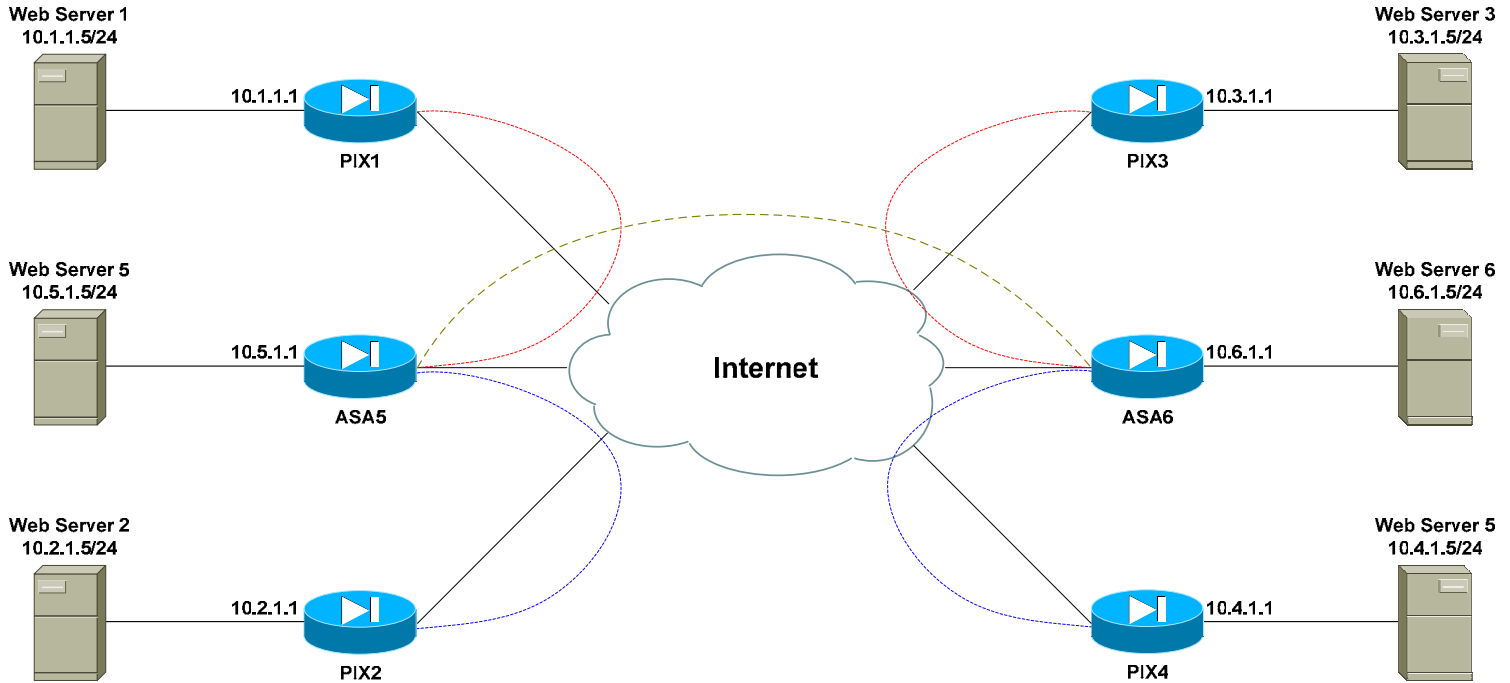


- PIX Advanced IPSEC Lab -

Configuring Advanced PIX IPSEC – Lab



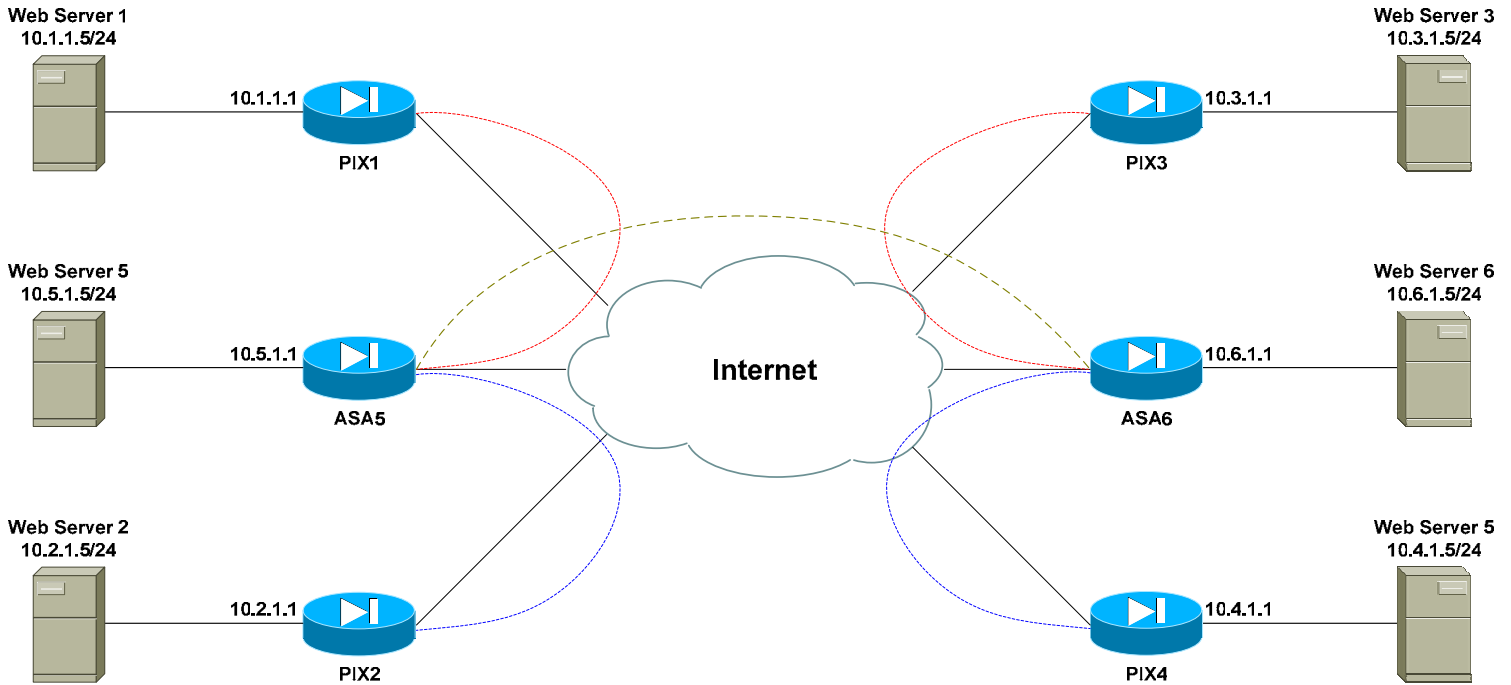
Basic Objectives:

1. Configure and cable the Ethernet interfaces as indicated in the above diagram.
2. Configure a web server for each network, and apply an IP address as diagrammed.
3. Your instructor will configure a router or Layer-3 switch to function as a pseudo “Internet.”

* * *

