SearchNetworkingChannel.com
The Web's best resource for networking channel professionals

NETWORK INFRASTRUCTURE

Checklist: How to configure a PIX firewall

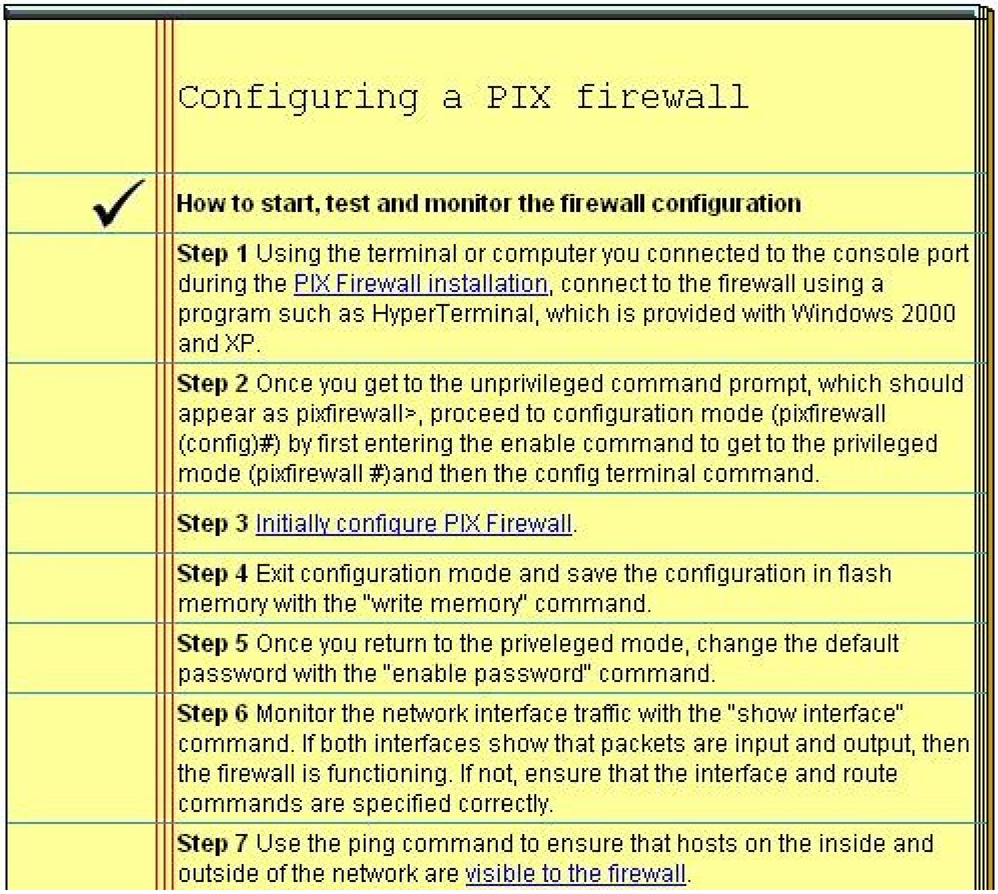
Judith Myerson

12.19.2007

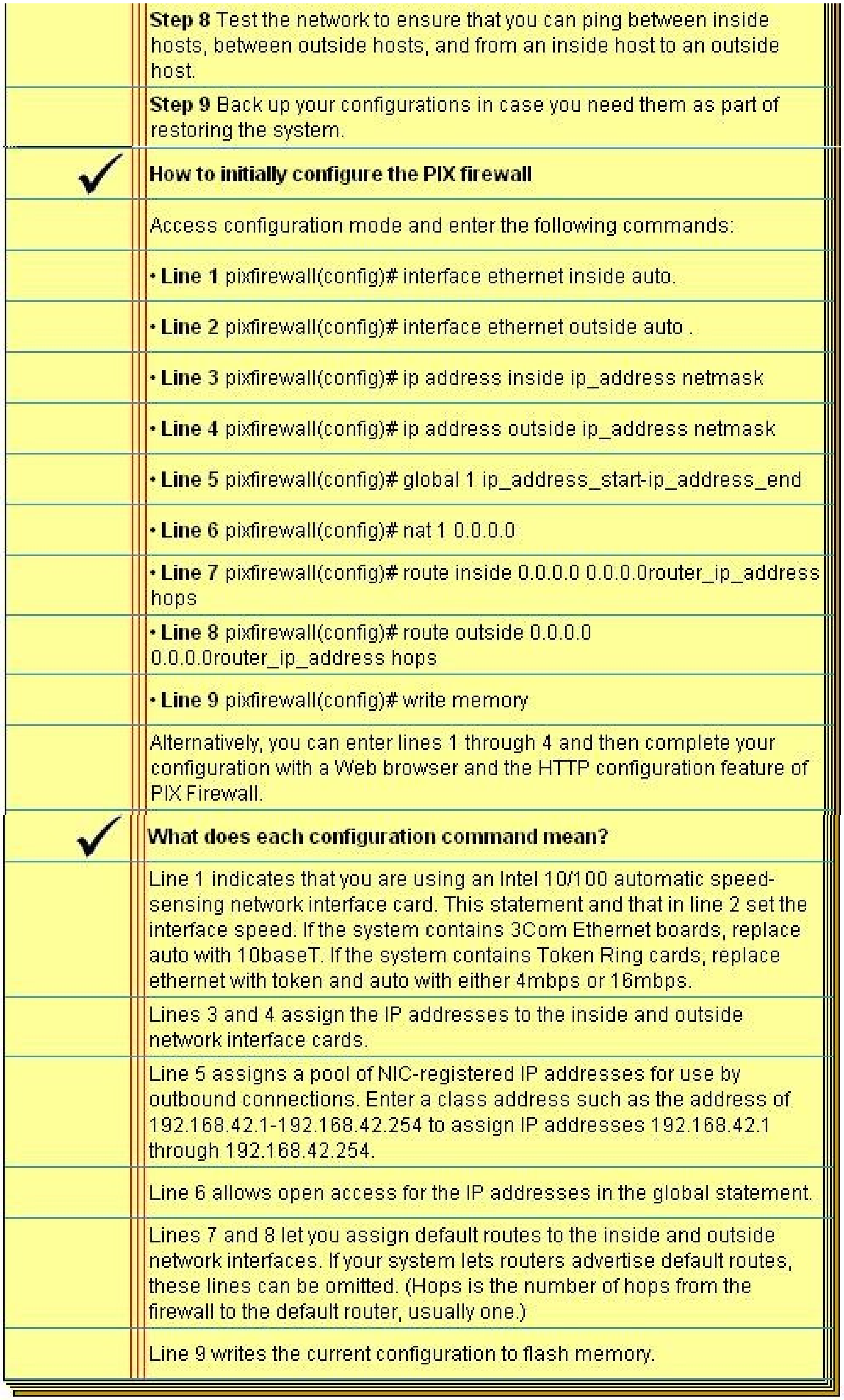
Service provider takeaway: *Proper initial PIX firewall configuration can help network service providers protect customer networks from malicious attacks.*

