# Newer Cisco SBA Guides Available

This guide is part of an older series of Cisco Smart Business Architecture designs. To access the latest Cisco SBA Guides, go to http://www.cisco.com/go/sba

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a new series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

SBA

SBA

BORDERLESS NETWORKS

DEPLOYMENT GUIDE

# IPv6 DMZ Web Service Deployment Guide

SMART BUSINESS ARCHITECTURE

August 2012 Series

# Preface

## Who Should Read This Guide

This Cisco® Smart Business Architecture (SBA) guide is for people who fill a variety of roles:

- Systems engineers who need standard procedures for implementing solutions
- Project managers who create statements of work for Cisco SBA implementations
- Sales partners who sell new technology or who create implementation documentation
- Trainers who need material for classroom instruction or on-the-job training

In general, you can also use Cisco SBA guides to improve consistency among engineers and deployments, as well as to improve scoping and costing of deployment jobs.

## Release Series

Cisco strives to update and enhance SBA guides on a regular basis. As we develop a series of SBA guides, we test them together, as a complete system. To ensure the mutual compatibility of designs in Cisco SBA guides, you should use guides that belong to the same series.

The Release Notes for a series provides a summary of additions and changes made in the series.

All Cisco SBA guides include the series name on the cover and at the bottom left of each page. We name the series for the month and year that we release them, as follows:

**month year** Series

For example, the series of guides that we released in August 2012 are the "August 2012 Series".

You can find the most recent series of SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel

## How to Read Commands

Many Cisco SBA guides provide specific details about how to configure Cisco network devices that run Cisco IOS, Cisco NX-OS, or other operating systems that you configure at a command-line interface (CLI). This section describes the conventions used to specify commands that you must enter.

Commands to enter at a CLI appear as follows:

```
configure terminal
```

Commands that specify a value for a variable appear as follows:

```
ntp server 10.10.48.17
```

Commands with variables that you must define appear as follows:

```
class-map [highest class name]
```

Commands shown in an interactive example, such as a script or when the command prompt is included, appear as follows:

```
Router# enable
```

Long commands that line wrap are underlined. Enter them as one command:

```
wrr-queue random-detect max-threshold 1 100 100 100 100 100
100 100 100
```

Noteworthy parts of system output or device configuration files appear highlighted, as follows:

```
interface Vlan64
  ip address 10.5.204.5 255.255.255.0
```

## Comments and Questions

If you would like to comment on a guide or ask questions, please use the SBA feedback form.

If you would like to be notified when new comments are posted, an RSS feed is available from the SBA customer and partner pages.

# Table of Contents

# What's In This SBA Guide

## Cisco SBA Borderless Networks

Cisco SBA helps you design and quickly deploy a full-service business network. A Cisco SBA deployment is prescriptive, out-of-the-box, scalable, and flexible.

Cisco SBA incorporates LAN, WAN, wireless, security, data center, application optimization, and unified communication technologies—tested together as a complete system. This component-level approach simplifies system integration of multiple technologies, allowing you to select solutions that solve your organization's problems—without worrying about the technical complexity.

Cisco SBA Borderless Networks is a comprehensive network design targeted at organizations with up to 10,000 connected users. The SBA Borderless Network architecture incorporates wired and wireless local area network (LAN) access, wide-area network (WAN) connectivity, WAN application optimization, and Internet edge security infrastructure.

## Route to Success

To ensure your success when implementing the designs in this guide, you should first read any guides that this guide depends upon—shown to the left of this guide on the route below. As you read this guide, specific prerequisites are cited where they are applicable.

## About This Guide

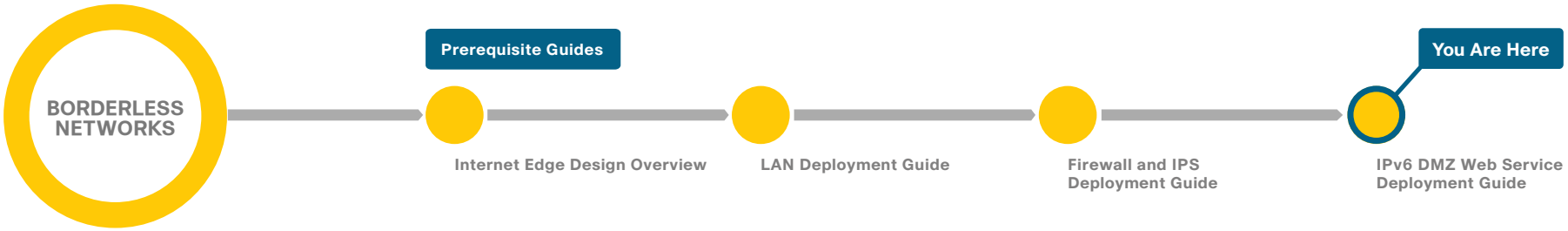
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- Business Overview—Describes the business use case for the design. Business decision makers may find this section especially useful.
- Technology Overview—Describes the technical design for the business use case, including an introduction to the Cisco products that make up the design. Technical decision makers can use this section to understand how the design works.
- Deployment Details—Provides step-by-step instructions for deploying and configuring the design. Systems engineers can use this section to get the design up and running quickly and reliably.
- You can find the most recent series of Cisco SBA guides at the following sites:

You can find the most recent series of Cisco SBA guides at the following sites:

Customer access: http://www.cisco.com/go/sba

Partner access: http://www.cisco.com/go/sbachannel



# Introduction

## Business Overview

IPv4 addresses are becoming harder to get and eventually will no longer be available. The last IPv4 allocations have been handed out by the Internet Assigned Numbers Authority (IANA), and the Regional Internet Registries (RIRs) will run out of IPv4 addresses at some point. Technologies like Network Address Translation (NAT) and the use of RFC 1918 addressing will allow most organizations to continue operating on IPv4 for the foreseeable future, but the transition to IPv6 is coming, and new devices and organizations will begin running on IPv6 soon.

Most customer interaction currently happens over IPv4, but the transition to IPv6 is already occurring in some regions of the world and will quickly spread worldwide. Many governments are mandating the use of IPv6 in government, education, and public Internet deployments. If you plan and implement IPv6 in parallel to IPv4 today, you can help ensure that you can connect to new customers and markets tomorrow.