All original material copyright © 2008 by Aaron Balchunas (aaron@routeralley.com), unless otherwise noted. All other material copyright © of their respective owners. This material may be copied and used freely, but may not be altered or sold without the expressed written consent of the owner of the above copyright. Updated material may be found at <http://www.routeralley.com>.

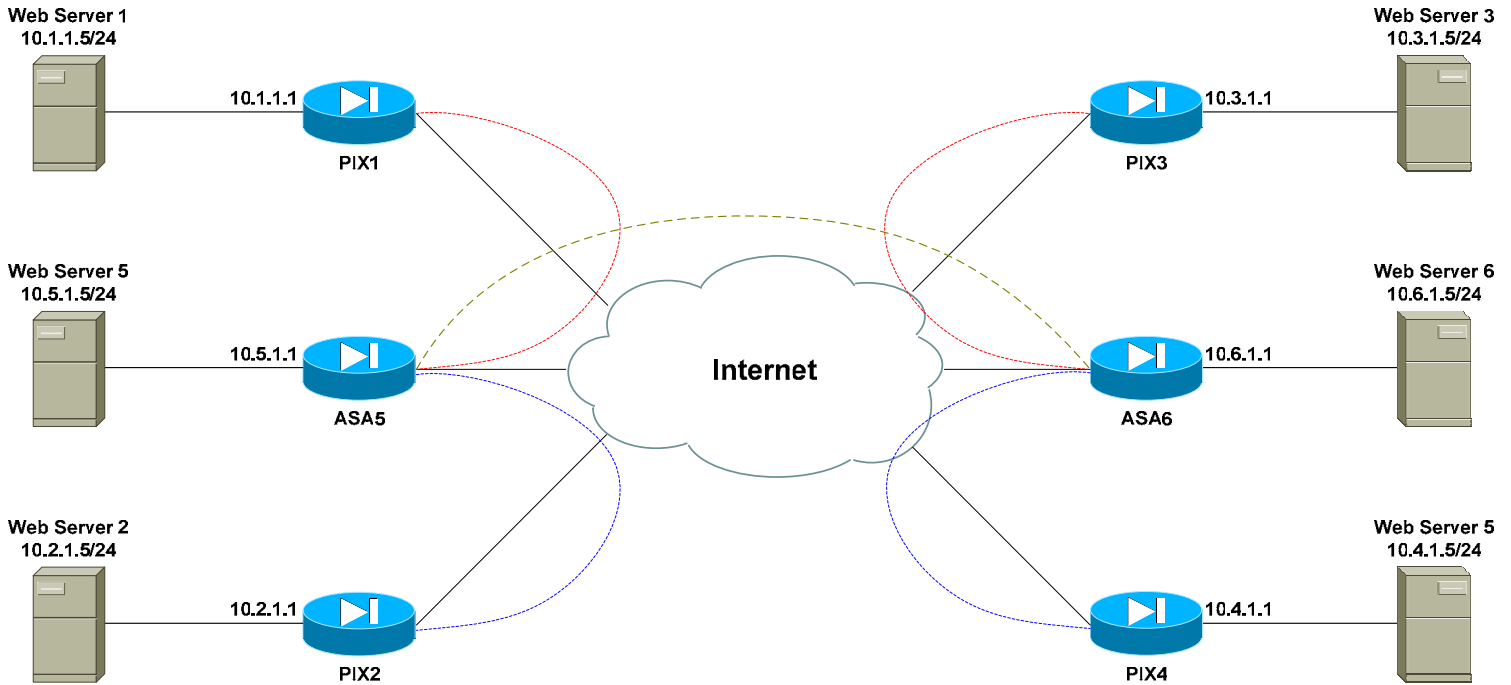
Configuring Advanced PIX IPSEC – Lab (continued)



