SBA

BORDERLESS NETWORKS

DEPLOYMENT GUIDE

IPv6 DMZ Web Service Deployment Guide

SMART BUSINESS ARCHITECTURE

February 2013 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 February 2013 is the "February 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

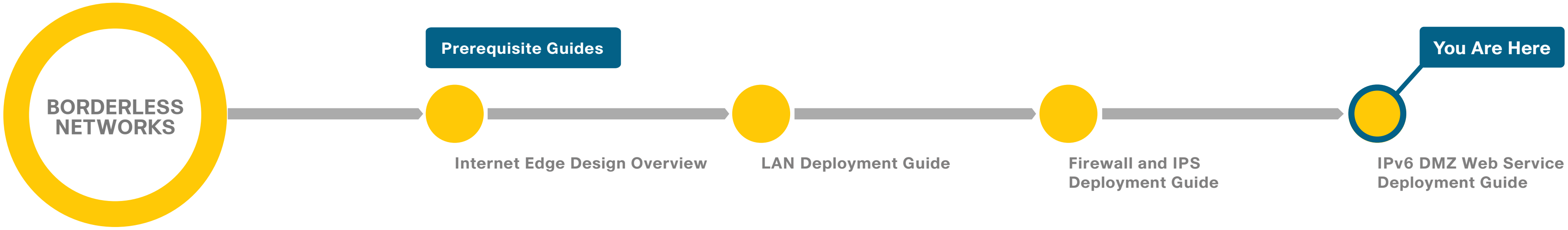
This *deployment guide* contains one or more deployment chapters, which each include the following sections:

- 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:

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

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


BORDERLESS NETWORKS
Prerequisite Guides
Internet Edge Design Overview
LAN Deployment Guide
Firewall and IPS Deployment Guide
You Are Here
IPv6 DMZ Web Service Deployment Guide

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.

In some cases, legacy systems do not support IPv6 or because of business reasons cannot be migrated to IPv6 today. In such cases other means are needed to connect these IPv4-only systems to IPv6 enabled networks during the transition period.

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 two options for connecting existing hardware in the Internet Edge to support IPv6 access to Internet-facing services. One for servers that have native IPv6 support and one for IPv6 Internet addressing translated with NAT64 to an IPv4-only service, 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
- NAT64 translation for IPv6 access to IPv4-only services in the demilitarized zone (DMZ)
- 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 translate the web server's hostname to an IPv6 address for clients on the Internet. During testing it is possible to access the native IPv6 server via its IPv6 address rather than by using DNS, but an IPv6 AAAA DNS record may be needed for the NAT64 configuration to work properly and the service accessed by DNS name rather than IP address.

Notes

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

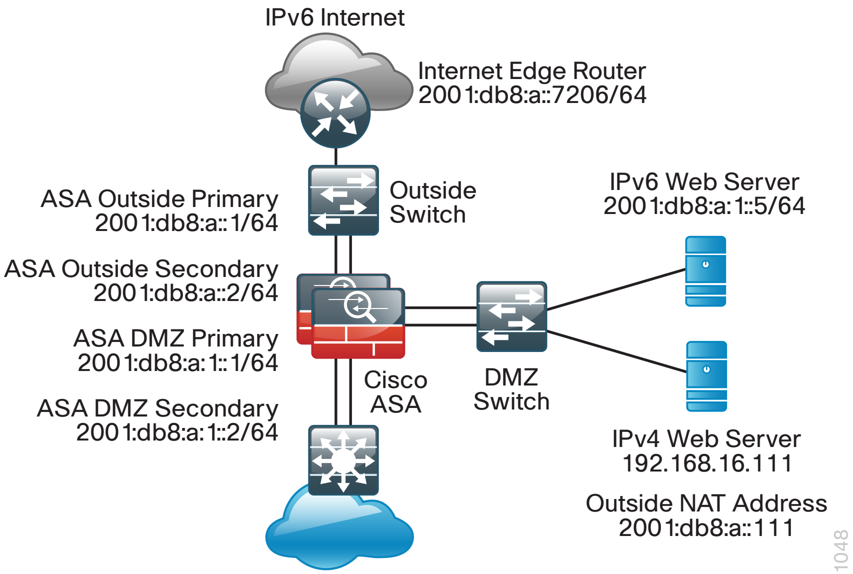


Table 1 - IPv6 addresses for this configuration

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
IPv4 Web server in DMZ	192.168.16.111
IPv4 Web server Outside IPv6 address	2001:db8:a::111/64

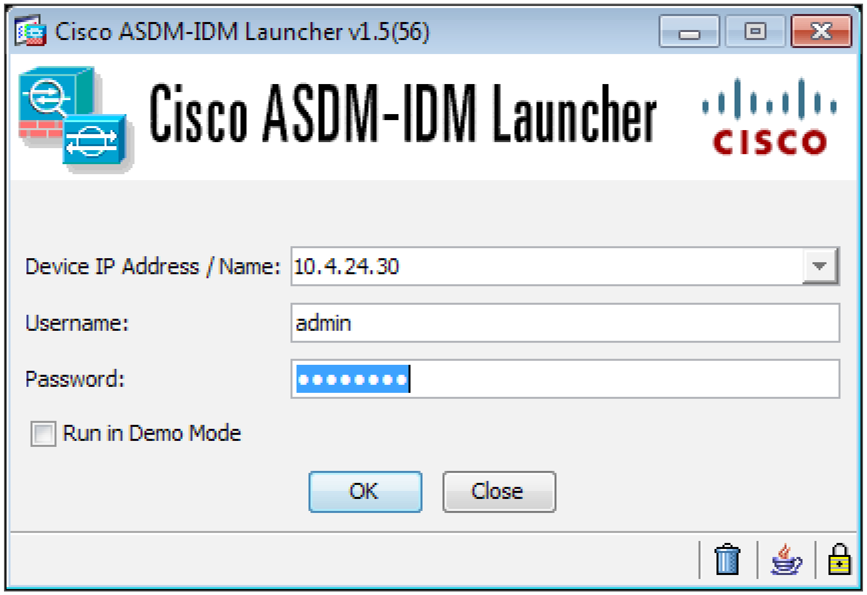
Process

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.



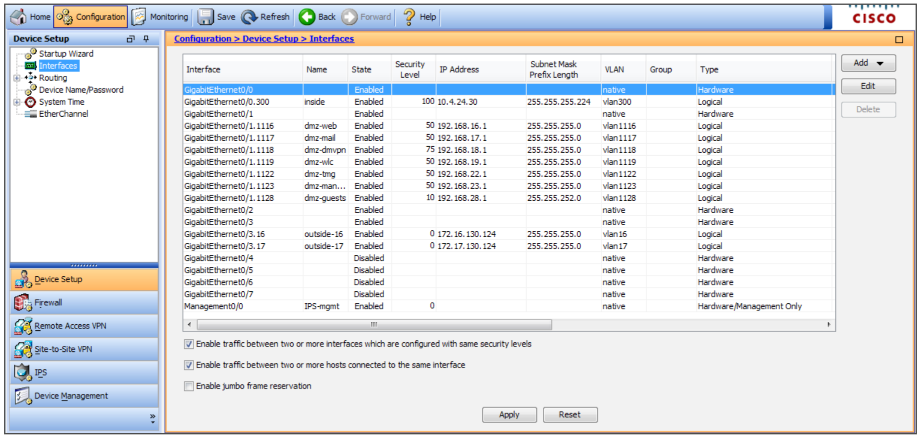
Device IP Address / Name: 10.4.24.30

Username: admin

Password: ●●●●●●●●

□ Run in Demo Mode

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



Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group	Type
GigabitEthernet0/0		Enabled				native		Hardware
GigabitEthernet0/0.300	inside	Enabled	100	10.4.24.30	255.255.255.224	vlan300		Logical
GigabitEthernet0/1		Enabled				native		Hardware
GigabitEthernet0/1.1116	dmz-web	Enabled	50	192.168.16.1	255.255.255.0	vlan1116		Logical
GigabitEthernet0/1.1117	dmz-mail	Enabled	50	192.168.17.1	255.255.255.0	vlan1117		Logical
GigabitEthernet0/1.1118	dmz-dmvpn	Enabled	75	192.168.18.1	255.255.255.0	vlan1118		Logical
GigabitEthernet0/1.1119	dmz-wlc	Enabled	50	192.168.19.1	255.255.255.0	vlan1119		Logical
GigabitEthernet0/1.1122	dmz-tmg	Enabled	50	192.168.22.1	255.255.255.0	vlan1122		Logical
GigabitEthernet0/1.1123	dmz-man...	Enabled	50	192.168.23.1	255.255.255.0	vlan1123		Logical
GigabitEthernet0/1.1128	dmz-guests	Enabled	10	192.168.28.1	255.255.252.0	vlan1128		Logical
GigabitEthernet0/2		Enabled				native		Hardware
GigabitEthernet0/3		Enabled				native		Hardware
GigabitEthernet0/3.16	outside-16	Enabled	0	172.16.130.124	255.255.255.0	vlan16		Logical
GigabitEthernet0/3.17	outside-17	Enabled	0	172.17.130.124	255.255.255.0	vlan17		Logical
GigabitEthernet0/4		Disabled				native		Hardware
GigabitEthernet0/5		Disabled				native		Hardware
GigabitEthernet0/6		Disabled				native		Hardware
GigabitEthernet0/7		Disabled				native		Hardware
Management0/0	IPS-mgmt	Enabled	0			native		Hardware/Management Only