## Technology Overview

Cisco Smart Business Architecture (SBA) easily accommodates IPv6 Internet Edge servers. This guide describes how your organization can stay ahead of the technology curve by providing Internet server access via native IPv6 without interruption to IPv4 clients. A network supporting dual stacks—IPv4 and IPv6 simultaneously—allows for IPv4 and IPv6 to coexist.

This guide shows how to use existing hardware in the Internet Edge to support native IPv6 access to Internet-facing services, a web server in this example.

IPv6 can be added to the Cisco SBA Internet Edge through additional configuration of existing software that is specified for the existing IPv4 Internet Edge. After you perform the procedures in this guide, both IPv4 and IPv6 networks will coexist on the same equipment but will be logically separate.

IPv4 will be in use for years to come; during the migration to IPv6, it is critical to support both address spaces. This configuration builds an IPv6 infrastructure upon the existing IPv4 network. This configuration is intended to be an add-on to the existing foundation deployment; it will not function properly on its own.

The solution described in this guide accommodates IPv6 web traffic, specifically HTTP and HTTPS web traffic to and from the Internet Edge. This solution assumes:

- The ISP has provisioned an IPv6 Ethernet handoff.
- The Internet Edge routers in this diagram are in the provider network and are not included as part of the configuration.
- The Internet Edge routers will have a route directing IPv6 traffic to the networks that are hosted on the organization's Cisco Adaptive Security Appliances (ASA) firewall.
- IPv6 connectivity from the ISP border router will terminate on a pair of resilient Cisco ASA firewalls.

The Cisco ASA firewalls provide the following:

- Termination of the ISP IPv6 connection
- Static routing to the ISP network
- Security with IPv6 access control lists (ACLs)
- Intrusion prevention for servers in the IPv6 DMZ

As you plan for your IPv6 deployment, you need to take your organization's security policy into account. IPv6 is a different protocol, but applications operate the same as they do over IPv4. The Cisco ASA firewall for IPv4 provides application inspection and IPS for applications running over IPv6. The IPv4 security policy deployed currently in the Internet Edge deployment carries over to IPv6 networking. This design configures ACLs that permit HTTP and HTTPS traffic.

### Domain Name System for IPv6

Domain Name System (DNS) for IPv6 is handled by the ISP in the example in this guide. IPv6 introduces the AAAA record, which maps an IPv6 address to a host. This is similar to an A record in IPv4 DNS, which maps an IPv4 address to a host. In the configuration described in this guide, you do not have to deploy IPv6 DNS on the server. However, the ISP does need to deploy IPv6 DNS to propagate the web server's address to IPv6 clients on the Internet.

# Deployment Details

The Cisco ASA firewalls configured in the Internet Edge are configured and managed via IPv4, and this will not change with this configuration. The Internet Edge guidance in the Firewall and IPS Deployment Guide provides for IPv4 connectivity, high availability, and management. Existing IPv4 connectivity is not affected by the configuration described in this guide.

## Recommended Deployment Setup for IPv6 Internet Edge

This guide uses IPv6 addresses from the range 2001:0db8::/32, which is a non-Internet-routable range, defined in RFC 3849, for use in documentation. Internet-routable IPv6 address space can be obtained from an ISP or provider-independent space allocated by a local RIR.

*Figure 1 - IPv6 Internet Edge deployment architecture*

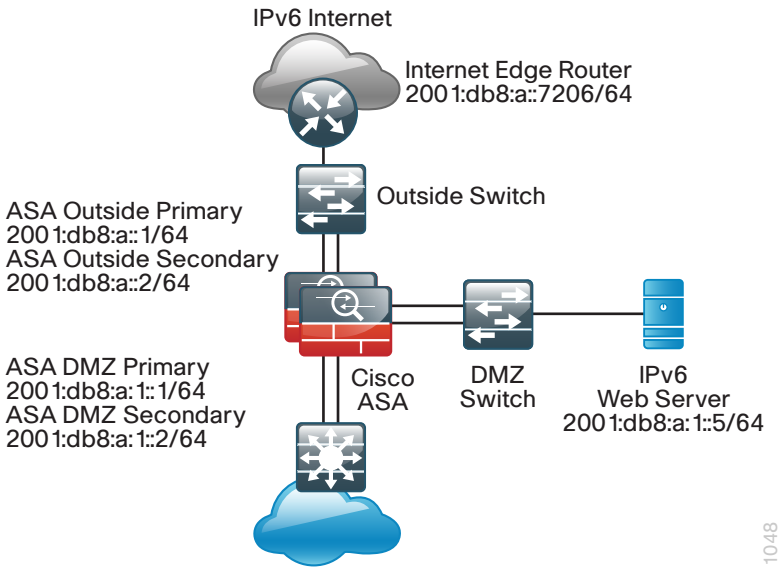



*Table 1 - IPv6 addresses for this configuration*

| Endpoint | IPv6 address |
|---|---|
| ISP Internet Edge Router | 2001:db8:a::7206/64 |
| ASA Outside Interface Primary | 2001:db8:a::1/64 |
| ASA Outside Interface Secondary | 2001:db8:a::2/64 |
| ASA DMZ Interface Primary | 2001:db8:a:1::1/64 |
| ASA DMZ Interface Secondary | 2001:db8:a:1::2/64 |
| Web server in DMZ | 2001:db8:a:1::5/64 |