PIX Objectives:

4. Each network has been assigned a pool of public addresses, in the YY.YY.YY.64/29 range, where “Y” is the network or PIX/ASA number. For example, PIX3 has been assigned the 33.33.33.64/29 range of public addresses. Similarly, ASA5 has been assigned the 55.55.55.64/29 range of public addresses.
5. The first usable address in each public range will be the next-hop address to the Internet. The second usable address in each public range should be applied to the outside interface of each PIX/ASA.

Configuring Advanced PIX IPSEC – Lab (continued)

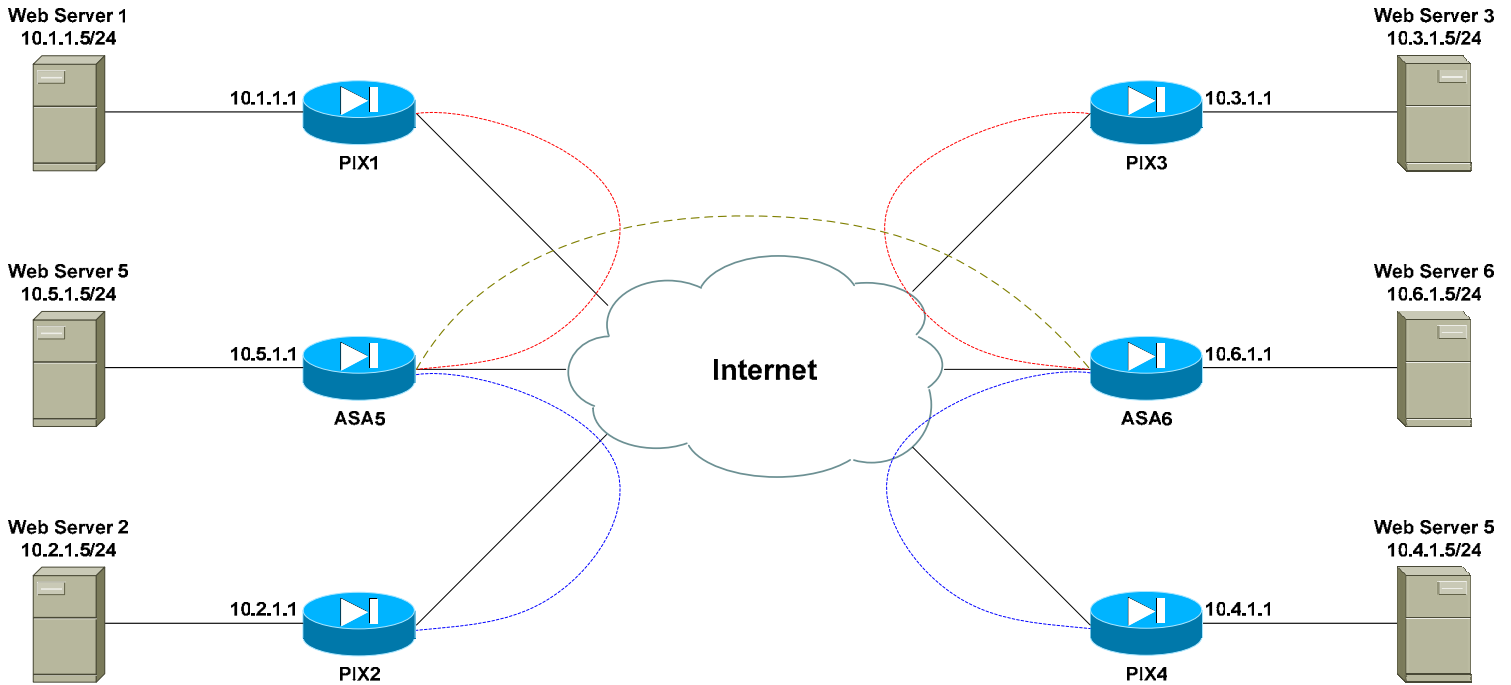


PIX Objectives:

- 6. Ensure that hosts on each local LAN are NAT'ed using PAT when accessing the Internet. Use a public address of your choosing.