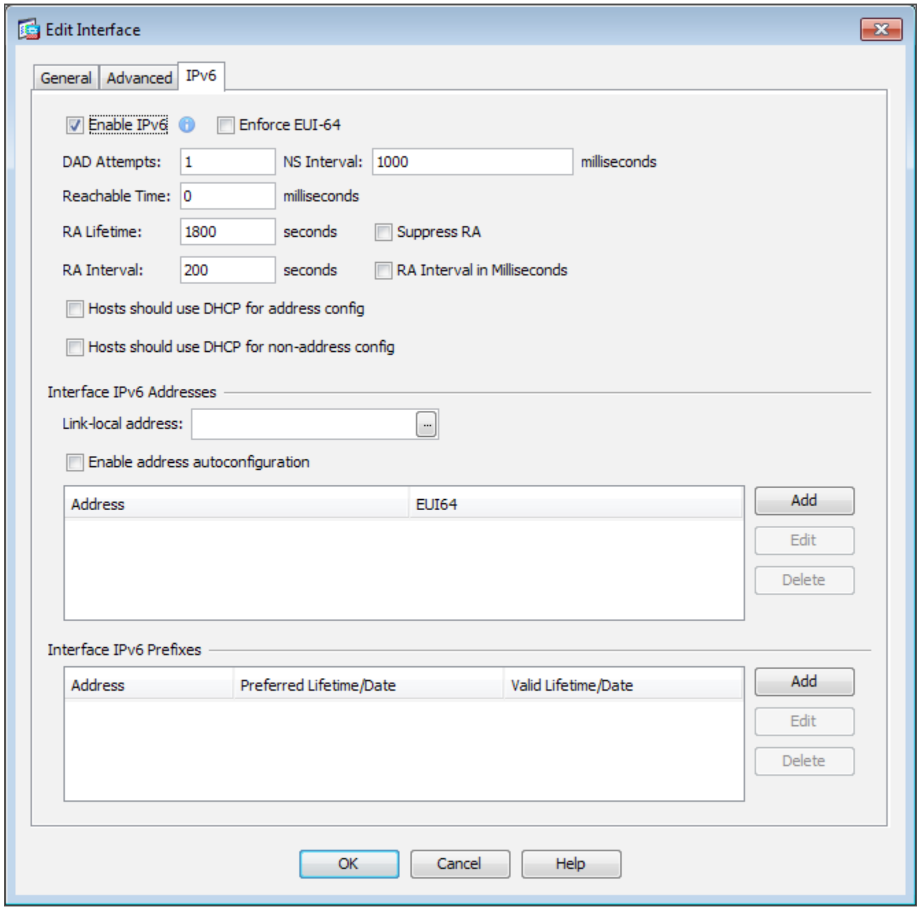
☑ Enable traffic between two or more interfaces which are configured with same security levels

☑ Enable traffic between two or more hosts connected to the same interface

□ Enable jumbo frame reservation

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

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



☑ Enable IPv6 □ Enforce EUI-64

DAD Attempts: 1 NS Interval: 1000 milliseconds

Reachable Time: 0 milliseconds

RA Lifetime: 1800 seconds □ Suppress RA

RA Interval: 200 seconds □ RA Interval in Milliseconds

□ Hosts should use DHCP for address config

□ Hosts should use DHCP for non-address config

Interface IPv6 Addresses

Link-local address:

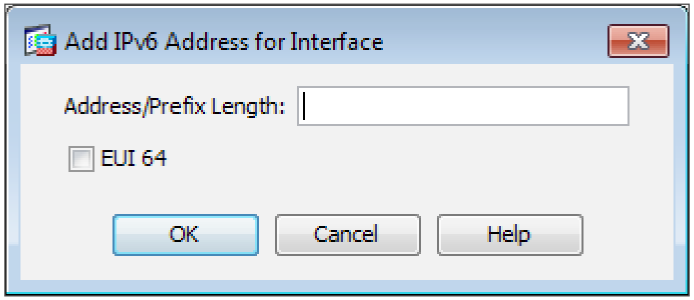
□ Enable address autoconfiguration

Address	EUI64

Interface IPv6 Prefixes

Address	Preferred Lifetime/Date	Valid Lifetime/Date

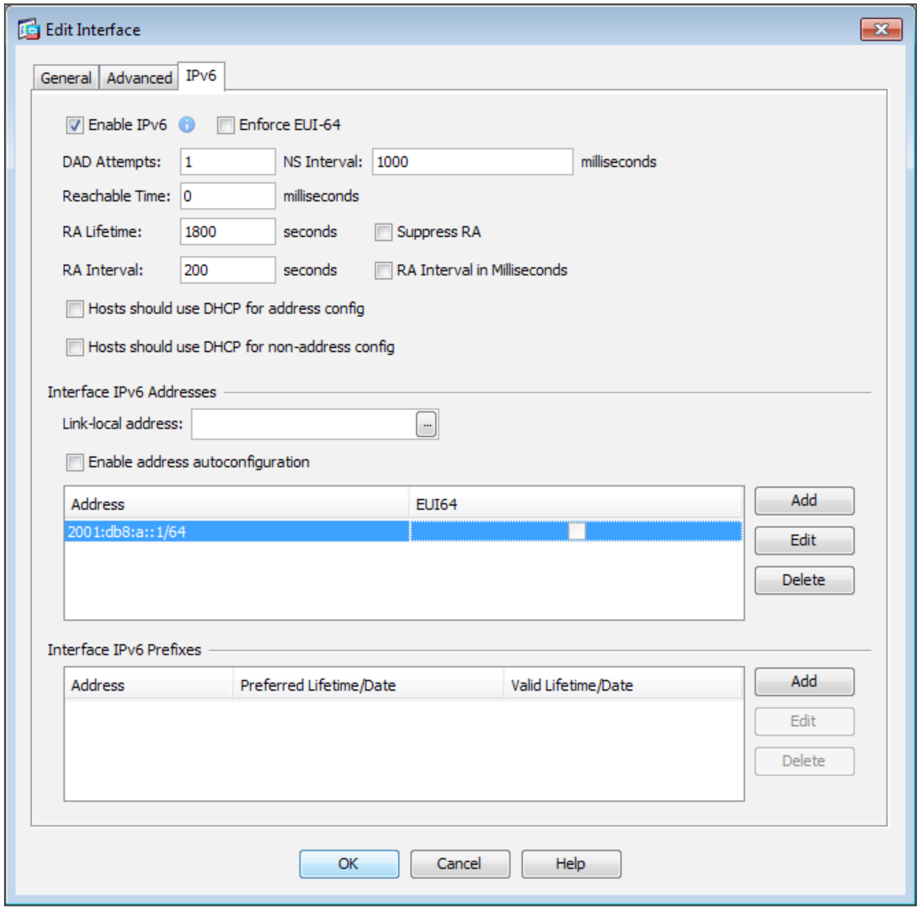
Step 5: Enter the outside IPv6 address, **2001:db8:a::1/64**, and then click **OK**.



Address/Prefix Length:

□ EUI 64

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



☑ Enable IPv6 □ Enforce EUI-64

DAD Attempts: 1 NS Interval: 1000 milliseconds

Reachable Time: 0 milliseconds

RA Lifetime: 1800 seconds □ Suppress RA

RA Interval: 200 seconds □ RA Interval in Milliseconds

□ Hosts should use DHCP for address config

□ Hosts should use DHCP for non-address config

Interface IPv6 Addresses

Link-local address:

□ Enable address autoconfiguration

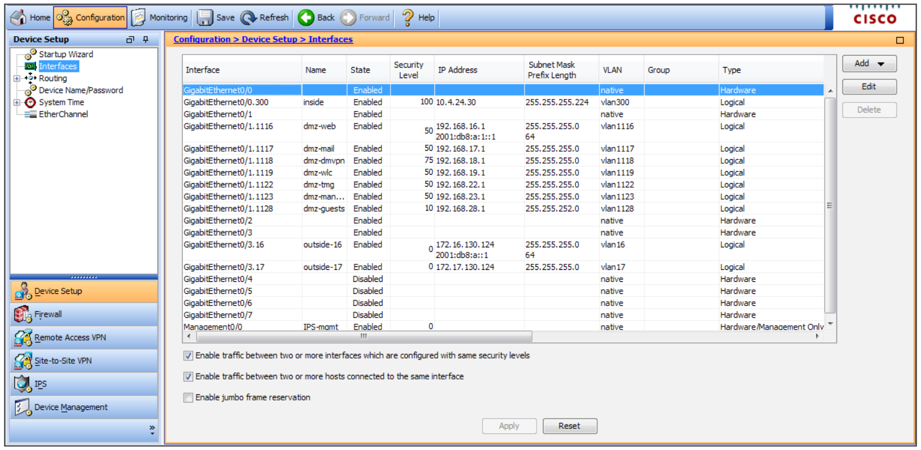
Address	EUI64
2001:db8:a::1/64	□

Interface IPv6 Prefixes

Address	Preferred Lifetime/Date	Valid Lifetime/Date

Step 6: Click **OK** to close the window. 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.



Configuration > Device Setup > Interfaces

Interface	Name	State	Security Level	IP Address	Subnet Mask Prefix Length	VLAN	Group	Type
GigabitEthernet0/0		Enabled				native		Hardware
GigabitEthernet0/0.300	inside	Enabled	100	10.4.24.30	255.255.255.224	vlan300		Logical
GigabitEthernet0/1		Enabled				native		Hardware
GigabitEthernet0/1.1116	dmz-web	Enabled	50	192.168.16.1 2001:db8:a:1::1	255.255.255.0 64	vlan1116		Logical
GigabitEthernet0/1.1117	dmz-mail	Enabled	50	192.168.17.1	255.255.255.0	vlan1117		Logical
GigabitEthernet0/1.1118	dmz-dmvpn	Enabled	75	192.168.18.1	255.255.255.0	vlan1118		Logical
GigabitEthernet0/1.1119	dmz-wlc	Enabled	50	192.168.19.1	255.255.255.0	vlan1119		Logical
GigabitEthernet0/1.1122	dmz-tmg	Enabled	50	192.168.22.1	255.255.255.0	vlan1122		Logical
GigabitEthernet0/1.1123	dmz-man...	Enabled	50	192.168.23.1	255.255.255.0	vlan1123		Logical
GigabitEthernet0/1.1128	dmz-guests	Enabled	10	192.168.28.1	255.255.252.0	vlan1128		Logical
GigabitEthernet0/2		Enabled				native		Hardware
GigabitEthernet0/3		Enabled				native		Hardware
GigabitEthernet0/3.16	outside-16	Enabled	0	172.16.130.124 2001:db8:a::1	255.255.255.0 64	vlan16		Logical
GigabitEthernet0/3.17	outside-17	Enabled	0	172.17.130.124	255.255.255.0	vlan17		Logical
GigabitEthernet0/4		Disabled				native		Hardware
GigabitEthernet0/5		Disabled				native		Hardware
GigabitEthernet0/6		Disabled				native		Hardware
GigabitEthernet0/7		Disabled				native		Hardware
Management0/0	IPS-mgmt	Enabled	0			native		Hardware/Management Only

☑ Enable traffic between two or more interfaces which are configured with same security levels

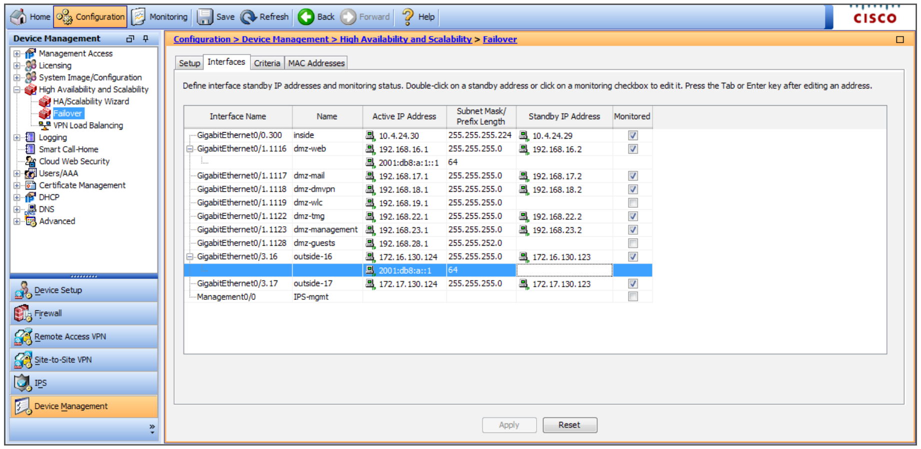
☑ Enable traffic between two or more hosts connected to the same interface

☐ Enable jumbo frame reservation

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 and Scalability > Failover > Interfaces.** On the Interfaces tab, the interfaces configured for IPv4 and IPv6 are displayed.