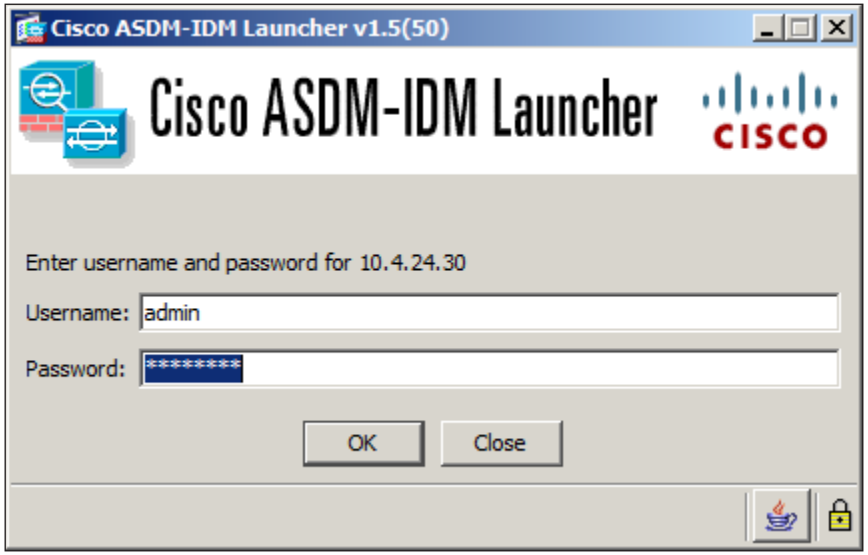
### Process

Configuring IPv6 on the Cisco ASA Firewall

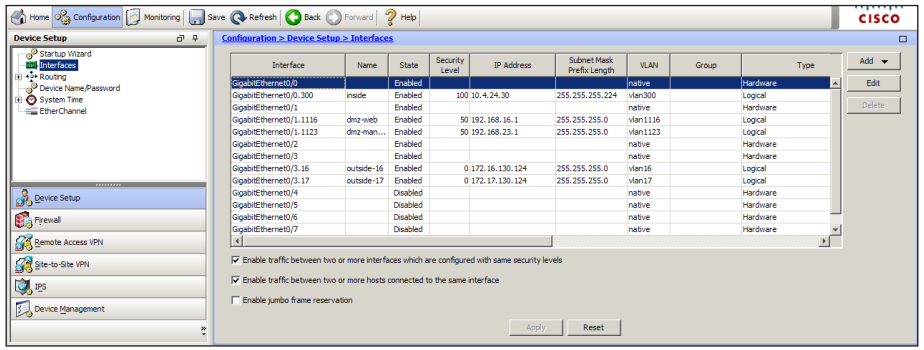
1. Configure IPv6 on Cisco ASA interfaces
2. Configure high availability for IPv6
3. Configure static routing for IPv6

## Procedure 1 Configure IPv6 on Cisco ASA interfaces

**Step 1:** Connect to Cisco Adaptive Security Device Manager (ASDM) by navigating to https://<ASA-IP-Address>/admin, and then logging in with your username and password.

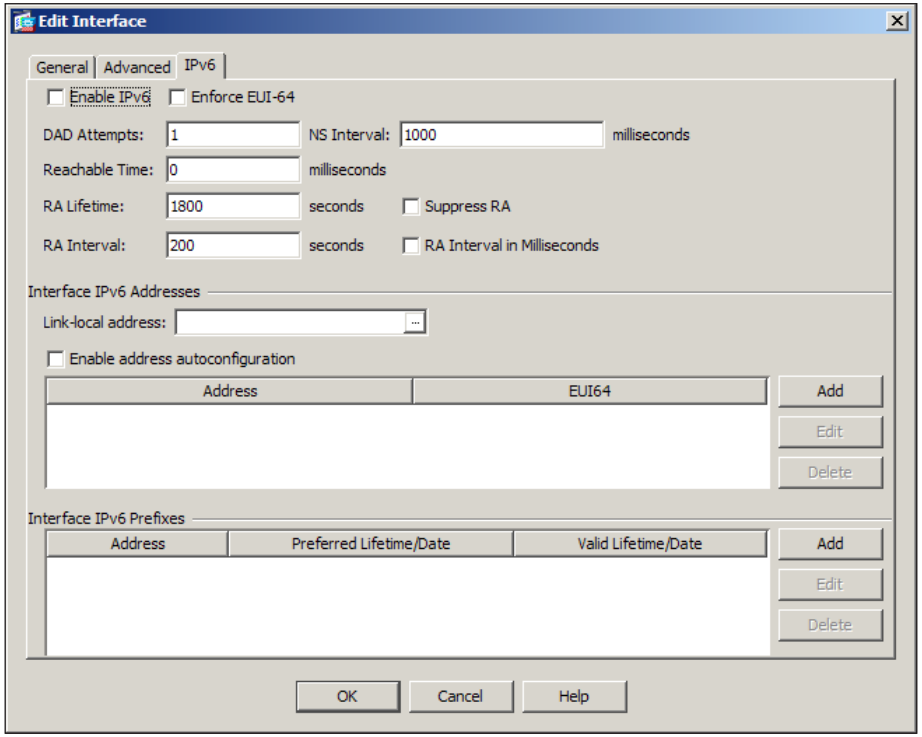



**Step 2:** Navigate to **Configuration > Device Setup > Interfaces.**

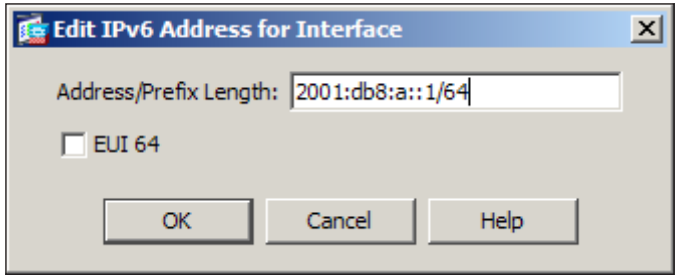



**Step 3:** Select the primary outside interface, **outside-16** in this example, and then click **Edit**. The Edit Interface dialog box appears.