- 7. Ensure that all interfaces on each PIX/ASA are pingable.

Configuring Advanced PIX IPSEC – Lab (continued)



PIX Objectives:

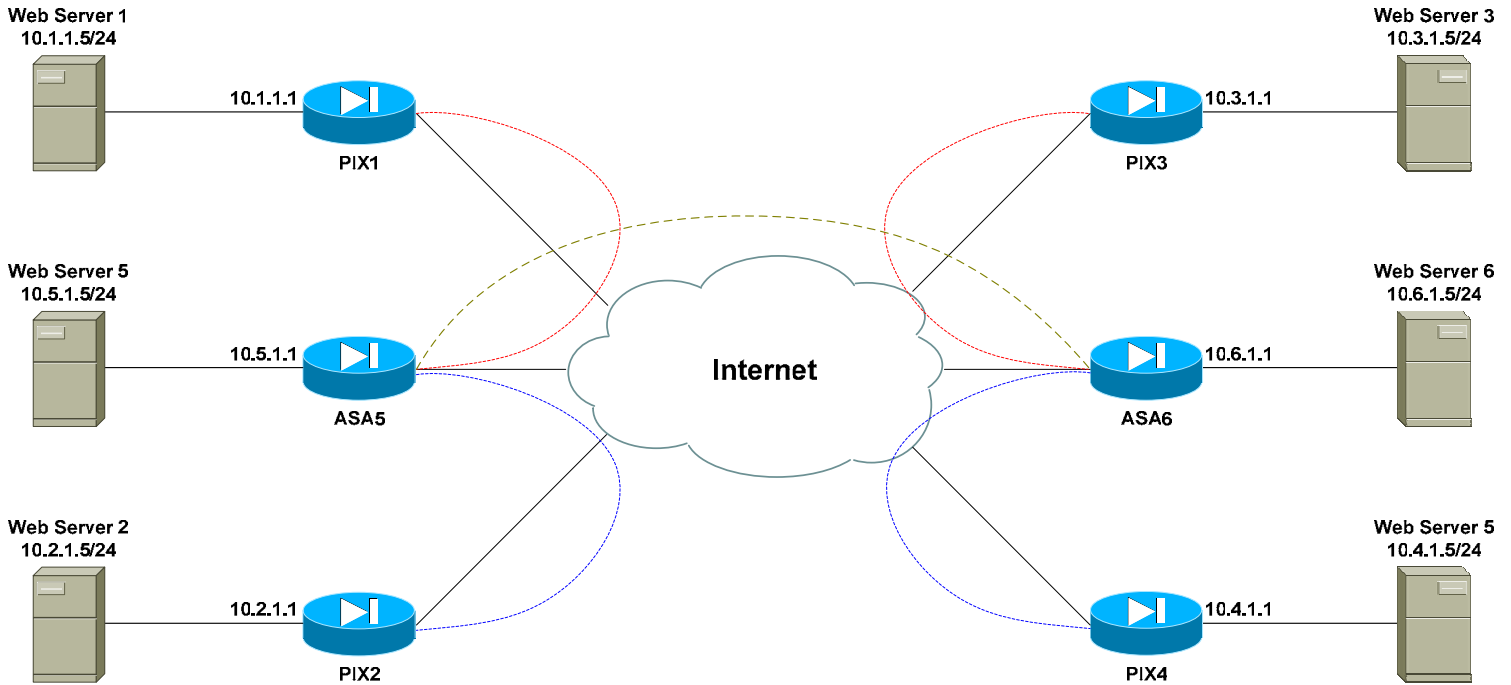
8. Configure the following site-to-site IPsec tunnels:

PIX1 to ASA5
PIX2 to ASA5

PIX3 to ASA6
PIX4 to ASA6

Use the strongest supported forms of encryption and hashing. Use a pre-shared key of CISCO.