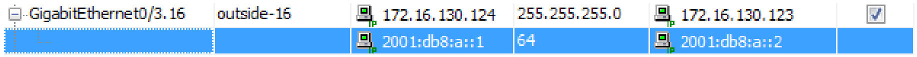


Configuration > Device Management > High Availability and Scalability > Failover

Define interface standby IP addresses and monitoring status. Double-click on a standby address or click on a monitoring checkbox to edit it. Press the Tab or Enter key after editing an address.

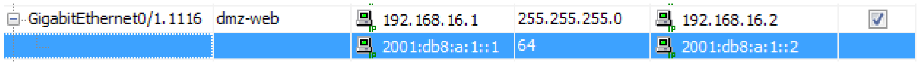
Interface Name	Name	Active IP Address	Subnet Mask/ Prefix Length	Standby IP Address	Monitored
GigabitEthernet0/0.300	inside	10.4.24.30	255.255.255.224	10.4.24.29	☑
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	☑
		2001:db8:a:1::1	64		
GigabitEthernet0/1.1117	dmz-mail	192.168.17.1	255.255.255.0	192.168.17.2	☑
GigabitEthernet0/1.1118	dmz-dmvpn	192.168.18.1	255.255.255.0	192.168.18.2	☑
GigabitEthernet0/1.1119	dmz-wlc	192.168.19.1	255.255.255.0		☐
GigabitEthernet0/1.1122	dmz-tmg	192.168.22.1	255.255.255.0	192.168.22.2	☑
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	☑
GigabitEthernet0/1.1128	dmz-guests	192.168.28.1	255.255.252.0		☐
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	☑
		2001:db8:a::1	64		
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	☑
Management0/0	IPS-mgmt				☐

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	172.16.130.124	255.255.255.0	172.16.130.123	☑
		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**.



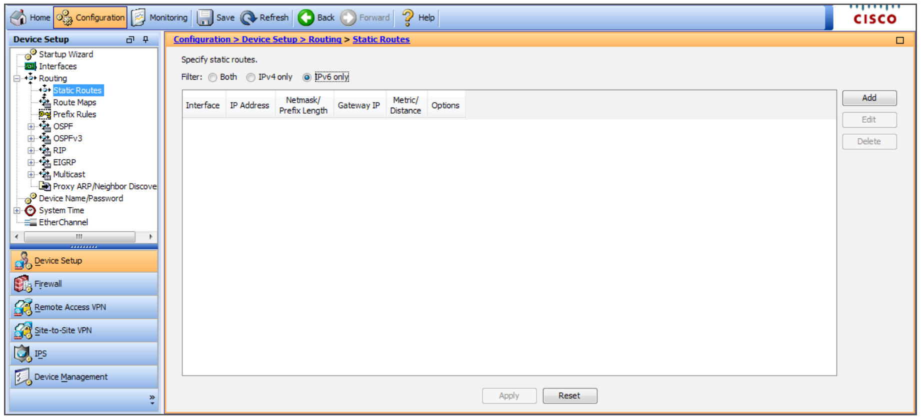
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	☑
		2001:db8:a:1::1	64	2001:db8:a:1::2	

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 towards 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.



Configuration > Device Setup > Routing > Static Routes

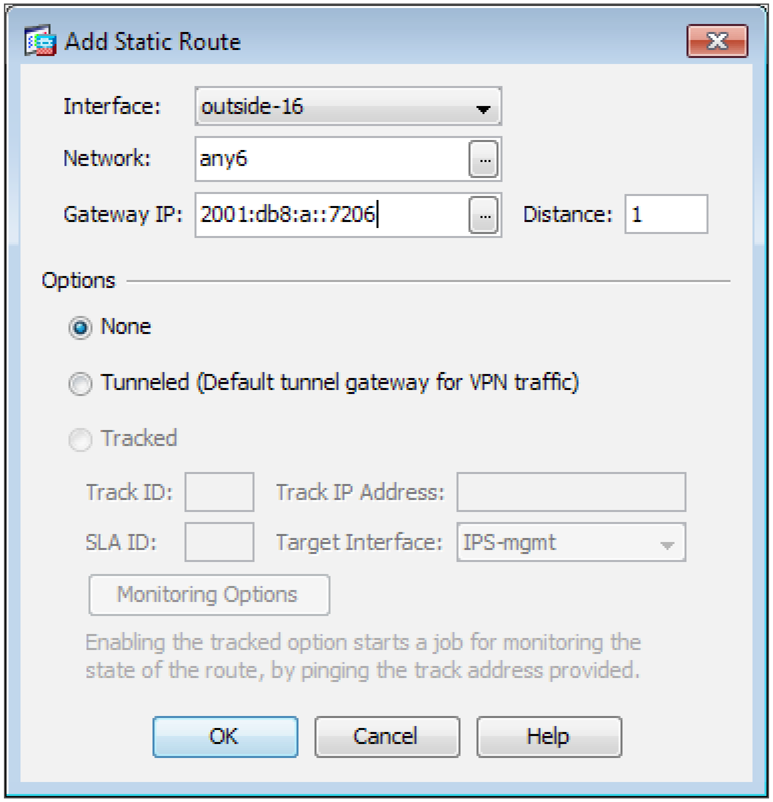
Specify static routes.

Filter: ○ Both ○ IPv4 only ● IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options

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

- Interface—outside-16
- Network—any6
- Gateway IP—2001:db8:a::7206



Add Static Route

Interface: outside-16

Network: any6

Gateway IP: 2001:db8:a::7206

Distance: 1

Options

● None

○ Tunneled (Default tunnel gateway for VPN traffic)

○ Tracked

Track ID:

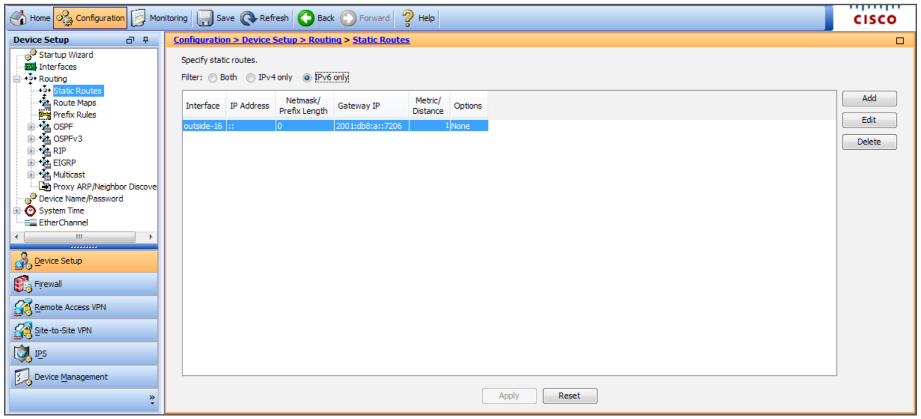
Track IP Address:

SLA ID:

Target Interface: IPS-mgmt

Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.

The static route table reflects the new values.



Configuration > Device Setup > Routing > Static Routes

Specify static routes.

Filter: ○ Both ○ IPv4 only ● IPv6 only

Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options
outside-16	::	0	2001:db8:a::7206	1	None

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

Process

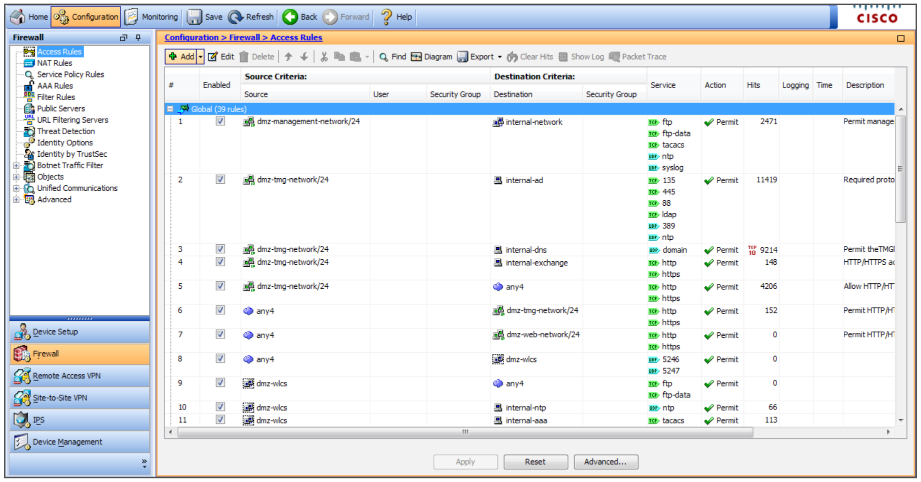
Configuring Cisco ASA Interfaces to Permit Access to IPv6 Web Servers

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**, and then click **Add**.