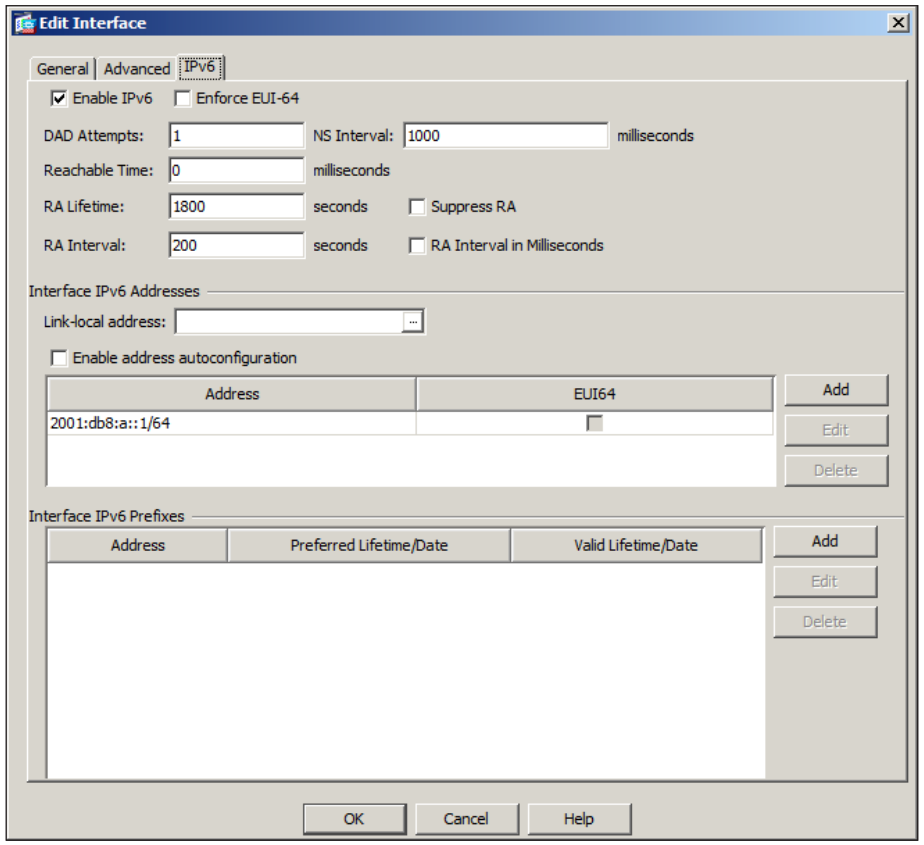
**Step 4:** In the Edit Interface dialog box, click the **IPv6** tab, select **Enable IPv6,** and then, under Interface IPv6 Addresses, click **Add.**




**Step 5:** Enter the outside IPv6 address, **2001:db8:a::1/64**, and then click **OK**.

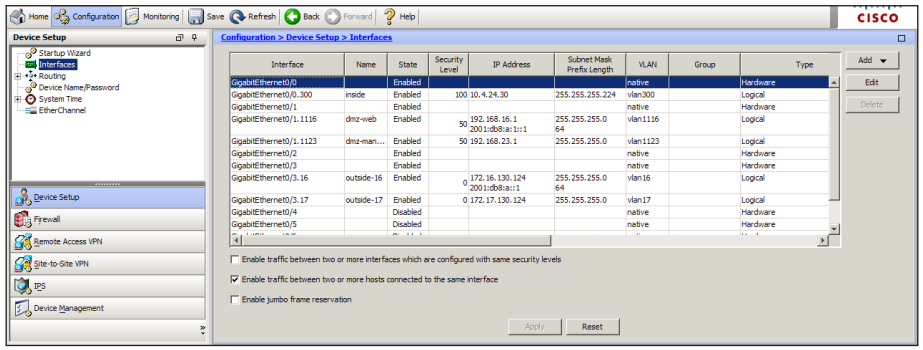


In the Edit Interface dialog box, under Interface IPv6 Addresses, the IPv6 address appears.




**Step 6:** Repeat Step 3 through Step 5, selecting the **dmz-web** interface and using the IPv6 address **2001:db8:a:1::1/64**.

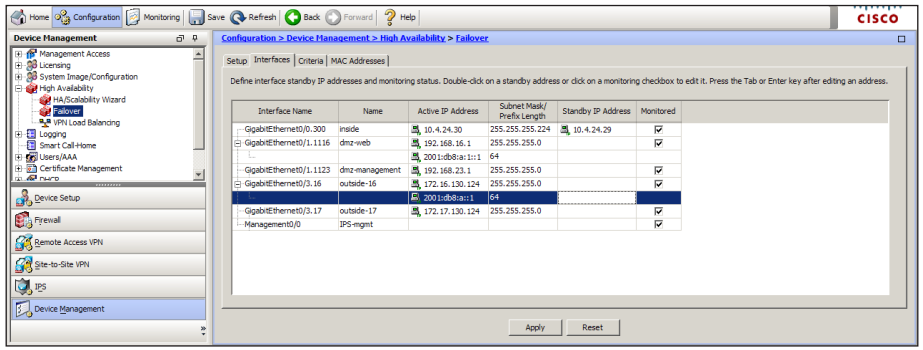
**Step 7:** At the bottom of the window, click **Apply**. This saves the configuration.




## Procedure 2 Configure high availability for IPv6

High availability allows the firewall to continue operating in the event of a failure. To ensure that failover works properly, for each interface configured for IPv6 you must configure a high availability IPv6 address for the secondary Cisco ASA interface.

**Step 1:** Navigate to **Configuration > Device Management > High Availability > Failover > Interfaces.** On the Interfaces tab, the interfaces configured for IPv4 and IPv6 are displayed.



**Step 2:** Select the IPv6 outside interface, **outside-16** in this example, click the empty **Standby IP Address** field, type the failover IPv6 address **2001:db8:a::2**, and then press **Enter**.

| | | | | | |
|---|---|---|---|---|---|
| GigabitEthernet0/3.16 | outside-16 | 172.16.132.124 | 255.255.255.0 | 172.16.132.123 | ☑ |
| | | 2001:db8:a::1 | 64 | 2001:db8:a::2 | |

**Step 3:** Select the IPv6 **dmz-web** interface, click the empty **Standby IP Address** field, type the failover IPv6 address **2001:db8:a:1::2**, and then press **Enter**.