Configuring Advanced PIX IPSEC – Lab (continued)

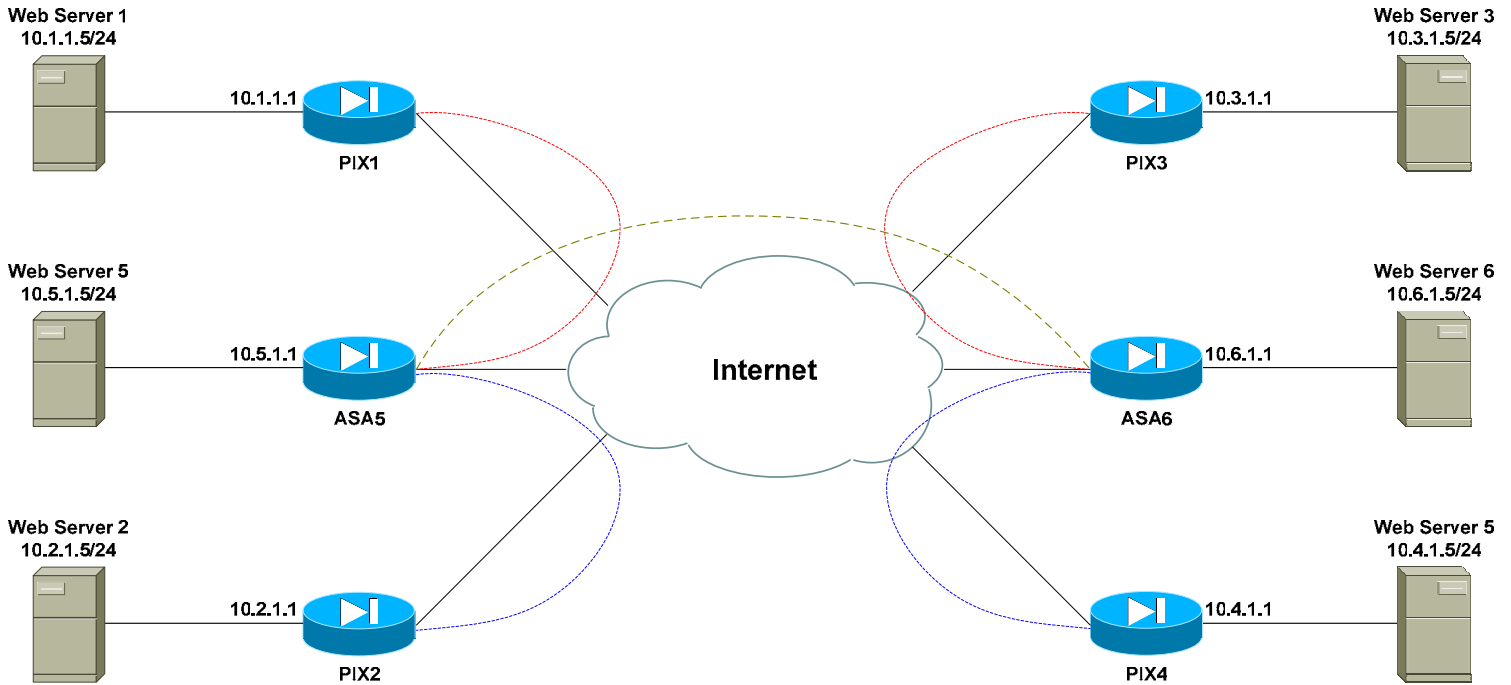


PIX Objectives:

- 9. Ensure that Web Server 1 and Web Server 2 can access Web Server 5 by its private address (and vice-versa).

- 10. Ensure that Web Server 3 and Web Server 4 can access Web Server 6 by its private address (and vice-versa).

Configuring Advanced PIX IPSEC – Lab (continued)