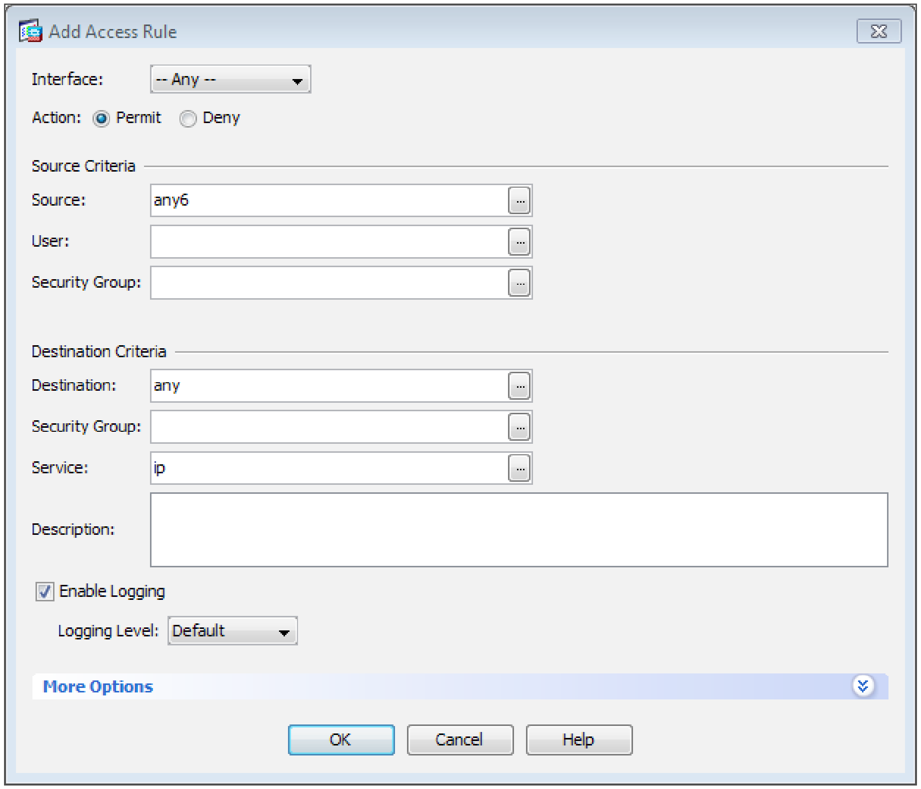


#	Enabled	Source Criteria: Source	Source Criteria: User	Source Criteria: Security Group	Destination Criteria: Destination	Destination Criteria: Security Group	Service	Action	Hits	Logging	Time	Description
Global (39 rules)												
1	☑	dmz-management-network/24			internal-network		ftp ftp-data tacacs ntp syslog	✓ Permit	2471			Permit manage
2	☑	dmz-tmg-network/24			internal-ad		135 445 88 ldap 389 ntp	✓ Permit	11419			Required proto
3	☑	dmz-tmg-network/24			internal-dns		domain	✓ Permit	9214			Permit theTMG
4	☑	dmz-tmg-network/24			internal-exchange		http https	✓ Permit	148			HTTP/HTTPS ac
5	☑	dmz-tmg-network/24			any4		http https	✓ Permit	4206			Allow HTTP/HT
6	☑	any4			dmz-tmg-network/24		http https	✓ Permit	152			Permit HTTP/HT
7	☑	any4			dmz-web-network/24		http https	✓ Permit	0			Permit HTTP/HT
8	☑	any4			dmz-wlcs		5246 5247	✓ Permit	0			
9	☑	dmz-wlcs			any4		ftp ftp-data	✓ Permit	0			
10	☑	dmz-wlcs			internal-ntp		ntp	✓ Permit	66			
11	☑	dmz-wlcs			internal-aaa		tacacs	✓ Permit	113			

Step 2: On the Add Access Rule dialog box, ensure that **Interface** is set to **Any**.

Step 3: In the **Source** text box, click the ellipsis button (**...**), and then select **any6**.

Step 4: On the Add Access Rule dialog box, in the **Destination** text box, click the ellipsis button (**...**).



Interface: -- Any --

Action: ● Permit ○ Deny

Source: any6

User:

Security Group:

Destination: any

Security Group:

Service: ip

Description:

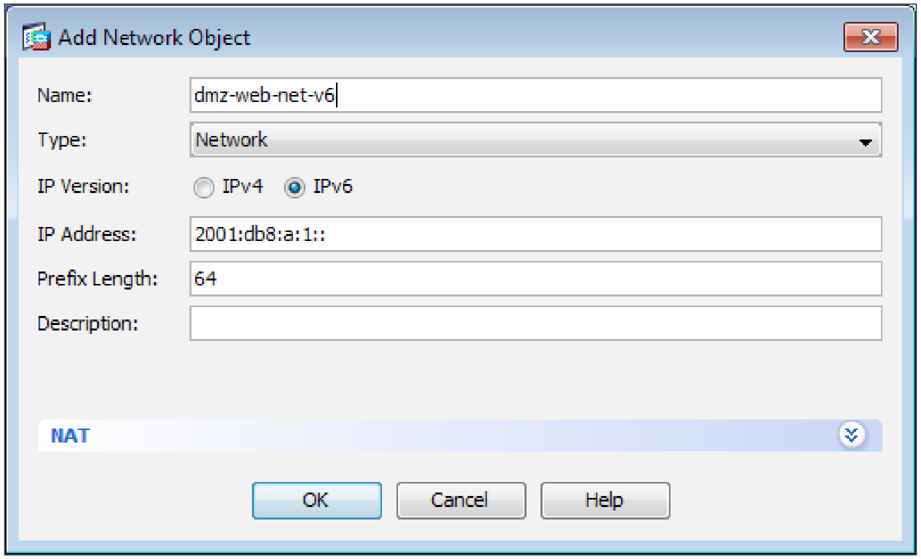
☑ Enable Logging

Logging Level: Default

Step 5: On the Browse Destination dialog box, click **Add**, and then select **Network Object**.

Step 6: On the Add Network Object dialog box, enter the values listed below, and then click **OK.**

- Name—dmz-web-net-v6
- Type—Network
- IP Version—IPv6
- IP Address—2001:db8:a:1::
- Prefix Length—64



Name: dmz-web-net-v6

Type: Network

IP Version: ○ IPv4 ● IPv6

IP Address: 2001:db8:a:1::

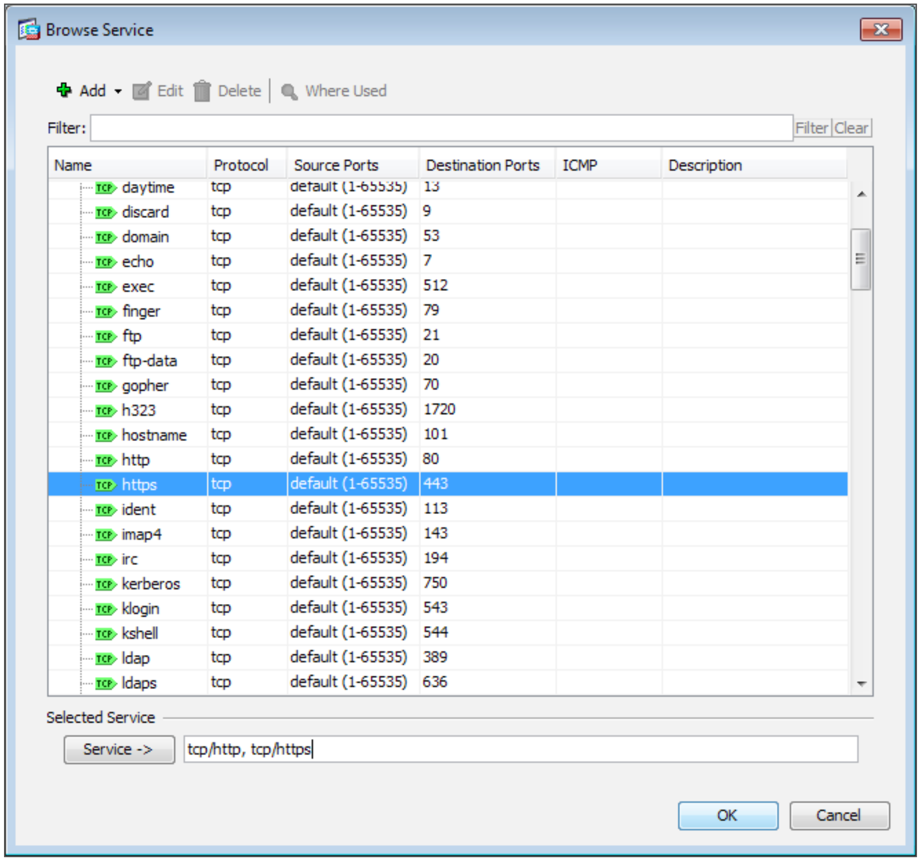
Prefix Length: 64

Description:

Step 7: Double-click the network object that was just created, and then click OK.

Step 8: On the Add Access Rule dialog box, in the **Service** text box, click the ellipsis button (**…**).

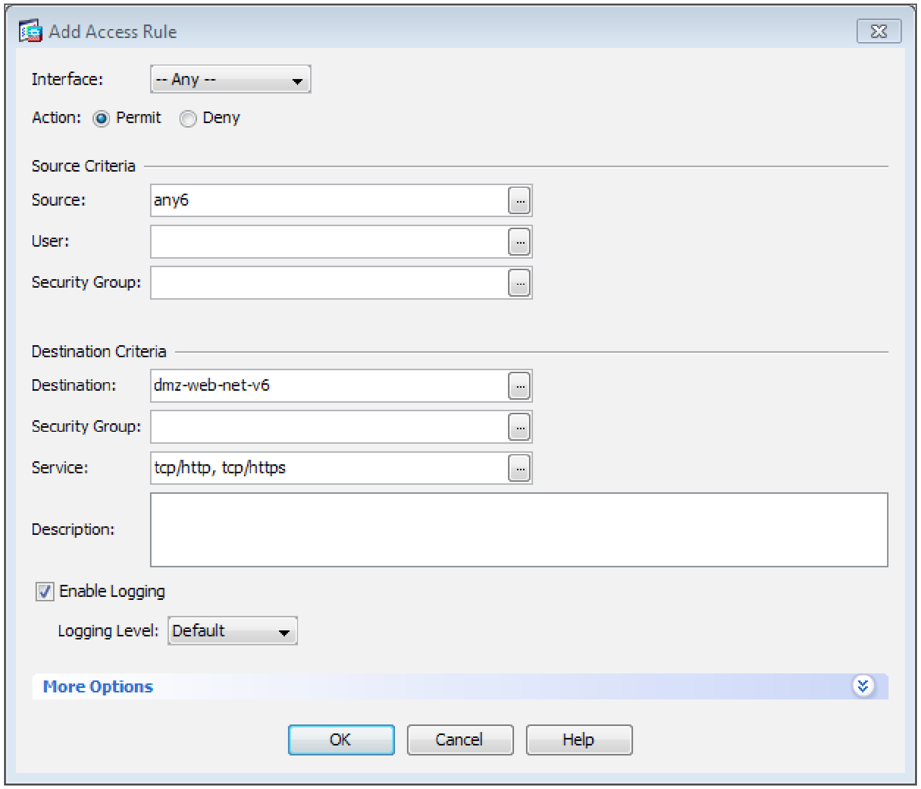
Step 9: On the Browse Service dialog box, scroll down and double-click **http** and **https**, and then click **OK.**



Name	Protocol	Source Ports	Destination Ports	ICMP	Description
daytime	tcp	default (1-65535)	13		
discard	tcp	default (1-65535)	9		
domain	tcp	default (1-65535)	53		
echo	tcp	default (1-65535)	7		
exec	tcp	default (1-65535)	512		
finger	tcp	default (1-65535)	79		
ftp	tcp	default (1-65535)	21		
ftp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
h323	tcp	default (1-65535)	1720		
hostname	tcp	default (1-65535)	101		
http	tcp	default (1-65535)	80		
https	tcp	default (1-65535)	443		
ident	tcp	default (1-65535)	113		
imap4	tcp	default (1-65535)	143		
irc	tcp	default (1-65535)	194		
kerberos	tcp	default (1-65535)	750		
klogin	tcp	default (1-65535)	543		
kshell	tcp	default (1-65535)	544		
ldap	tcp	default (1-65535)	389		
ldaps	tcp	default (1-65535)	636		

Service -> tcp/http, tcp/https

Step 10: Verify that the Add Access Rule dialog box resembles the following illustration, and then click **OK**.