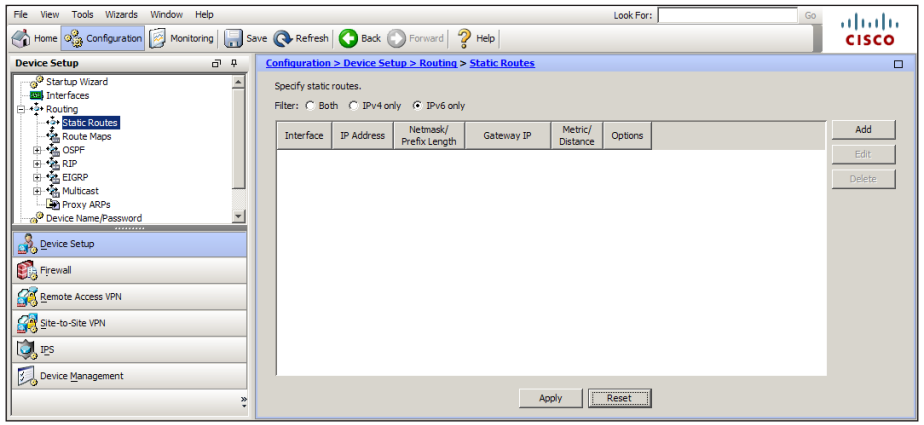
| | | | | | |
|---|---|---|---|---|---|
| GigabitEthernet0/1.1116 | dmz-web | 192.168.16.1 | 255.255.255.0 | 192.168.16.2 | ☑ |
| | | 2001:db8:a:1::1 | 64 | 2001:db8:a:1::2 | |

**Step 4:** At the bottom of the window, click **Apply**. This saves the configuration.

## Procedure 3 Configure static routing for IPv6

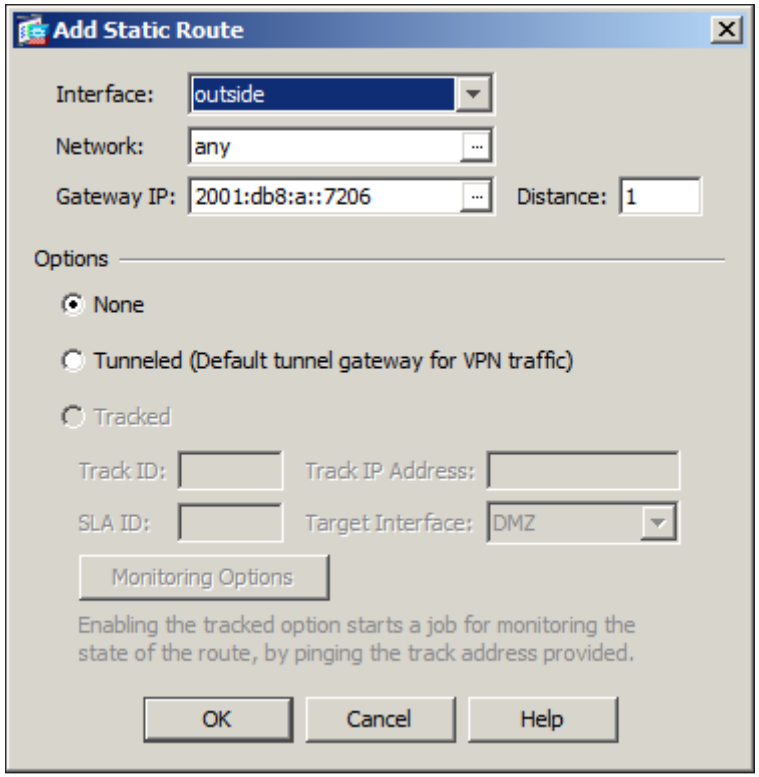
Next, on the Cisco ASA interface, configure static routing for IPv6 Internet access. This setup uses a static default route to send IPv6 traffic to the ISP.

**Step 1:** Navigate to **Configuration** > **Device Setup** > **Routing** > **Static Routes**, select **IPv6 only**, and then click **Add**. The Add Static Route dialog box appears.

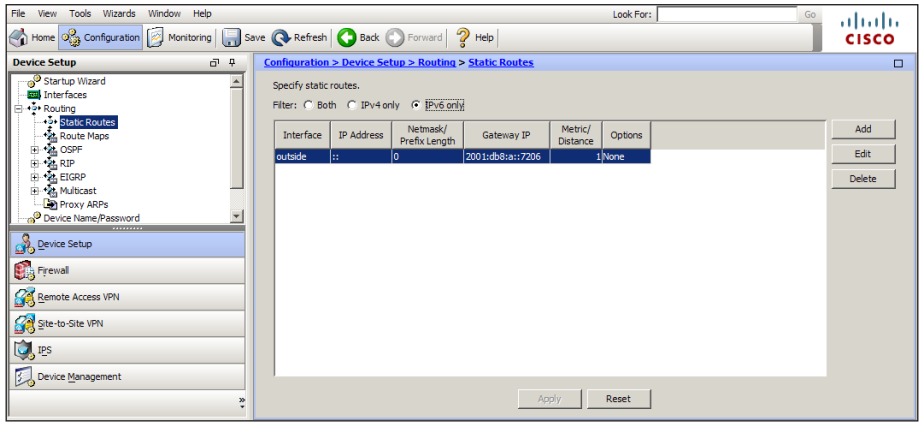



**Step 2:** In the Add Static Route dialog box, enter the values below, and then click **OK**.

- Interface—**outside-16**
- Network—**any**
- Gateway IP—**2001:db8:a::7206**



The static route table reflects the new values.




**Step 3:** At the bottom of the window, click **Apply**. This saves the configuration.

## Process

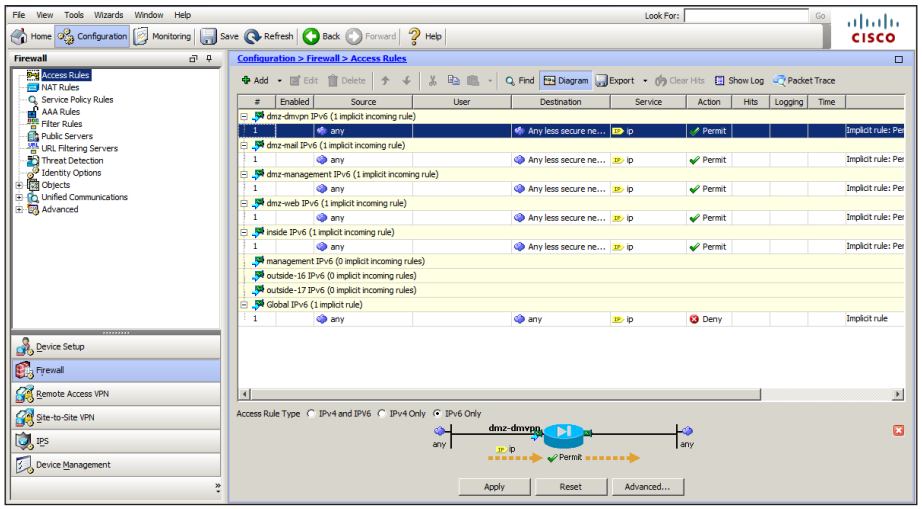
Configuring Cisco ASA Interfaces to Permit Access to IPv6 Web Servers

