PIX.

```
<#root>

Source file name [cdisk]?
```

5. Cuando se le solicite iniciar la copia de TFTP, escriba yes.

```
<#root>

copying tftp://172.18.173.123/pix701.bin to flash:image
[yes|no|again]?

yes
```

6. La imagen se copia nuevamente desde el servidor TFTP a la memoria Flash.

   Este mensaje aparece e indica que la transferencia se ha realizado correctamente, que la imagen binaria antigua de Flash se ha borrado y que la nueva imagen se ha escrito e instalado.

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5066808 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
Image installed
pixfirewall#
```

7. Recargue el dispositivo PIX para iniciar la nueva imagen.

```
<#root>

pixfirewall#

reload

Proceed with reload? [confirm]




Rebooting....
```

8. El PIX ahora inicia la imagen 7.0, y esto completa el proceso de actualización.

Ejemplo de Configuración: Actualización del PIX Appliance con el comando copy tftp flash

```
<#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]?

yes

!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Received 5124096 bytes
Erasing current image
Writing 5066808 bytes of image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
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 @ 0xfff00000

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
------------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(1)

********************************* 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>
```

Nota: Ejecute el comando show version para verificar que PIX ahora ejecute la versión 7.x.

Nota: Para revisar cualquier error producido durante la migración de la configuración, ejecute el comando show startup-config errors. Los errores aparecen en esta salida después de iniciar el PIX por primera vez.

Actualización del PIX Security Appliance desde el Modo Monitor

Acceso al modo Monitor

Complete estos pasos para ingresar al Modo Monitor en el PIX.

1. Conecte un cable de consola al puerto de consola en el PIX con el uso de estas configuraciones de comunicación:
    - 9600 bits por segundo
    - 8 bits de datos
    - sin paridad
    - 1 bit de parada
    - sin control de flujo
2. Inicie el ciclo o recargue el PIX. Durante el arranque, se le solicita que utilice BREAK o ESC para interrumpir el inicio de la memoria Flash. Tiene diez segundos para interrumpir el proceso de arranque normal.
3. Presione la tecla ESC o envíe un carácter BREAK para acceder al Modo Monitor.
    - Si utiliza Hyper Terminal de Windows, puede presionar la tecla Esc o Ctrl+Break para enviar un carácter BREAK.
    - Si se conecta a un servidor terminal a través de Telnet para acceder al puerto de consola de PIX, debe presionar Ctrl+] (Control + corchete derecho) para obtener una solicitud del comando Telnet. Luego, ejecute el comando send break.
4. Se visualizará el mensaje monitor>.
5. Continúe con la sección Actualización de PIX desde el Modo Monitor.

Actualice el PIX desde el Modo Monitor

Complete estos pasos para actualizar su PIX desde el Modo Monitor.

1. Copie la imagen binaria del dispositivo PIX, por ejemplo, pix701.bin, al directorio raíz del servidor TFTP.
2. Entre en el Modo Monitor en el PIX. Si no está seguro de cómo hacerlo, consulte Acceso al Modo Monitor.

Nota: Una vez en Modo Monitor, puede utilizar la tecla "?" para ver una lista de opciones disponibles.

3. Introduzca el número de interfaz al que está conectado el servidor TFTP o la interfaz más cercana al servidor TFTP. La interfaz predeterminada es la 1 (interna).

```
<#root>

monitor>

interface
```

Nota: En el Modo Monitor, la interfaz siempre negocia la velocidad y el dúplex automáticamente. La configuración de la interfaz no se puede codificar de forma rígida. Por consiguiente, si la interfaz de PIX se conecta al switch codificado de forma rígida para velocidad/dúplex, reconfigúrela en auto negotiate (negociación automática) mientras esté en el Modo Monitor. Tenga en cuenta también que el dispositivo PIX no puede inicializar una interfaz Gigabit Ethernet desde el Modo Monitor. Debe utilizar una interfaz Fast Ethernet en su lugar.

4. Introduzca la dirección IP de la interfaz definida en el paso tres.