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: any6

User:

Security Group:

Destination Criteria

Destination: dmz-web-net-v6

Security Group:

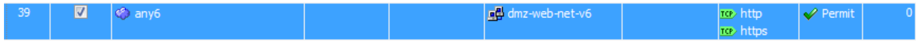
Service: tcp/http, tcp/https

Description:

☑ Enable Logging

Logging Level: Default

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



39	☑	any6			dmz-web-net-v6		http https	✓ Permit	0

Step 11: At the bottom of the window, click **Apply**. This saves the configuration.

Process

Configuring NAT64 on the ASA Firewall

1. Configure IPv6 to IPv4 Static Translation
2. Configure IPv6 Source Address Translation
3. Permit HTTP/HTTPS to the NATed Server

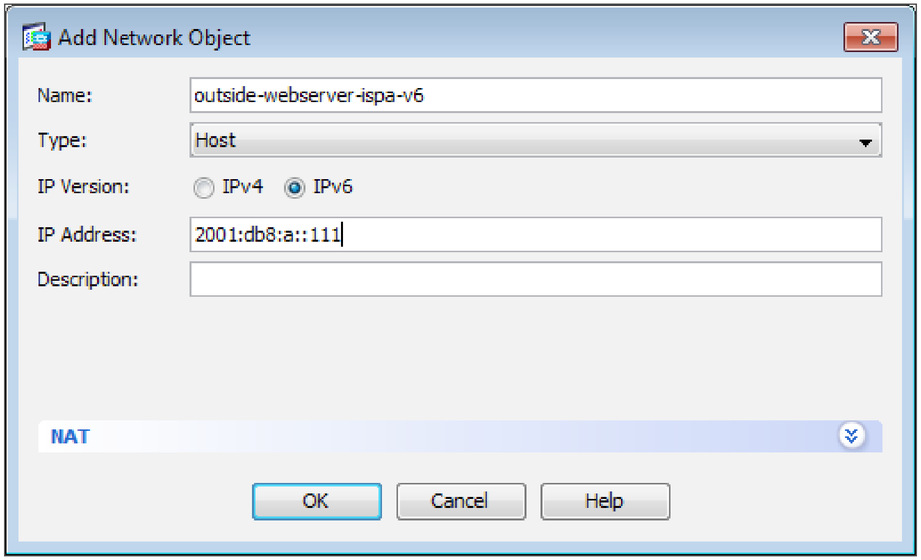
Procedure 1 Configure IPv6 to IPv4 Static Translation

In this procedure, you map an outside IPv6 static address to the IPv4 address of the server in the DMZ. This will translate the destination address of the client connection from the Internet to the real IPv4 address on the server.

Step 1: Navigate to **Configuration** > **Firewall** > **Objects** > **Network Objects/Groups**, click **Add**, and then select **Network Object.** The Add Network Object dialog box appears**.**

Step 2: On the Add Network Object dialog box, enter the values listed below, and then click **OK.**

- Name—oustide-webserver-ispa-v6
- Type—Host
- IP Version—IPv6
- IP Address—2001:db8:a::111



Name: outside-webserver-ispa-v6

Type: Host

IP Version: ○ IPv4 ● IPv6

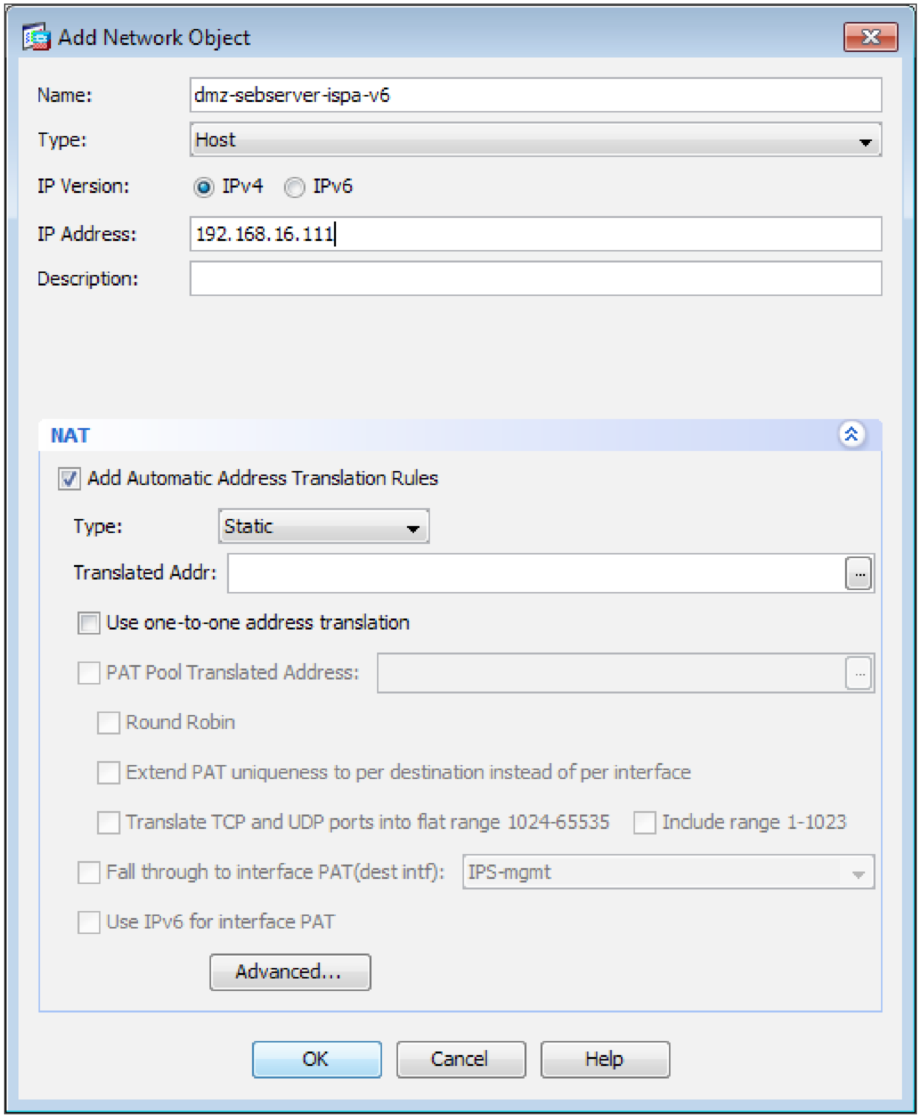
IP Address: 2001:db8:a::111

Description:

Step 3: Navigate to **Configuration > Firewall > NAT Rules**, in **the Add** list, choose **Add "Network Object" Nat Rule.** The Add Network Object dialog box appears**.**

Step 4: On the Add Network Object dialog box, enter the values listed below.

- Name—**dmz-webserver-ispa-v6**
- Type—**Host**
- IP Version—**IPv4**
- IP Address—**192.168.16.111**



Name: dmz-sebserver-ispa-v6

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address: 192.168.16.111

Description:

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr:

□ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT(dest intf): IPS-mgmt

□ Use IPv6 for interface PAT

Step 5: On the Add Network Object dialog box, in the NAT section, next to Translated Addr, click the ellipsis (**...**). The Browse Translated Addr dialog box appears.

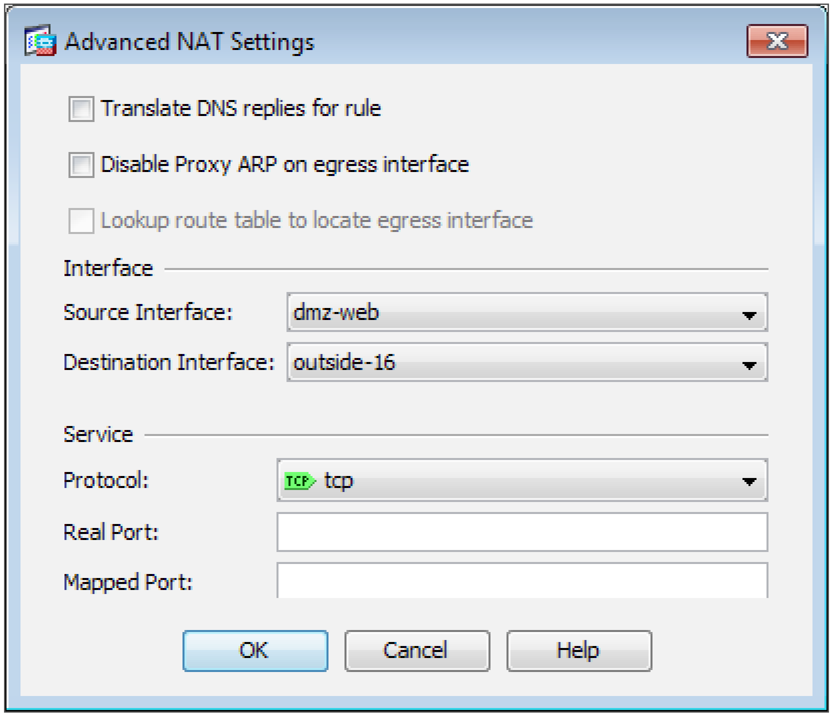
Step 6: On the Browse Translated Addr dialog box, locate the object (example: outside-webserver-ispa-v6) created in Step 2, double-click the object, and then click **OK**.

