

PIX 6.3 Upgrade to a New PIX 7.0 Appliance Configuration Example

Document ID: 71928

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Configure

- PIX Software Version 6.3.5 Configuration
- Apply a PIX Software Version 6.3.5 Configuration to PIX Software Version 7.0
- Apply a PIX Software Version 6.3.5 Configuration to ASA Software Version 7.0

Verify

Troubleshoot

Related Information

Introduction

This document explains how to upgrade or move a configuration from a PIX Security Appliance that runs software version 6.3 to a new PIX Security Appliance that runs software version 7.0.

Note: Administrators who upgrade software version 6.2 or 6.3 to version 7.0 on the same PIX device should refer to the Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0.

Prerequisites

Requirements

This document is designed to assist administrators with the migration of a PIX configuration to a new appliance. This document should not be a replacement for the documents listed here. It is strongly recommended that you read and understand these two documents before you upgrade and use PIX software version 7.x.

- Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0
- Cisco PIX Firewall Software Release Notes

Note: Save and copy your configurations to a text file or TFTP server before any upgrade attempts. In order to download the freeware version of the TFTP server, Cisco recommends that you use TFTP32 .

Components Used

The information in this document is based on these software and hardware versions:

- PIX 515E Security Appliance with software version 6.3.5
- PIX 515E Security Appliance with software version 7.0.6

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure

that you understand the potential impact of any command.

Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

Configure

In this section, you are presented with the information to configure the features described in this document.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

This document uses these configurations:

- PIX Software Version 6.3.5 Configuration
- Apply a PIX Software Version 6.3.5 Configuration to PIX Software Version 7.0
- Apply a PIX Software Version 6.3.5 Configuration to Adaptive Security Appliance (ASA) Software Version 7.0

PIX Software Version 6.3.5 Configuration

The document begins with a PIX 515E and software version 6.3.5. The configuration includes several options typically found in production environments.

```
pix515e#show version

Cisco PIX Firewall Version 6.3(5)

Compiled on Thu 04-Aug-05 21:40 by morlee

pix515e up 39 secs

Hardware:   PIX-515E, 64 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0x300, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

0: ethernet0: address is 0012.4364.ea30, irq 10
1: ethernet1: address is 0012.4364.ea31, irq 11
2: ethernet2: address is 00e0.b602.fe67, irq 11
3: ethernet3: address is 00e0.b602.fe66, irq 10
4: ethernet4: address is 00e0.b602.fe65, irq 9
5: ethernet5: address is 00e0.b602.fe64, irq 5
Licensed Features:
Failover:                Enabled
VPN-DES:                 Enabled
VPN-3DES-AES:           Enabled
Maximum Physical Interfaces: 6
Maximum Interfaces:     10
Cut-through Proxy:      Enabled
Guards:                 Enabled
URL-filtering:          Enabled
Inside Hosts:           Unlimited
Throughput:             Unlimited
IKE peers:              Unlimited
```

This PIX has an Unrestricted (UR) license.

Serial Number:

Running Activation Key: 0x8e62bc4d 0x20ffa2ba 0x52ea1945 0x9bb024fb
Configuration has not been modified since last system restart.