```
<#root>

monitor>

address
```

5. Introduzca la dirección IP del servidor TFTP.

```
<#root>

monitor>

server
```

6. (Opcional) Introduzca la dirección IP del gateway. Se requiere una dirección de gateway si la interfaz del PIX no está en la misma red que el servidor TFTP.

```
<#root>

monitor>

gateway
```

7. Introduzca el nombre del archivo en el servidor TFTP que desea cargar. Este es el nombre del archivo de imagen binaria de PIX.

```
<#root>

monitor>

file
```

8. Haga ping desde el PIX al servidor TFTP para verificar la conectividad IP.

   Si los pings fallan, vuelva a verificar los cables, la dirección IP de la interfaz de PIX y el servidor TFTP, y la dirección IP de la gateway (si es necesario). Los pings deben ejecutarse correctamente antes de continuar.

```
<#root>

monitor>

ping
```

9. Escriba tftp para iniciar la descarga del TFTP.

<#root>

monitor>

tftp

10. El PIX descarga la imagen en la RAM y la inicia automáticamente.

    Durante el proceso de arranque, el sistema de archivos se convierte junto con la configuración actual. Sin embargo, aún no ha terminado. Tenga en cuenta este mensaje de advertencia después del inicio y continúe con el paso 11:

```
************************************************************
  **                                                      **
  **   *** 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. Una vez iniciado, ingrese al modo de habilitación y copie la misma imagen en el PIX nuevamente. Esta vez, ejecute el comando copy tftp flash.

    Esto guarda la imagen en el sistema de archivos Flash. Si no puede realizar este paso, la próxima vez que el PIX se recargue, se producirá un bucle de inicio.

<#root>

pixfirewall>

enable

pixfirewall#

copy tftp flash

    Nota: Para obtener instrucciones detalladas sobre cómo copiar la imagen otra vez con el comando copy tftp flash, consulte la sección Actualización del PIX Security Appliance con el Comando copy tftp flash.

12. Una vez copiada la imagen nuevamente con el comando copy tftp flash, el proceso de actualización ha finalizado.

```
<#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 @ 0xfffd8000
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.

Saving the datafile
!
Saving a copy of old datafile for downgrade
!
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
The version of image file in flash is not bootable in the current version of
software.
Use the downgrade command first to boot older version of software.
The file is being saved as image_old.bin anyway.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Upgrade process complete

```
Need to burn loader....
Erasing sector 0...[OK]
Burning sector 0...[OK]
Erasing sector 64...[OK]
Burning sector 64...[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+ (Crypto5823 revision 0x1)
  ------------------------------------------------------------------------
                                .            .
                                |            |
                               |||          |||
                             .|| ||.      .|| ||.
                           .:||| | |||:..:||| | |||:.
                            C i s c o  S y s t e m s
  ------------------------------------------------------------------------

Cisco PIX Security Appliance Software Version 7.0(1)