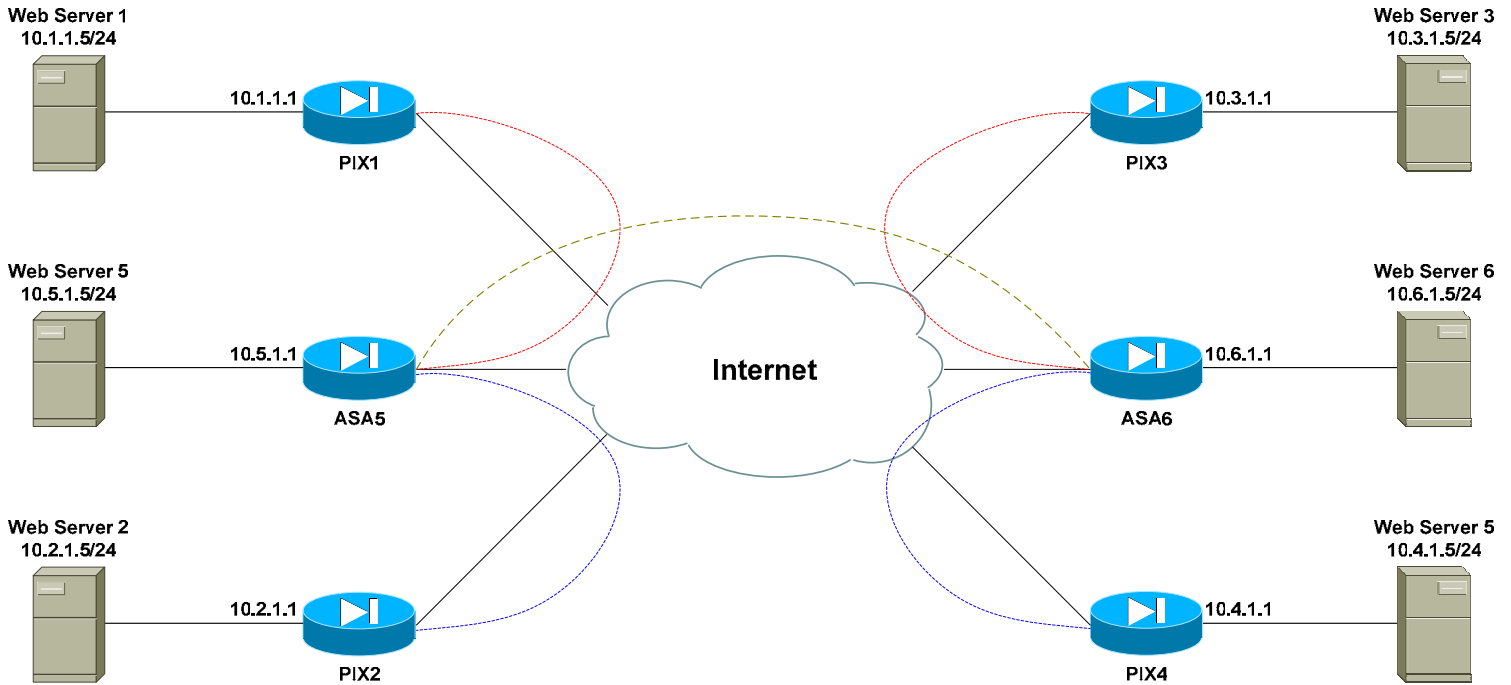


PIX Objectives:

11. Perform whatever additional configuration is necessary to allow Web Server 1 to access Web Server 2 by its private address, **without creating a direct VPN tunnel between PIX1 and PIX2.**

12. Perform whatever additional configuration is necessary to allow Web Server 3 to access Web Server 4 by its private address, **without creating a direct VPN tunnel between PIX3 and PIX4.**

Configuring Advanced PIX IPSEC – Lab (continued)