Step 7: Select **Use one-to-one address translation**.

Step 8: On the Add Network Object dialog box, click **Advanced**. The Advanced NAT Settings dialog box appears.

Step 9: On the Advanced NAT Settings dialog box, in the **Source Interface** list, choose **dmz-web.**

Step 10: On the Advanced NAT Settings dialog box, in the Destination Interface list, choose **oustide-16**, and then click **OK.**



Advanced NAT Settings

□ Translate DNS replies for rule

□ Disable Proxy ARP on egress interface

□ Lookup route table to locate egress interface

Interface

Source Interface: dmz-web

Destination Interface: outside-16

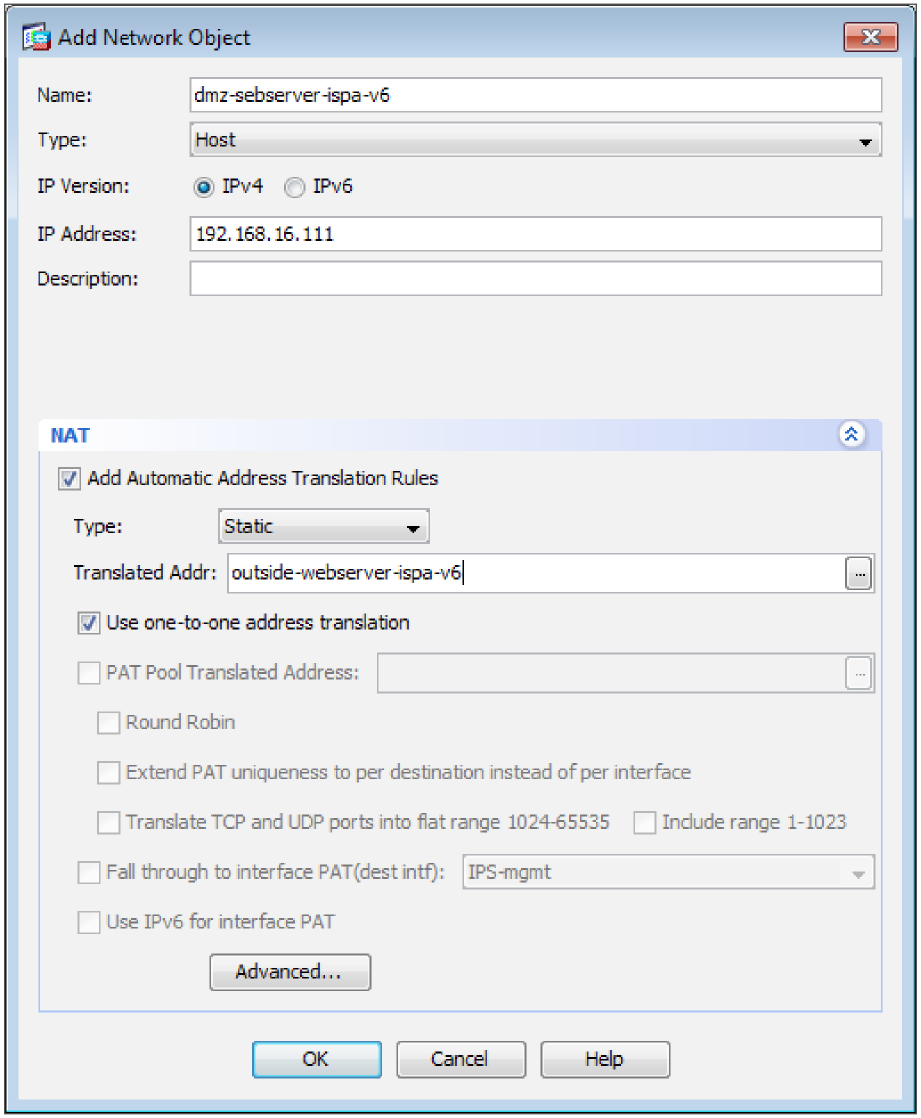
Service

Protocol: tcp

Real Port:

Mapped Port:

Step 11: On the Add Network Object dialog box, click **OK**.



Add Network Object

Name: dmz-sebserver-ispa-v6

Type: Host

IP Version: ● IPv4 ○ IPv6

IP Address: 192.168.16.111

Description:

NAT

☑ Add Automatic Address Translation Rules

Type: Static

Translated Addr: outside-webserver-ispa-v6

☑ Use one-to-one address translation

□ PAT Pool Translated Address:

□ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

□ Fall through to interface PAT(dest intf): IPS-mgmt

□ Use IPv6 for interface PAT

Step 12: At the bottom of the NAT Rules window, click **Apply**.

Now all traffic destined for 2001:db8:a::111 will be translated to 192.168.16.111.

Tech Tip

When configuring NAT64 or NAT46 a network object for the translated address must be added before the NAT rule is created, attempting to add it during NAT rule creation will result in an invalid IP version error and you will not be able to continue.

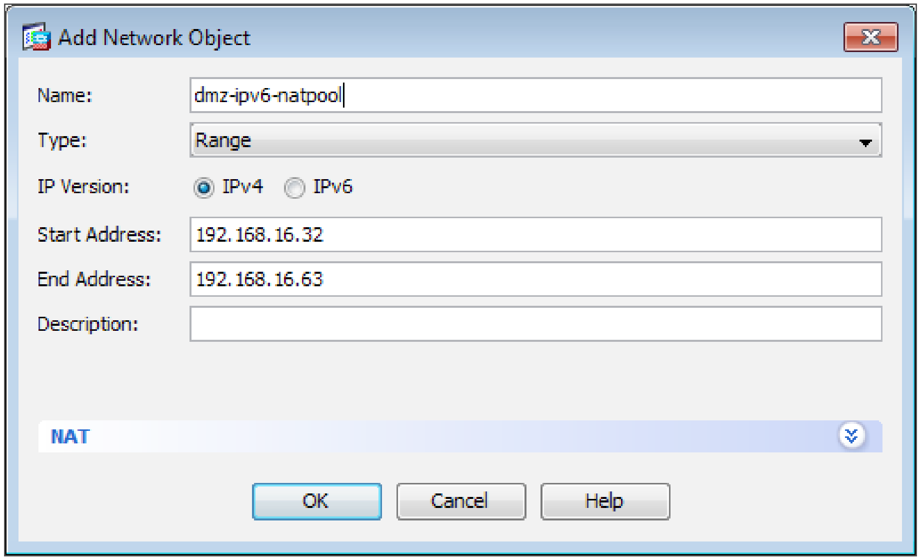
Procedure 2 Configure IPv6 Source Address Translation

Configuring NAT64 is a two-part process. You have already translated the IPv6 destination address to the real IPv4 server address, now you need to translate the clients IPv6 source address to an IPv4 address. In order to accomplish the source address translation, you will configure a NAT pool of addresses out of the free address space on the webserver DMZ. It is important to note that you can at most translate 65,535 IPv6 addresses for each IPv4 address you have in the NAT pool, so you must provision enough addresses for the NAT pool to handle the expected amount of IPv6 clients.

Step 1: Navigate to **Configuration > Firewall > Objects > Network Objects/Groups**, click **Add**, and then select **Network Object**. The Add Network Object dialog box appears.

Step 2: On the Add Network Object dialog box, enter the values listed below, and then click **OK.**

- Name—**dmz-ipv6-natpool**
- Type—**Range**
- IP Version—**IPv4**
- Start Address—**192.168.16.32**
- End Address—**192.168.16.63**


Add Network Object

Name: dmz-ipv6-natpool

Type: Range

IP Version: ● IPv4 ○ IPv6

Start Address: 192.168.16.32

End Address: 192.168.16.63

Description:

Step 3: Navigate to **Configuration > Firewall > NAT Rules,** in the Add list, choose **Add "Network Object" Nat Rule**. The Add Network Object dialog box appears.

Step 4: On the Add Network Object dialog box, enter the values listed below.

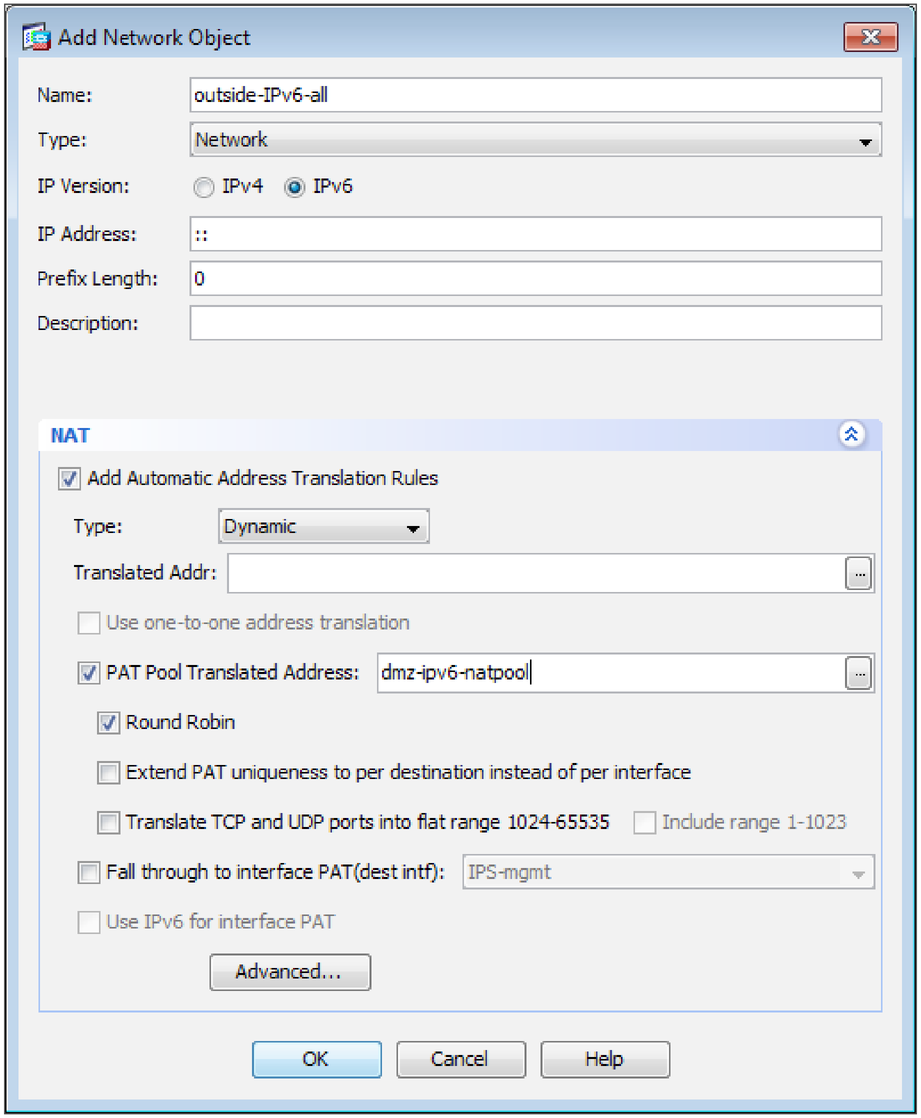
- Name—**outside-IPv6-all**
- Type—**Network**
- IP Version—**IPv6**
- IP Address—**::**
- Prefix Length—**0**

Step 5: On the Add Network Object dialog box, in the NAT section, in **Type** list, choose **Dynamic**.