  ****************************** 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 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#
```

Conversión de los Nombres de Interfaz de Cisco PIX Software 7.0 al Formato de Cisco ASA

El próximo paso en el proceso es editar la nueva configuración basada en Cisco PIX Software 7.0 fuera de línea.

Como la convención de denominación de interfaz de Cisco ASA es diferente de las de los Cisco PIX Security Appliances, debe realizar cambios en la configuración de Cisco PIX antes de copiar o cargarla en Cisco ASA 5500 Series Security Appliance.

Para realizar los cambios de nombre de interfaz en la configuración de PIX, siga estos pasos:

1. Copie la nueva configuración basada en Cisco PIX Software 7.0 fuera de línea. Para esto,

cargue la configuración en un servidor TFTP/FTP o cópiela desde una sesión de consola a un editor de texto.

Para cargar la configuración de PIX en un servidor TFTP/FTP, desde la consola, ejecute este comando:

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

2. Una vez que se carga el archivo de configuración basada en Cisco PIX Software 7.0 en el servidor TFTP/FTP con éxito (o se copia y pega en un editor de texto), abra Notepad/WordPad o cualquier editor de texto favorito para cambiar los nombres de interfaz en la configuración de PIX.

   Los Cisco PIX Security Appliances numeran las interfaces de 0 a n. Los Cisco ASA 5500 Series Security Appliances numeran las interfaces según la ubicación/ranura. Las interfaces integradas se enumeran de 0/0 a 0/3 y la interfaz de administración es Management 0/0. Las interfaces en el módulo 4GE SSM se enumeran de 1/0 a 1/3.

   Cisco ASA 5510 con licencia básica que ejecuta 7.0 cuenta con tres puertos Fast Ethernet (0/0 a 0/2) y la interfaz Management 0/0 disponible. Cisco ASA 5510 con licencia Security Plus tiene cinco interfaces Fast Ethernet disponibles. Cisco ASA 5520 y 5540 cuentan con cuatro puertos Gigabit Ethernet y un puerto de administración Fast Ethernet. Cisco ASA 5550 cuenta con ocho puertos Gigabit Ethernet y un puerto Fast Ethernet.

   Cambie los nombres de interfaz en la configuración de PIX al formato de interfaz de ASA.

   Por ejemplo:

   <#root>

   ```
   Ethernet0 ==> Ethernet
   ```

   0/0

   ```
   Ethernet1 ==> Ethernet
   ```

   0/1

   ```
   GigabitEthernet0 ==> GigabitEthernet
   ```

   0/0

   Refiérase a la sección "Configuración de los Parámetros de la Interfaz" de la Guía de Configuración de la Línea de Comandos de Cisco Security Appliance, Versión 7.0 para obtener más información.

Copia de la Configuración de PIX en ASA

En esta instancia, usted tiene una configuración basada en Cisco PIX Software 7.0 con los nombres de interfaz modificados, listos para ser copiados o cargados en Cisco ASA 5500 Series. Hay dos formas de cargar la configuración basada en Cisco PIX Software 7.0 en los dispositivos Cisco ASA 5500 Series.

Complete los pasos del Método 1: Copia/Pegado Manual o del Método 2: Descarga desde TFTP/FTP.

Método 1: copiar/pegar manualmente

Copie la configuración mediante el método copiar/pegar desde la consola de PIX:

1. Inicie sesión en la serie Cisco ASA 5500 a través de la consola y ejecute el comando clear config all para borrar la configuración antes de pegar la configuración modificada de Cisco PIX Software 7.0.

   <#root>

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

2. Copie y pegue la configuración en la consola de ASA y guárdela.

   Nota: Asegúrese de que el estado de todas las interfaces sea no shutdown antes de comenzar la prueba.

Método 2: descargar desde TFTP/FTP

El segundo método consiste en descargar la configuración basada en Cisco PIX Software 7.0 de un servidor TFTP/FTP. Para esto, debe configurar la interfaz de administración en el dispositivo Cisco ASA 5500 Series para descarga del TFTP/FTP:

1. Desde la consola de ASA, ejecute:

   <#root>

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

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

Nota: (Opcional) route management <ip> <mask> <next-hop>

2. Una vez configurada la interfaz de administración, puede descargar la configuración de PIX en ASA:

<#root>

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

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

3. Guarde la configuración.

Aplicación de la Configuración de la Versión 6.x del Software PIX en la Versión 7.x del Software ASA

La conversión de una configuración PIX 6.2 o 6.3 a un nuevo dispositivo de seguridad ASA es un proceso manual. El administrador ASA/PIX debe convertir la sintaxis PIX 6.x para que coincida con la sintaxis ASA y escribir los comandos en la configuración ASA. Puede cortar y pegar algunos comandos, como access-list. Asegúrese de comparar detenidamente la configuración de PIX 6.2 o 6.3 con la nueva configuración de ASA, para corroborar que no se ha producido ningún error en la conversión.

Nota: Cisco CLI Analyzer (sólo para clientes registrados) se puede utilizar para convertir algunos

de los comandos antiguos, no admitidos, como apply, outbound o conduit a la lista de acceso adecuada. Las declaraciones convertidas deben ser revisadas detenidamente. Es necesario verificar que la conversión coincida con las políticas de seguridad.

Nota: El proceso de actualización a un nuevo dispositivo ASA es diferente del de actualización a un nuevo dispositivo PIX. Si se intenta actualizar a un ASA mediante un proceso PIX, se producirán varios errores de configuración en el ASA.

Resolución de problemas: conversión manual de la configuración

Dispositivo Atascado en el Bucle de Reinicio

- Después de utilizar el método copy tftp flash para actualizar el PIX y reiniciarlo, se atasca en este bucle de reinicio:

<#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.
```