PIX 6.3.5 Configuration

```
pix515e#show running-config
: Saved
:
PIX Version 6.3(5)
interface ethernet0 auto
interface ethernet1 auto
interface ethernet2 auto
interface ethernet3 auto
interface ethernet3 vlan30 physical
interface ethernet3 vlan40 logical
interface ethernet3 vlan50 logical
interface ethernet4 auto shutdown
interface ethernet5 auto
nameif ethernet0 outside security0
nameif ethernet1 inside security100
nameif ethernet2 dmz security50
nameif ethernet3 vlan30 security85
nameif ethernet4 intf4 security8
nameif ethernet5 failover security99
nameif vlan40 vlan40 security90
nameif vlan50 vlan50 security90
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname pix515e
domain-name companyx.com
fixup protocol dns maximum-length 512
fixup protocol ftp 21
fixup protocol h323 h225 1720
fixup protocol h323 ras 1718-1719
fixup protocol http 80
no fixup protocol rsh 514
fixup protocol rtsp 554
fixup protocol sip 5060
fixup protocol sip udp 5060
fixup protocol skinny 2000
no fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol tftp 69
names
object-group network inside_networks
  network-object 172.22.1.0 255.255.255.0
  network-object 172.31.0.0 255.255.0.0
  network-object 172.16.0.0 255.255.0.0
access-list inside permit ip object-group inside_networks any
access-list outside permit tcp any host 10.0.0.100 eq www
access-list outside permit tcp any host 10.0.0.100 eq https
access-list outside permit tcp any host 10.0.0.150 eq smtp
access-list dmz permit tcp host 192.168.0.150 host 172.22.1.200 eq telnet
access-list dmz deny ip any object-group inside_networks
access-list dmz permit ip 192.168.0.0 255.255.255.0 any
access-list vpn permit ip 172.22.1.0 255.255.255.0 10.255.1.0 255.255.255.0
access-list vpn permit ip 10.255.1.0 255.255.255.0 172.22.1.0 255.255.255.0
access-list inside_nonat permit ip any 3.3.3.0 255.255.255.0
access-list inside_nonat permit ip 172.22.1.0 255.255.255.0 10.255.1.0 255.255.255.0
pager lines 24
logging on
logging buffered debugging
logging trap informational
logging host dmz 192.168.0.2
icmp permit any outside
icmp permit any inside
```

```
mtu outside 1500
mtu inside 1500
mtu dmz 1500
mtu vlan30 1500
mtu intf4 1500
mtu failover 1500
ip address outside 10.0.0.1 255.255.255.0
ip address inside 172.22.1.159 255.255.255.0
ip address dmz 192.168.0.1 255.255.255.0
ip address vlan30 172.22.30.1 255.255.255.0
no ip address intf4
ip address failover 1.1.1.1 255.255.255.252
ip address vlan40 172.22.40.1 255.255.255.0
ip address vlan50 172.22.50.1 255.255.255.0
ip audit info action alarm
ip audit attack action alarm
ip local pool migratepool 3.3.3.1-3.3.3.254
no failover
failover timeout 0:00:00
failover poll 15
failover ip address outside 10.0.0.2
failover ip address inside 172.22.1.251
failover ip address dmz 192.168.0.2
failover ip address vlan30 172.22.30.2
no failover ip address intf4
failover ip address failover 1.1.1.2
failover ip address vlan40 172.22.40.2
failover ip address vlan50 172.22.50.2
failover link failover
pdm history enable
arp timeout 14400
global (outside) 1 10.0.0.50
global (dmz) 1 192.168.0.10
nat (inside) 0 access-list inside_nonat
nat (inside) 1 0.0.0.0 0.0.0.0 0 0
nat (vlan30) 1 0.0.0.0 0.0.0.0 0 0
nat (vlan40) 1 0.0.0.0 0.0.0.0 0 0
nat (vlan50) 1 0.0.0.0 0.0.0.0 0 0
static (dmz,outside) 10.0.0.100 192.168.0.100 netmask 255.255.255.255 0 0
static (dmz,outside) 10.0.0.150 192.168.0.150 netmask 255.255.255.255 0 0
static (inside,dmz) 172.22.1.200 172.22.1.200 netmask 255.255.255.255 0 0
access-group outside in interface outside
access-group inside in interface inside
access-group dmz in interface dmz
router ospf 100
  network 172.22.1.0 255.255.255.0 area 0
  log-adj-changes
  redistribute connected
  redistribute static
route outside 0.0.0.0 0.0.0.0 10.0.0.2 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h225 1:00:00
timeout h323 0:05:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server TACACS+ max-failed-attempts 3
aaa-server TACACS+ deadtime 10
aaa-server RADIUS protocol radius
aaa-server RADIUS max-failed-attempts 3
aaa-server RADIUS deadtime 10
aaa-server LOCAL protocol local
aaa-server acs protocol tacacs+
aaa-server acs max-failed-attempts 3
aaa-server acs deadtime 10
aaa-server acs (inside) host 172.22.1.254 test timeout 10
```

```

aaa authentication ssh console acs
no snmp-server location
no snmp-server contact
snmp-server community public
no snmp-server enable traps
floodguard enable
crypto ipsec transform-set sha3des esp-3des esp-sha-hmac
crypto ipsec transform-set ESP-3DES-MD5 esp-3des esp-md5-hmac
crypto dynamic-map outside_dyn_map 20 set transform-set ESP-3DES-MD5
crypto map vpn 10 ipsec-isakmp
crypto map vpn 10 match address vpn
crypto map vpn 10 set peer 10.255.255.1
crypto map vpn 10 set transform-set sha3des
crypto map vpn 20 ipsec-isakmp dynamic outside_dyn_map
crypto map vpn interface outside
isakmp enable outside
isakmp key ***** address 10.255.255.1 netmask 255.255.255.255
isakmp identity address
isakmp nat-traversal 20
isakmp policy 10 authentication pre-share
isakmp policy 10 encryption 3des
isakmp policy 10 hash sha
isakmp policy 10 group 2
isakmp policy 10 lifetime 86400
isakmp policy 30 authentication pre-share
isakmp policy 30 encryption 3des
isakmp policy 30 hash md5
isakmp policy 30 group 2
isakmp policy 30 lifetime 86400
vpngroup migration address-pool migratepool
vpngroup migration idle-time 1800
vpngroup migration password *****
telnet 172.22.1.0 255.255.255.0 inside
telnet timeout 5
ssh 172.22.1.0 255.255.255.0 inside
ssh timeout 5
console timeout 0
terminal width 80
: end

```

Apply a PIX Software Version 6.3.5 Configuration to PIX Software Version 7.0

This section describes how to move the PIX software version 6.3.5 configuration to a new PIX with software version 7.0.