When shipped from Cisco, each PIX firewall comes with a basic configuration boot-up, but PIX does not let network traffic pass through until the firewall is configured to do so. Resource-strapped small and medium-sized businesses (SMBs) may have trouble doing the initial configuration of a PIX firewall if they don't have anyone with experience on staff. Network service providers can use this checklist to ensure that initial configuration goes smoothly in customer shops.

The initial configuration examples used in this checklist are based on PIX Firewall software version 4.0.



	Configuring a PIX firewall
✓	**How to start, test and monitor the firewall configuration**
	Step 1 Using the terminal or computer you connected to the console port during the PIX Firewall installation, connect to the firewall using a program such as HyperTerminal, which is provided with Windows 2000 and XP.
	Step 2 Once you get to the unprivileged command prompt, which should appear as pixfirewall>, proceed to configuration mode (pixfirewall (config)#) by first entering the enable command to get to the privileged mode (pixfirewall #)and then the config terminal command.
	Step 3 Initially configure PIX Firewall.
	Step 4 Exit configuration mode and save the configuration in flash memory with the "write memory" command.
	Step 5 Once you return to the priveleged mode, change the default password with the "enable password" command.
	Step 6 Monitor the network interface traffic with the "show interface" command. If both interfaces show that packets are input and output, then the firewall is functioning. If not, ensure that the interface and route commands are specified correctly.
	Step 7 Use the ping command to ensure that hosts on the inside and outside of the network are visible to the firewall.



Step 8 Test the network to ensure that you can ping between inside hosts, between outside hosts, and from an inside host to an outside host.

Step 9 Back up your configurations in case you need them as part of restoring the system.

✓ How to initially configure the PIX firewall

Access configuration mode and enter the following commands:

- **Line 1** pixfirewall(config)# interface ethernet inside auto.
- **Line 2** pixfirewall(config)# interface ethernet outside auto .
- **Line 3** pixfirewall(config)# ip address inside ip_address netmask
- **Line 4** pixfirewall(config)# ip address outside ip_address netmask
- **Line 5** pixfirewall(config)# global 1 ip_address_start-ip_address_end
- **Line 6** pixfirewall(config)# nat 1 0.0.0.0
- **Line 7** pixfirewall(config)# route inside 0.0.0.0 0.0.0.0router_ip_address hops
- **Line 8** pixfirewall(config)# route outside 0.0.0.0 0.0.0.0router_ip_address hops
- **Line 9** pixfirewall(config)# write memory

Alternatively, you can enter lines 1 through 4 and then complete your configuration with a Web browser and the HTTP configuration feature of PIX Firewall.

✓ What does each configuration command mean?

Line 1 indicates that you are using an Intel 10/100 automatic speed-sensing network interface card. This statement and that in line 2 set the interface speed. If the system contains 3Com Ethernet boards, replace auto with 10baseT. If the system contains Token Ring cards, replace ethernet with token and auto with either 4mbps or 16mbps.

Lines 3 and 4 assign the IP addresses to the inside and outside network interface cards.

Line 5 assigns a pool of NIC-registered IP addresses for use by outbound connections. Enter a class address such as the address of 192.168.42.1-192.168.42.254 to assign IP addresses 192.168.42.1 through 192.168.42.254.

Line 6 allows open access for the IP addresses in the global statement.

Lines 7 and 8 let you assign default routes to the inside and outside network interfaces. If your system lets routers advertise default routes, these lines can be omitted. (Hops is the number of hops from the firewall to the default router, usually one.)

Line 9 writes the current configuration to flash memory.

About the author

Judith M. Myerson is a systems engineer/architect and a communications and electronics consultant/instructor. While as the former ADP Security Officer/Manager and Network Security Officer at a U.S. naval facility, she led a computer security program for an enterprise infrastructure of networks, servers, operating systems, and communications. A holder of Master of Science degree in Engineering, she is the editor of *Enterprise Systems Integration*, 2nd edition (Auerbach 2001) and the author of RFID in the *Supply Chain: a Guide to Selection and Implementation* (Auerbach, 2007). She is also the author of "Defense-in-Depth for multiple SOAs" (IBM, 2006) and "Mitigate risks for vulnerability with a SLA guarantee" (IBM, Jan 2005). Contact Judith directly at jmyerson@bellatlantic.net.