Los dispositivos PIX con versiones de BIOS anteriores a 4.2 no pueden actualizarse mediante el comando copy tftp flash. Debe actualizarlos con el método Modo Monitor.

- Después de ejecutar el PIX en la versión 7.x y reiniciarlo, se atasca en este bucle de reinicio:

<#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
```

Si el PIX se actualiza desde el Modo Monitor a la versión 7.0, pero la imagen de esta versión no se copia nuevamente en la memoria Flash después del primer inicio de la versión 7.0; cuando el PIX se recargue, se atascará en un bucle de reinicio.

La solución es cargar la imagen nuevamente desde el Modo Monitor. Una vez reiniciado, debe copiar la imagen una vez más mediante el método copy tftp flash.

Mensaje de error

Cuando actualiza con el método copy tftp flash, observa este mensaje de error:

<#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#
```

Generalmente, este mensaje aparece cuando se actualiza PIX 515 o PIX 535 con un PDM ya instalado con el método copy tftp flash.

Actualice con el método Modo Monitor para resolver este problema.

Aparentemente la Configuración No Es Correcta

Después de la actualización de PIX de la versión 6.x a 7.x, algunas de las opciones de configuración no migran adecuadamente.

La salida del comando show startup-config errors muestra cualquier error que se haya producido durante la migración de la configuración. Los errores aparecen en esta salida después de iniciar el PIX por primera vez. Examine estos errores e intente resolverlos.

Algunos Servicios como el FTP No Funcionan

En ocasiones, algunos servicios como el FTP no funcionan luego de una actualización.

La inspección para estos servicios no está habilitada después de la actualización. Active la inspección para los servicios correspondientes. Para esto, agréguelos a la política de inspección predeterminada/global o cree una política de inspección aparte para el servicio deseado.

Refiérase a la sección "Aplicación de la Inspección de Application Layer Protocol" de la Guía de Configuración de Línea de Comandos de Cisco Security Appliance, Versión 7.0 para obtener más información sobre las políticas de inspección.

No se puede acceder a Internet cuando el Cisco PIX Security Appliance se reemplaza con el Cisco Adaptive Security Appliance (ASA)

Utilice esta sección si no puede acceder a Internet después de sustituir el Cisco PIX Security Appliance por el Cisco Adaptive Security Appliance (ASA).

Cuando desconecta el PIX de la red y conecta el ASA en la red con una dirección IP de la interfaz externa que es la misma que la interfaz externa del PIX, el router ascendente todavía tiene la dirección mac para el PIX correspondiente a la dirección IP de la interfaz externa. Como resultado, no puede enviar los paquetes de respuesta al ASA. Para que el ASA funcione, debe borrar la entrada ARP en el router ascendente para que detecte la entrada de dirección mac nueva/correcta. Si elimina las entradas ARP cuando planea reemplazar el PIX con ASA, se resuelve el problema de conectividad a Internet. El vaciado de la entrada ARP debe ser realizado por el ISP en su extremo.

Información Relacionada

- Dispositivos de seguridad de la serie Cisco PIX 500 - Introducción
- Soporte Técnico y Documentación - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).