1. Add a rule to permit HTTP/HTTPS traffic

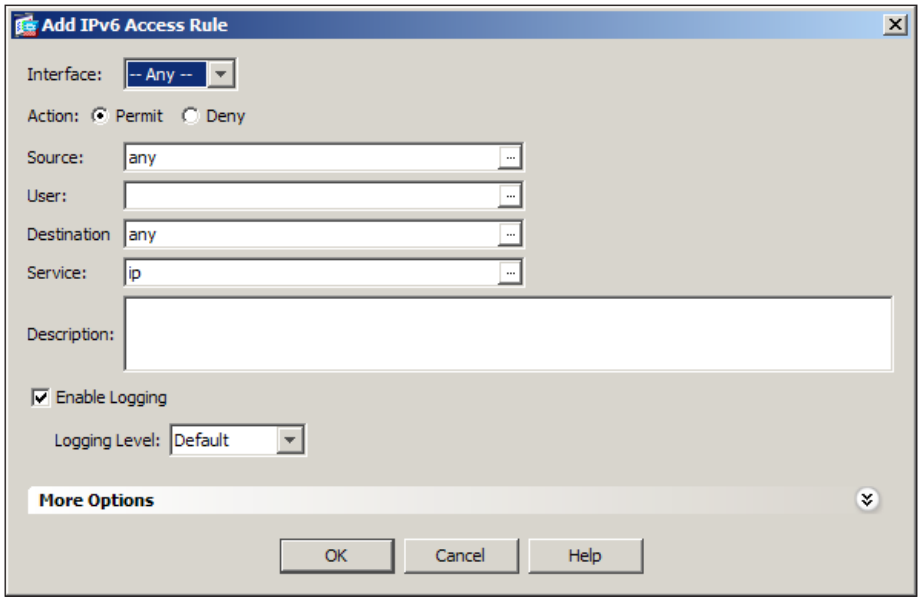
## Procedure 1 Add a rule to permit HTTP/HTTPS traffic

When you perform this procedure to create a rule to permit HTTP and HTTPS traffic to the IPv6-enabled web server, you create an object group for the IPv6 network in the DMZ. Network objects make it easier to read the firewall configuration and can help reduce errors; it is recommended that you build network objects as you add firewall rules.

**Step 1:** Navigate to **Configuration > Firewall > Access Rules**, select **IPv6 Only**, select **Global IPv6,** and then click **Add**.



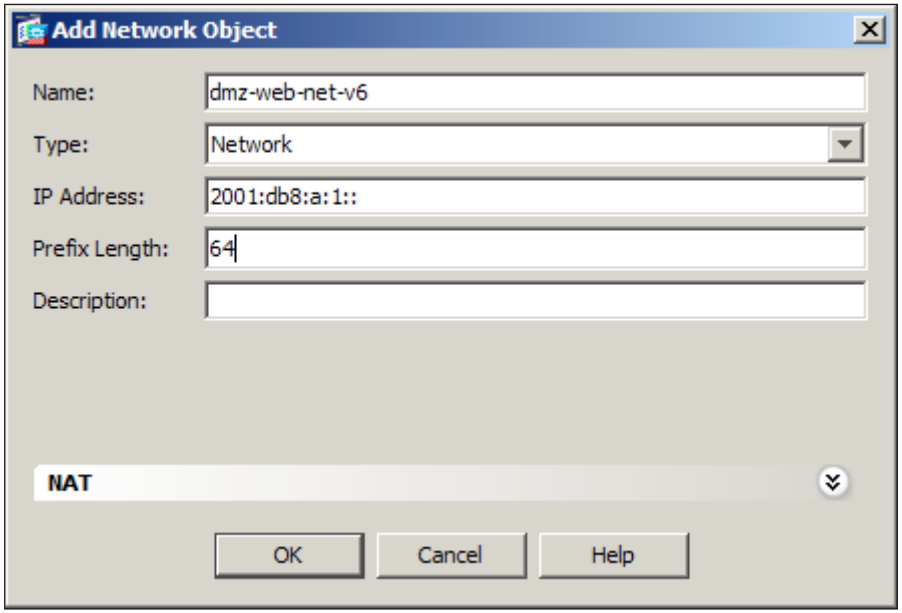

**Step 2:** In the Add IPv6 Access Rule dialog box, ensure that **Interface** is set to **Any, and then** in the **Destination** text box, click the ellipsis button **(...)**.




**Step 3:** In the Browse Destination dialog box, click **Add**, and then select **Network Object**.

**Step 4:** In the Add Network Object dialog box, enter the values listed below, and then click **OK.**

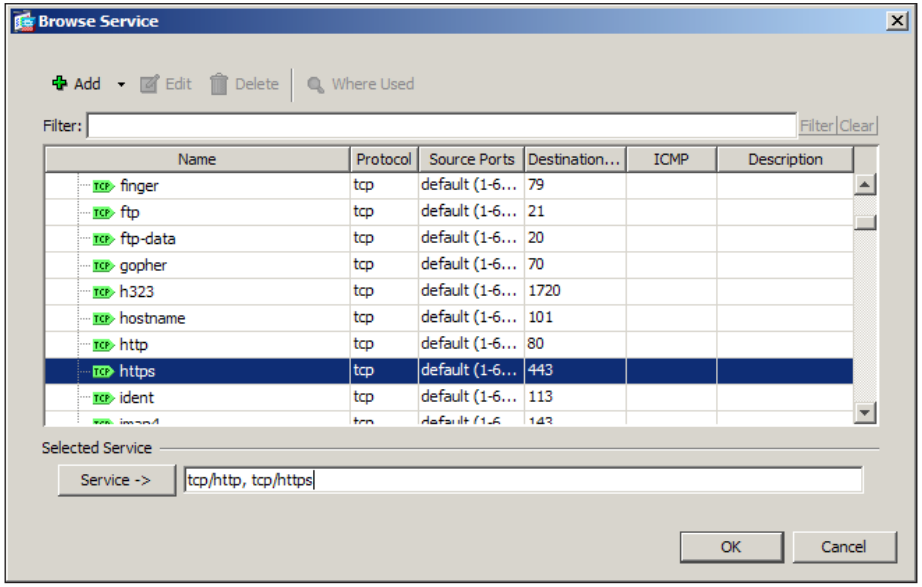
- Name—dmz-web-net-v6
- Type—Network
- IP Address—2001:db8:a:1::
- Prefix Length—64