From PIX 6.3.5, transfer the configuration to a TFTP server.

```

pix515e#write net 172.22.1.235:pix515e635
Building configuration...
TFTP write 'pix515e635' at 172.22.1.235 on interface 1
[OK]
pix515e#

```

Now that the configuration has been saved to a TFTP server, the new PIX with software version 7.0 can retrieve the configuration.

```

pixfirewall#configure terminal
pixfirewall(config)#interface e1
pixfirewall(config-if)#no shut
pixfirewall(config-if)#nameif inside
INFO: Security level for "inside" set to 100 by default.

```

```
pixfirewall(config-if)#ip address 172.22.1.159 255.255.255.0
pixfirewall(config-if)#exit
```

```
!--- The new appliance needs a temporary configuration
!--- to allow the 6.3.5 configuration
!--- to be transfered (TFTP) to the new appliance. The new PIX can be assigned any
!--- available IP address.
```

```
pixfirewall(config)#
pixfirewall(config)#exit
pixfirewall#copy tftp startup-config
```

```
Address or name of remote host []? 172.22.1.235
```

```
Source filename []? pix515e635
```

```
Accessing tftp://172.22.1.235/pix515e635...!!
```

```
Writing system file...
```

```
!!
```

```
5867 bytes copied in 0.180 secs
```

```
pixfirewall(config)#reload
```

```
!--- Disconnect the new appliance from the network. After the device reloads,
!--- the device has the IP address of the production PIX 6.3.5.
!--- Disconnecting the new device prevents duplicate
!--- IP addresses on the network.
```

```
Proceed with reload? [confirm]
```

```
pixfirewall(config)#
```

```
***
```

```
*** --- START GRACEFUL SHUTDOWN ---
```

```
Shutting down isakmp
```

```
Shutting down File system
```

```
***
```

```
*** --- SHUTDOWN NOW ---
```

```
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	1011	0026	PCI-to-PCI Bridge	
01	00	00	8086	1229	Ethernet	11
01	01	00	8086	1229	Ethernet	10
01	02	00	8086	1229	Ethernet	9
01	03	00	8086	1229	Ethernet	5

Cisco PIX Security Appliance Software Version 7.0(6)

***** 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) 1996-2006 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

*!--- PIX version 7.x reports its progress in
!--- converting the 6.x configuration that it encounters.*

```
.WARNING: interface dmz security level is 50.
*** Output from config line 115, "logging host dmz 192.168..."
INFO: Only classful networks will be redistributed
*** Output from config line 215, " redistribute connected"
INFO: Only classful networks will be redistributed
*** Output from config line 217, " redistribute static"
.
timeout sip-disconnect 0:02:00 sip-invite 0:03:00
      ^
ERROR: % Invalid input detected at '^' marker.
*** Output from config line 229, "timeout sip-disconnect 0..."
ERROR: This command is no longer needed. The LOCAL user database is always enabled.
*** Output from config line 245, "aaa-server LOCAL protoco..."
ERROR: This command is no longer needed. The 'floodguard' feature is always enabled.
*** Output from config line 265, "floodguard enable"
WARNING: the 'vpngroup' command has been deprecated,
and will be converted to the corresponding tunnel-group and group-policy syntax
*** Output from config line 313, "vpngroup migration addre..."
WARNING: the 'vpngroup' command has been deprecated,
and will be converted to the corresponding tunnel-group and group-policy syntax
*** Output from config line 315, "vpngroup migration idle-..."
```

```
WARNING: the 'vpngroup' command has been deprecated,  
and will be converted to the corresponding tunnel-group and group-policy syntax  
*** Output from config line 317, "vpngroup migration passw..."
```

```
Cryptochecksum (changed): 183101e6 b5760521 21f9fe61 bc9d29ed  
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 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 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.  
pix515e> en  
Password:  
pix515e#
```

Apply a PIX Software Version 6.3.5 Configuration to ASA Software Version 7.0

The conversion of a PIX 6.2 or 6.3 configuration to a new ASA Security Appliance is a manual process. The ASA/PIX administrator is required to convert PIX 6.x syntax to match the ASA syntax and type the commands into the ASA configuration. You can cut and paste some commands such as the **access-list** command. Be sure to closely compare the PIX 6.2 or 6.3 configuration to the new ASA configuration in order to ensure no mistakes have been made in the conversion.

Note: The process for upgrading to a new ASA appliance is different from an upgrade to a new PIX appliance. An attempt to upgrade to an ASA with PIX process generates a number of configuration errors on the ASA.

Verify

Verify the newly upgraded configuration to the PIX 6.2 or 6.3 configuration saved prior to the upgrade. Compare each line of the previously saved configuration with the new configuration. Even though the syntax has changed, the device policies (security, routing, interface, and so forth) should be the same.

Troubleshoot

There is currently no specific troubleshooting information available for this configuration.

Related Information

- [Cisco ASA 5500 Series Adaptive Security Appliances Support](#)
 - [Cisco PIX 500 Series Security Appliances Support](#)
 - [Cisco Secure PIX Firewall Command References](#)
 - [Security Product Field Notices \(including PIX\)](#)
 - [Requests for Comments \(RFCs\)](#)
 - [Technical Support & Documentation – Cisco Systems](#)
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Oct 13, 2008

Document ID: 71928