Step 6: On the Add Network Object dialog box, in the NAT section, select **PAT Pool Translated Address**, and then click the ellipsis button (**...**). The Browse PAT Pool Translated Address dialog box appears.

Step 7: On the Browse PAT Pool Translated Address dialog box, locate the object (example: dmz-ipv6-natpool) created in Step 2, Procedure 1 "Configure IPv6 to IPv4 Static Translation," double-click the object, and then click **OK**.

Step 8: In the **PAT Pool Translated Address** list, choose **Round Robin**.



Add Network Object

Name: outside-IPv6-all

Type: Network

IP Version: ○ IPv4 ● IPv6

IP Address: ::

Prefix Length: 0

Description:

NAT

☑ Add Automatic Address Translation Rules

Type: Dynamic

Translated Addr:

□ Use one-to-one address translation

☑ PAT Pool Translated Address: dmz-ipv6-natpool

☑ Round Robin

□ Extend PAT uniqueness to per destination instead of per interface

□ Translate TCP and UDP ports into flat range 1024-65535 □ Include range 1-1023

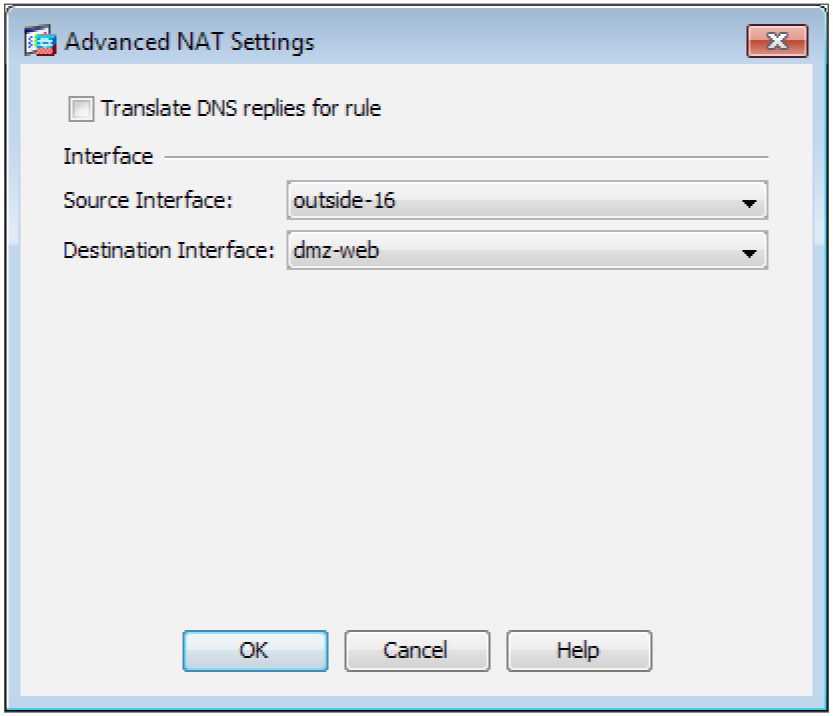
□ Fall through to interface PAT(dest intf): IPS-mgmt

□ Use IPv6 for interface PAT

Step 9: On the Add Network Object dialog box, click **Advanced**. The Advanced NAT Settings dialog box appears.

Step 10: On the Advanced NAT Settings dialog box, in the **Source Interface** list, choose **oustide-16.**

Step 11: On the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose **dmz-web**, and then click **OK.**



Advanced NAT Settings

□ Translate DNS replies for rule

Interface

Source Interface: outside-16

Destination Interface: dmz-web

Step 12: On the Add Network Object dialog box, click **OK**.

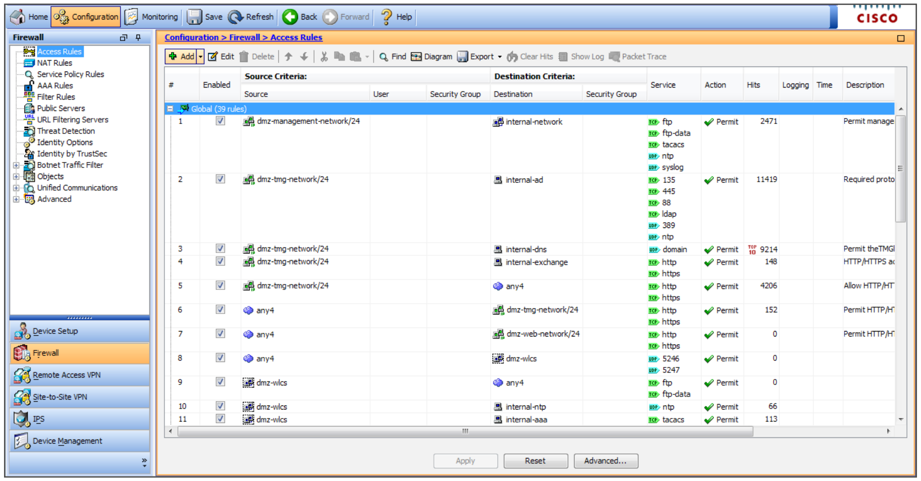
Step 13: At the bottom of the NAT Rules window, click **Apply**.

All client IPv6 source addresses will be translated to an address out of the pool you created. Using the Round Robin option uses a new pool address for each IPv6 client until all addresses are used, then additional clients are Port Address Translated (PATed) to the pool addresses in a round robin fashion. This has two benefits: it gives more detail about how many hosts are accessing the web server, which is helpful because all hosts will get unique addresses until the pool is exhausted; and, if you are pointing the clients at a load balancer that utilizes source address in its balancing algorithm rather than a server directly, you have more source addresses to balance from, making the load sharing more equal.

Procedure 3 Permit HTTP/HTTPS to the NATed Server

The last thing left to do is to create an access list to permit traffic to the server.

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

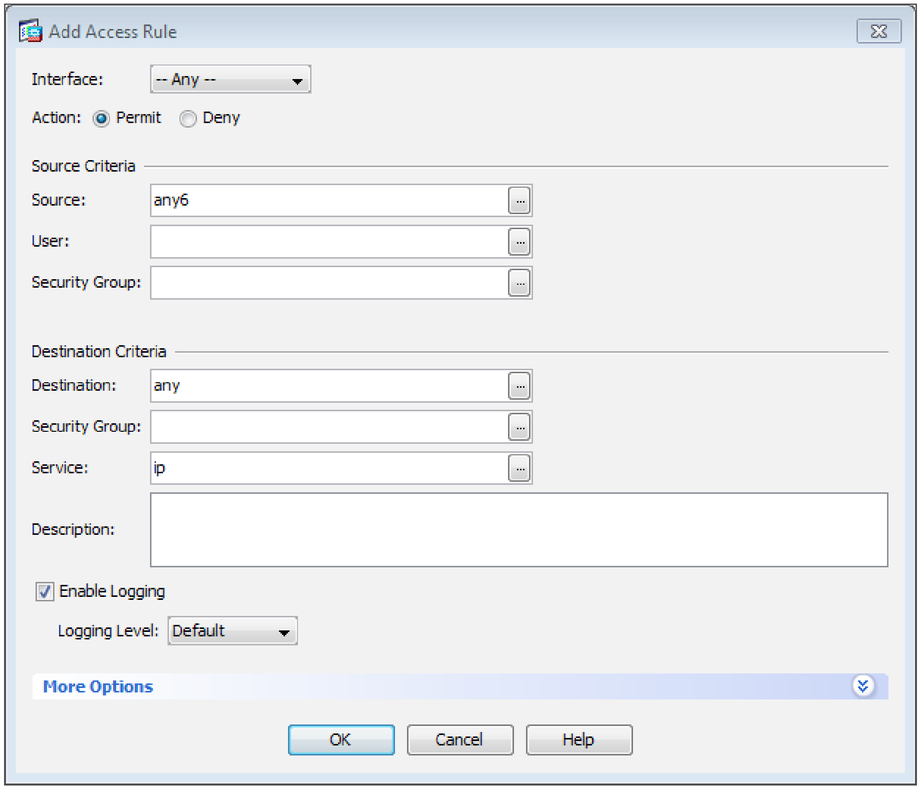


#	Enabled	Source Criteria:			Destination Criteria:		Service	Action	Hits	Logging	Time	Description
		Source	User	Security Group	Destination	Security Group						
Global (39 rules)												
1	☑	dmz-management-network/24			internal-network		ftp ftp-data tacacs ntp syslog	✓ Permit	2471			Permit manage
2	☑	dmz-tmg-network/24			internal-ad		135 445 88 ldap 389 ntp	✓ Permit	11419			Required proto
3	☑	dmz-tmg-network/24			internal-dns		domain	✓ Permit	TOP 10 9214			Permit theTMG
4	☑	dmz-tmg-network/24			internal-exchange		http https	✓ Permit	148			HTTP/HTTPS ac
5	☑	dmz-tmg-network/24			any4		http https	✓ Permit	4206			Allow HTTP/HT
6	☑	any4			dmz-tmg-network/24		http https	✓ Permit	152			Permit HTTP/HT
7	☑	any4			dmz-web-network/24		http https	✓ Permit	0			Permit HTTP/HT
8	☑	any4			dmz-wlcs		5246 5247	✓ Permit	0			
9	☑	dmz-wlcs			any4		ftp ftp-data	✓ Permit	0			
10	☑	dmz-wlcs			internal-ntp		ntp	✓ Permit	66			
11	☑	dmz-wlcs			internal-aaa		tacacs	✓ Permit	113			

Step 2: On the Add Access Rule dialog box, ensure that **Interface** is set to **Any**.