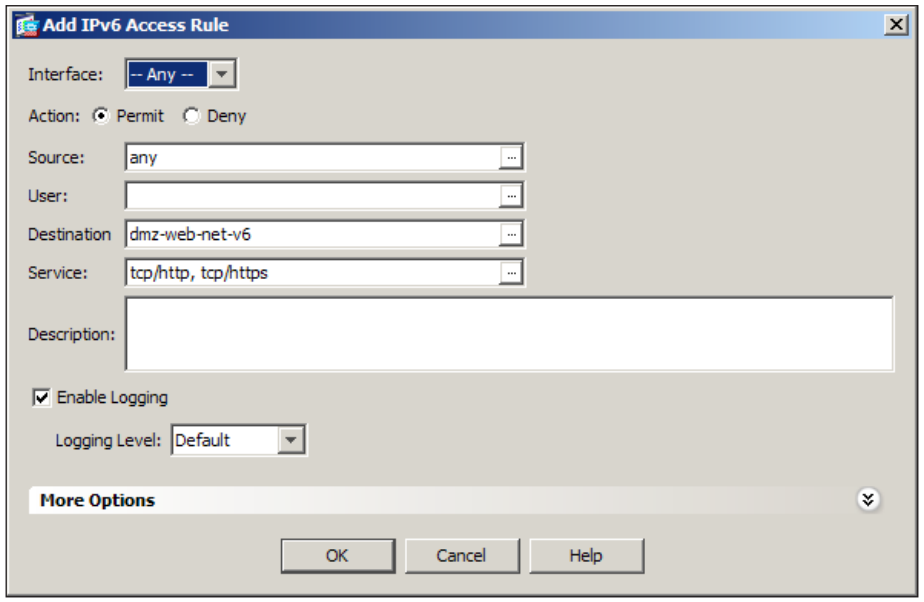

**Step 5:** Double-click the network object that was just created, and then click **OK.**

**Step 6:** In the Add IPv6 Access Rule dialog box, in the **Service** text box, click the ellipsis button **(...)**.

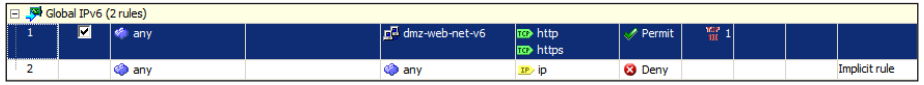
**Step 7:** In the Browse Service dialog box, scroll down and double-click **http** and **https**, and then click **OK.**



**Step 8:** Verify that the Add IPv6 Access Rule dialog box resembles the following illustration, and then click **OK**.




The rule that was just created will appear in the Global IPv6 rule table.




**Step 9:** At the bottom of the window, click **Apply**. This saves the configuration.

## Process

Configuring IPv6 on the DMZ Web Server

1. Configure IPv6 on a Windows 2008 Server

## Procedure 1 Configure IPv6 on a Windows 2008 Server

In this procedure, you configure the Cisco ASA network interface on a Windows 2008 server to support IPv6.

**Step 1:** From the Windows Server 2008 GUI, click **Start**, right-click **Network**, and then click **Properties**. The Network and Sharing Center opens.

**Step 2:** Click **Change Adapter Settings**.


**Step 3:** Right-click the Ethernet interface, and then click **Properties**.

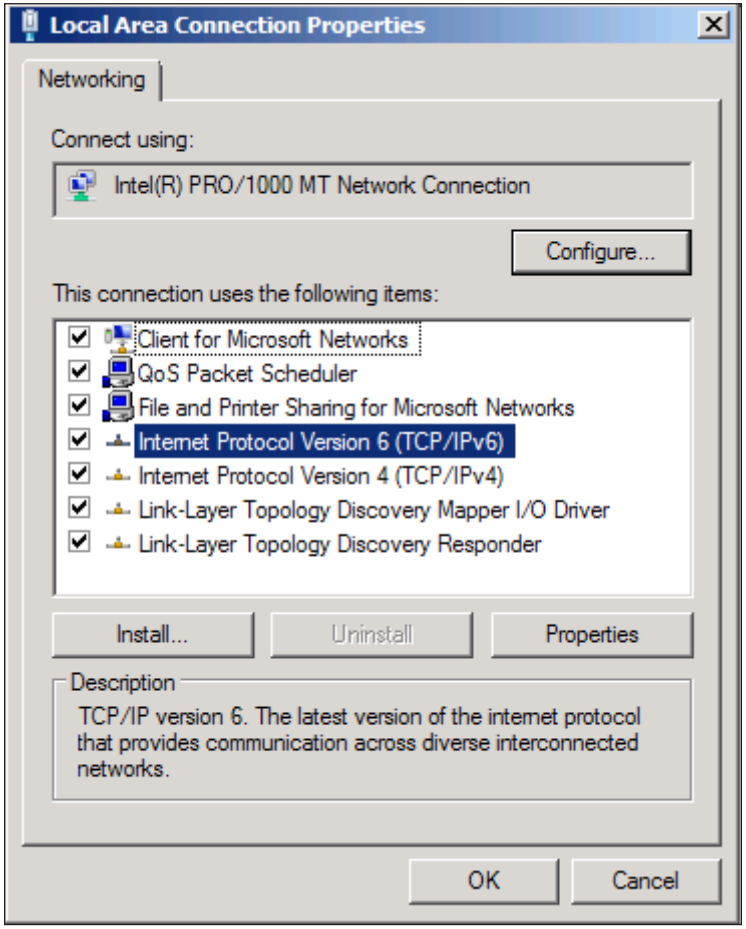
**Step 4:** If the **Internet Protocol Version 6 (TCP/IPv6)** check box is not selected, select it, click **OK**, and then repeat Step 3.

If the **Internet Protocol Version 6 (TCP/IPv6)** check box is selected, proceed to the following step.