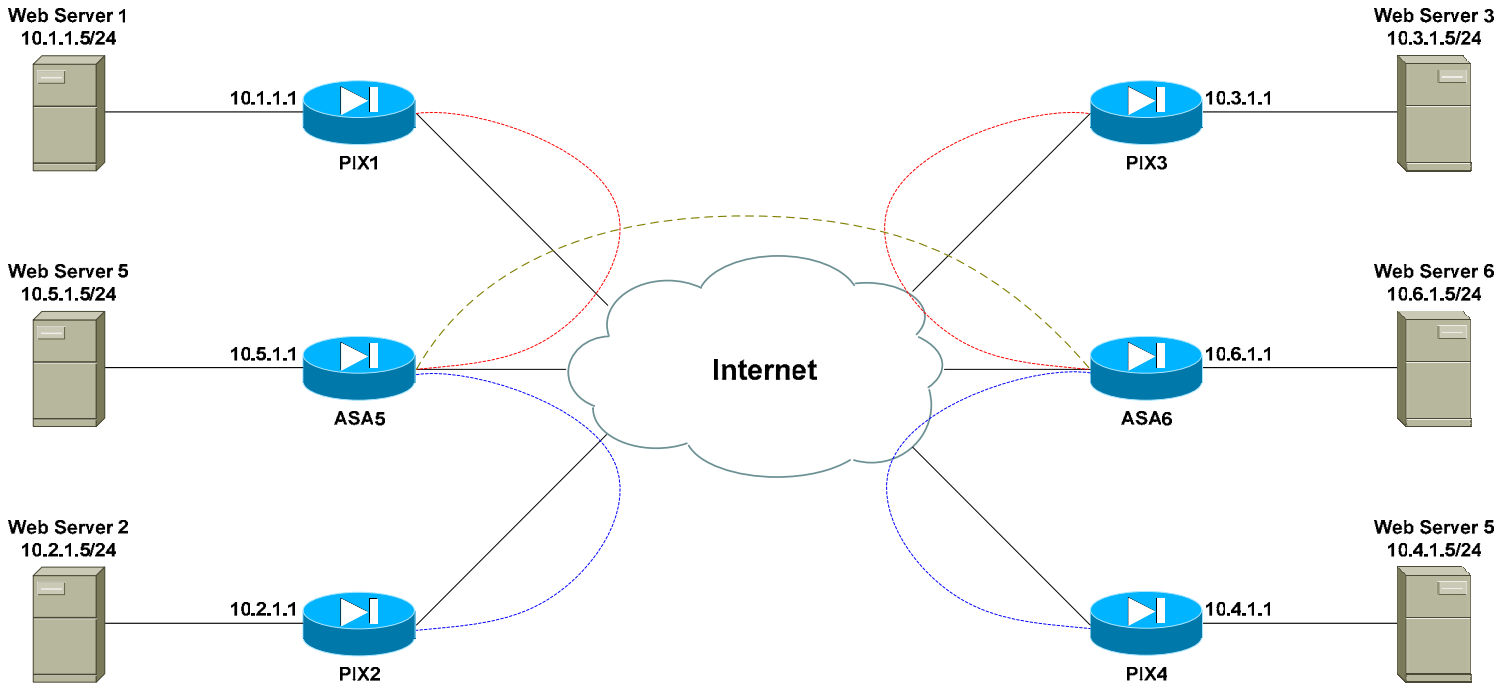


PIX Objectives:

14. Perform whatever additional configuration is necessary to allow Web Server 1 to access Web Server 3 by its private address, **without creating a direct VPN tunnel between PIX1 and PIX3.**

15. Perform whatever additional configuration is necessary to allow Web Server 2 to access Web Server 4 by its private address, **without creating a direct VPN tunnel between PIX2 and PIX4.**

Configuring Advanced PIX IPSEC – Lab (continued)

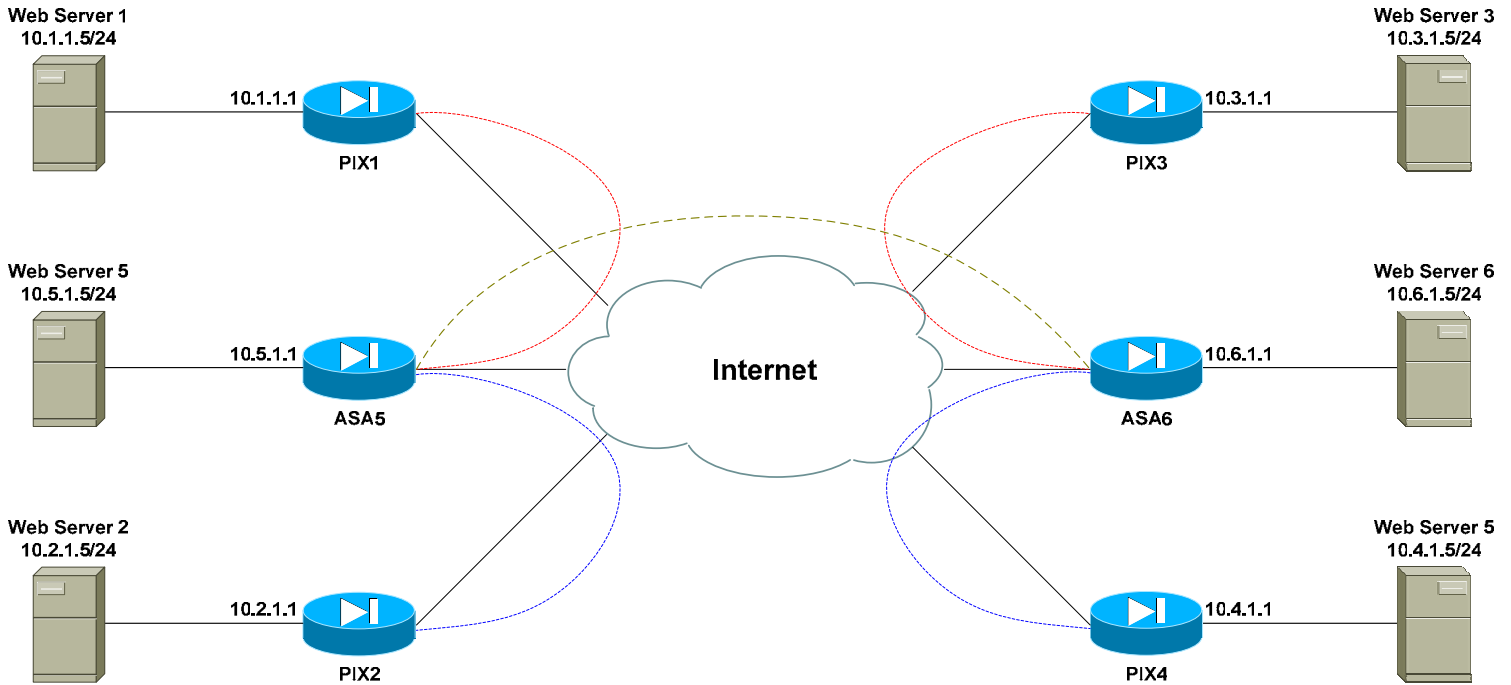


PIX Objectives:

16. Configure all PIX/ASA firewalls to accept incoming client VPN connections from the Internet. Use the following parameters for the VPN Group Policy:

- Group Name: ClientVPN x (where x is your PIX/ASA number)
- Group Password: CISCO
- IP Pool: 10. x .10.1 – 5 /24
- Domain Name: mydomain.net
- DNS Server: 10. x .1.10

Configuring Advanced PIX IPSEC – Lab (continued)

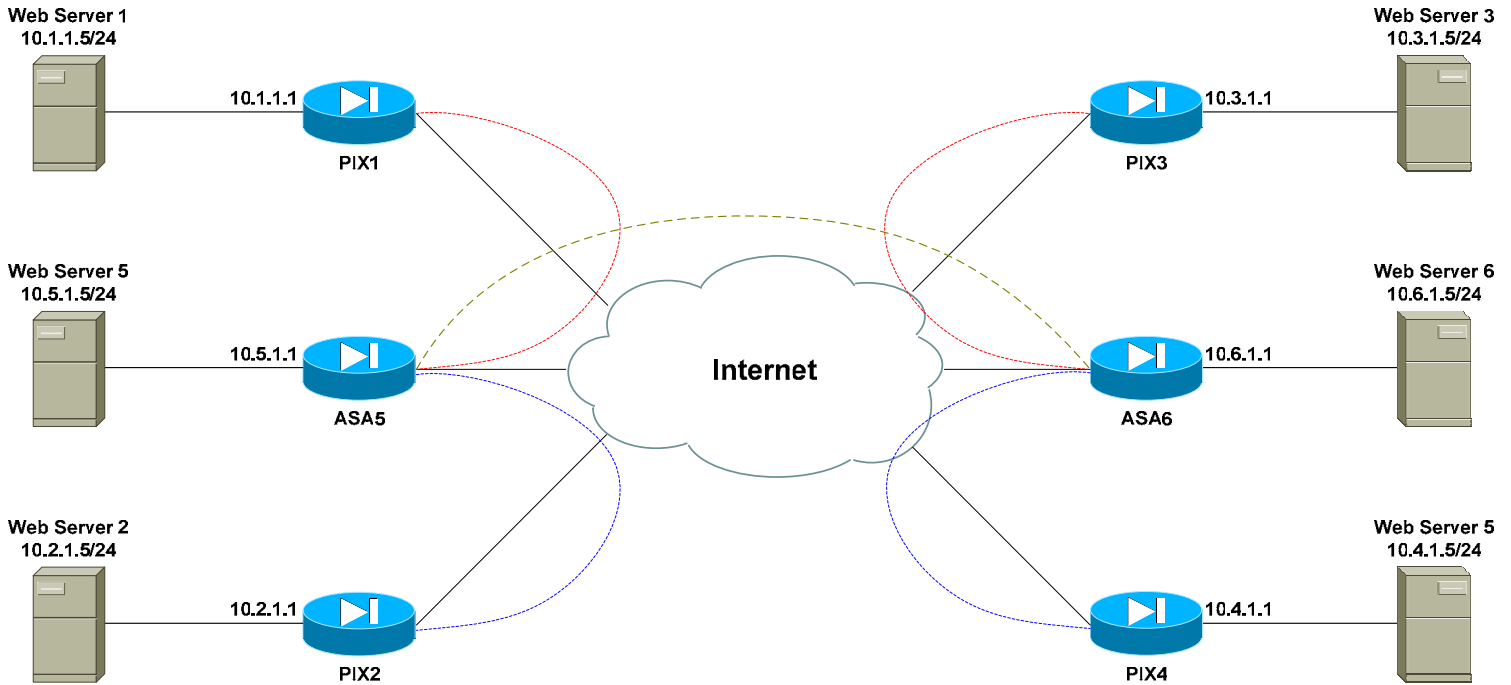


PIX Objectives:

17. Use a local username and password database on the PIX/ASA firewall to authenticate users. At a minimum, create a user named 'cisco' with a password of 'cisco'. Feel free to create additional accounts as well.

18. Test your new configuration using the Cisco VPN client.

Configuring Advanced PIX IPSEC – Lab (continued)



PIX Objectives:

19. Remove any locally created usernames/passwords on each PIX/ASA.

Install RADIUS on each Web Server. At a minimum, create a user named ‘user’ with a password of ‘user’. Feel free to create additional accounts as well. Use this RADIUS server to authenticate client VPN users. Use a key of CISCO between the RADIUS servers and each PIX/ASA.

20. Test your new configuration using the Cisco VPN client.