### Tech Tip

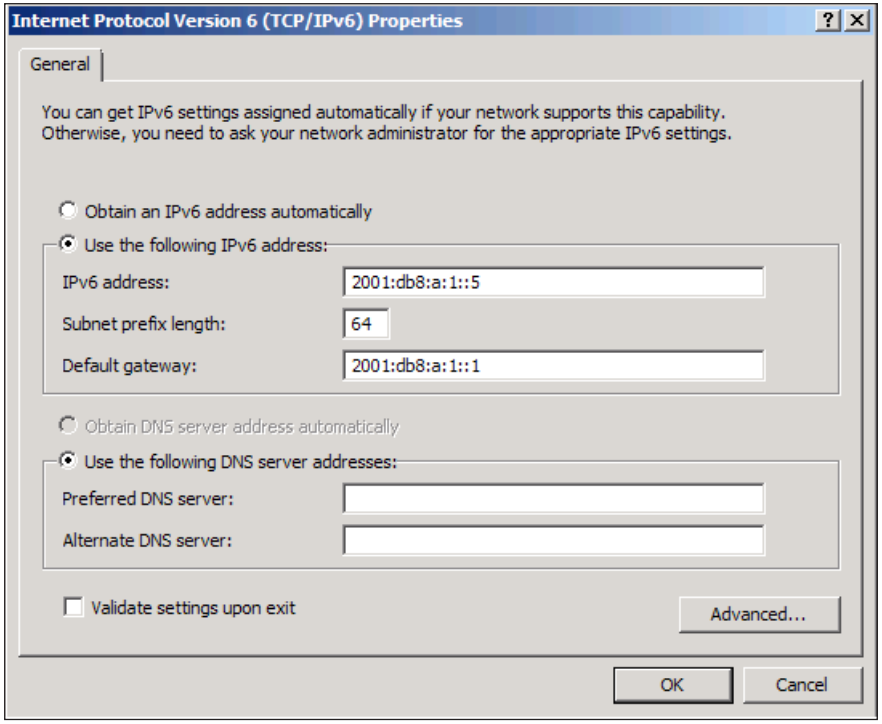
If you do not close and reopen the page the first time you enable IPv6, you will get an error and be unable to provision an IPv6 address.

**Step 5:** Click to highlight **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.



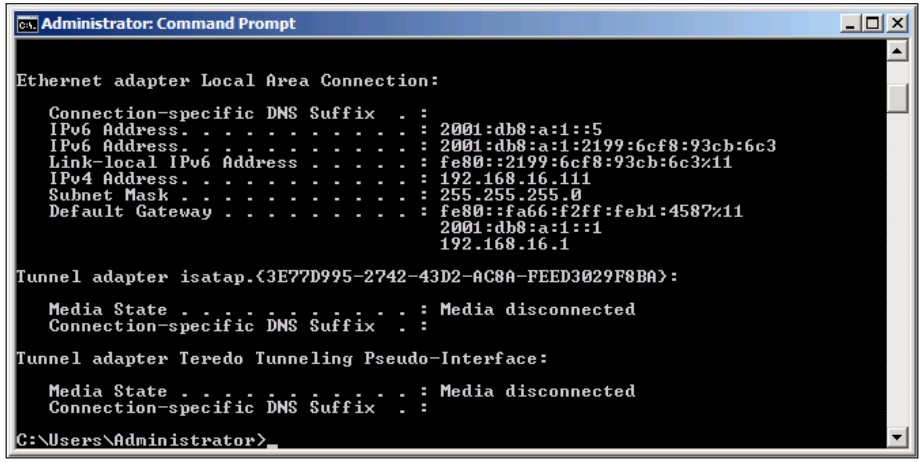

**Step 6:** In the Internet Protocol Version 6 (TCP/IPv6) Properties **dialog box,** select **Use the following IPv6 address**, enter the following values, and then click **OK**.

- IPv6 Address—2001:db8:a:1::5
- Subnet Prefix Length—64
- Default Gateway—2001:db8:a:1::1



**Step 7:** On the Ethernet interface, click **OK**. The configuration is complete.

**Step 8:** Verify that the IPv6 configuration is correct by typing **ipconfig** in a command-line window.




## Notes

# Appendix A: Product List

## Internet Edge

| Functional Area | Product Description | Part Numbers | Software |
|---|---|---|---|
| Firewall | Cisco ASA 5545-X IPS Edition - security appliance | ASA5545-IPS-K9 | ASA 8.6(1)1, IPS 7.1(4) E4 |
| | Cisco ASA 5525-X IPS Edition - security appliance | ASA5525-IPS-K9 | |
| | Cisco ASA 5515-X IPS Edition - security appliance | ASA5515-IPS-K9 | |
| | Cisco ASA 5512-X IPS Edition - security appliance | ASA5512-IPS-K9 | |
| | Cisco ASA5512-X Security Plus license | ASA5512-SEC-PL | |
| | Firewall Management | ASDM | 6.6.114 |

# Appendix B: CLI Configuration

## Cisco ASA

```
interface GigabitEthernet0/1.1116
 ipv6 address 2001:db8:a:1::1/64 standby 2001:db8:a:1::2
 ipv6 enable
!
interface GigabitEthernet0/3.16
 ipv6 address 2001:db8:a::1/64 standby 2001:db8:a::2
 ipv6 enable
!
object network dmz-web-net-v6
 subnet 2001:db8:a:1::/64
!
object-group service DM_INLINE_TCP_1 tcp
 port-object eq www
 port-object eq https
!
ipv6 route outside ::/0 2001:db8:a::7206
ipv6 access-list global_access_ipv6 permit tcp any object dmz-
web-net-v6 object-group DM_INLINE_TCP_1
```

**Notes**

# Appendix C: Changes

This appendix summarizes the changes to this guide since the previous Cisco SBA series.

- Updated IP addressing to align with current SBA release.
- Updated screen shots to show current ASA GUI.

**Notes**

## Feedback

Click here to provide feedback to Cisco SBA.

SMART BUSINESS ARCHITECTURE



**Americas Headquarters**
Cisco Systems, Inc.
San Jose, CA

**Asia Pacific Headquarters**
Cisco Systems (USA) Pte. Ltd.
Singapore

**Europe Headquarters**
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.



B-0000205-1 9/12