Step 3: In the **Source** text box, click the ellipsis button (**…**), and then select **any6**.

Step 4: On the Add Access Rule dialog box, in the **Destination** text box, click the ellipsis button (**…**).


Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: any6

User:

Security Group:

Destination Criteria

Destination: any

Security Group:

Service: ip

Description:

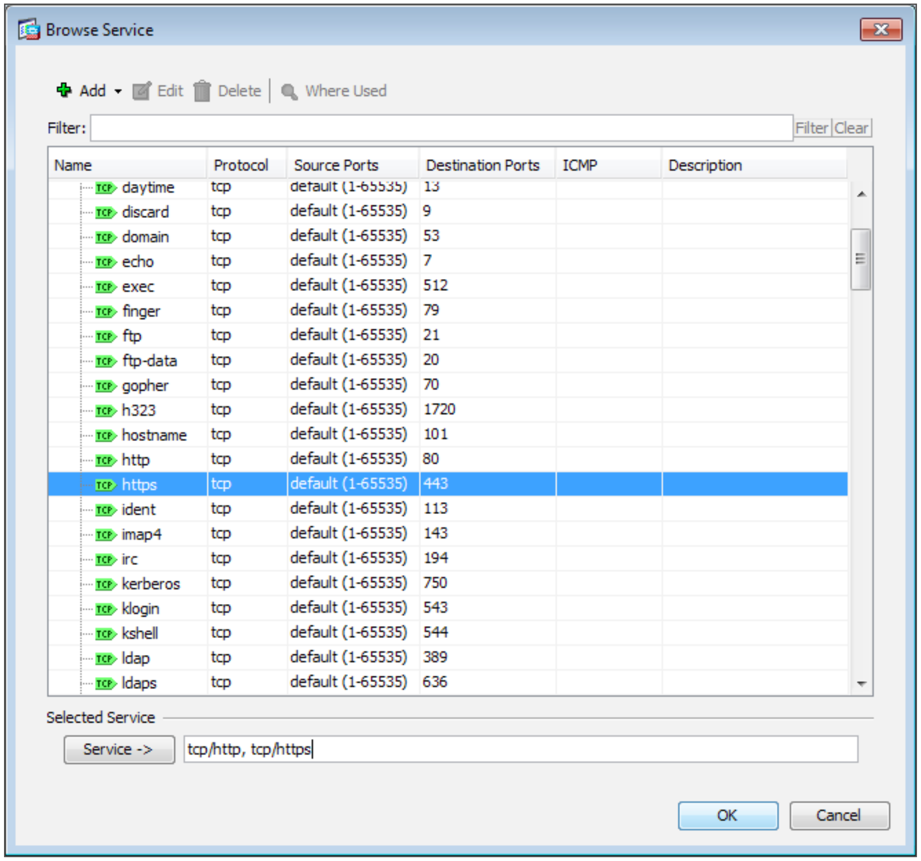
☑ Enable Logging

Logging Level: Default

Step 5: On the Browse Destination dialog box, double-click the object (example: dmz-webserver-ispa-v6) created earlier, and then click **OK**.

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

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



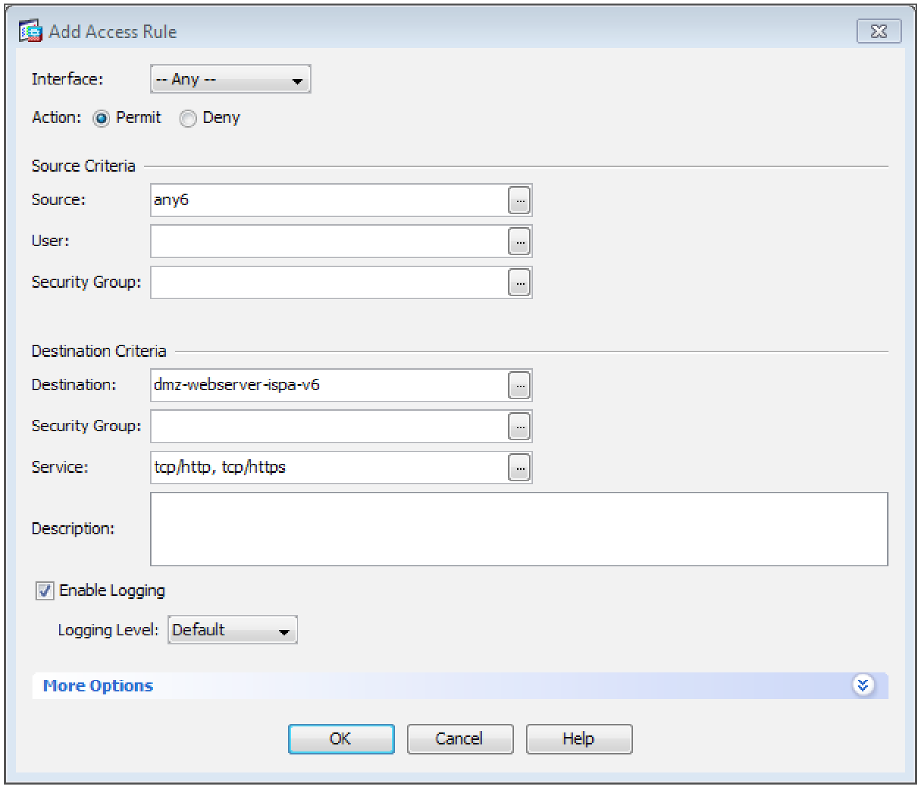
Browse Service

Name	Protocol	Source Ports	Destination Ports	ICMP	Description
daytime	tcp	default (1-65535)	13		
discard	tcp	default (1-65535)	9		
domain	tcp	default (1-65535)	53		
echo	tcp	default (1-65535)	7		
exec	tcp	default (1-65535)	512		
finger	tcp	default (1-65535)	79		
ftp	tcp	default (1-65535)	21		
ftp-data	tcp	default (1-65535)	20		
gopher	tcp	default (1-65535)	70		
h323	tcp	default (1-65535)	1720		
hostname	tcp	default (1-65535)	101		
http	tcp	default (1-65535)	80		
https	tcp	default (1-65535)	443		
ident	tcp	default (1-65535)	113		
imap4	tcp	default (1-65535)	143		
irc	tcp	default (1-65535)	194		
kerberos	tcp	default (1-65535)	750		
klogin	tcp	default (1-65535)	543		
kshell	tcp	default (1-65535)	544		
ldap	tcp	default (1-65535)	389		
ldaps	tcp	default (1-65535)	636		

Selected Service

Service -> tcp/http, tcp/https

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



Add Access Rule

Interface: -- Any --

Action: ● Permit ○ Deny

Source Criteria

Source: any6

User:

Security Group:

Destination Criteria

Destination: dmz-webserver-ispa-v6

Security Group:

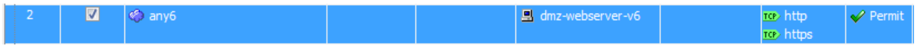
Service: tcp/http, tcp/https

Description:

☑ Enable Logging

Logging Level: Default

The rule that was just created appears in the Global rule table.



2	☑	any6			dmz-webserver-v6		http https	✓ Permit

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

Clients from the Internet can now access the IPv4-only server from IPv6-only clients for HTTP and HTTPS traffic.

Tech Tip

Cisco ASA software 8.3(1) and later have the concept of Real IP. When using NAT or PAT, mapped addresses and ports are no longer required in an ACL. You should now always use the real, untranslated addresses and ports.

Process

Configuring IPv6 on the DMZ Web Server

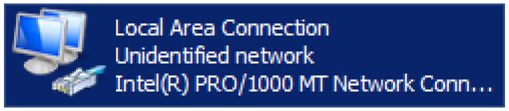
1. Configure IPv6 on a Windows 2008 server

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. This is used for direct untranslated access to the server from IPv6 clients.

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**.



Local Area Connection
Unidentified network
Intel(R) PRO/1000 MT Network Conn...

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

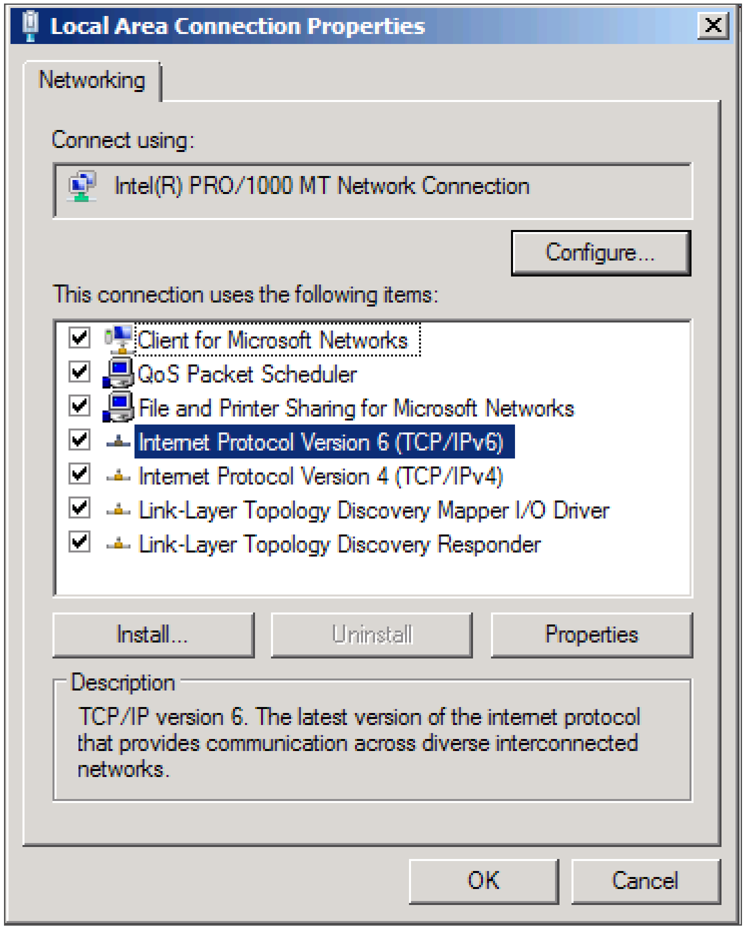
Step 4: If the **Internet Protocol Version 6 (TCP/IPv6)** check box is not selected, select it, click **OK**, and then repeat Step 3.

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**.



Connect using:

Intel(R) PRO/1000 MT Network Connection

This connection uses the following items:

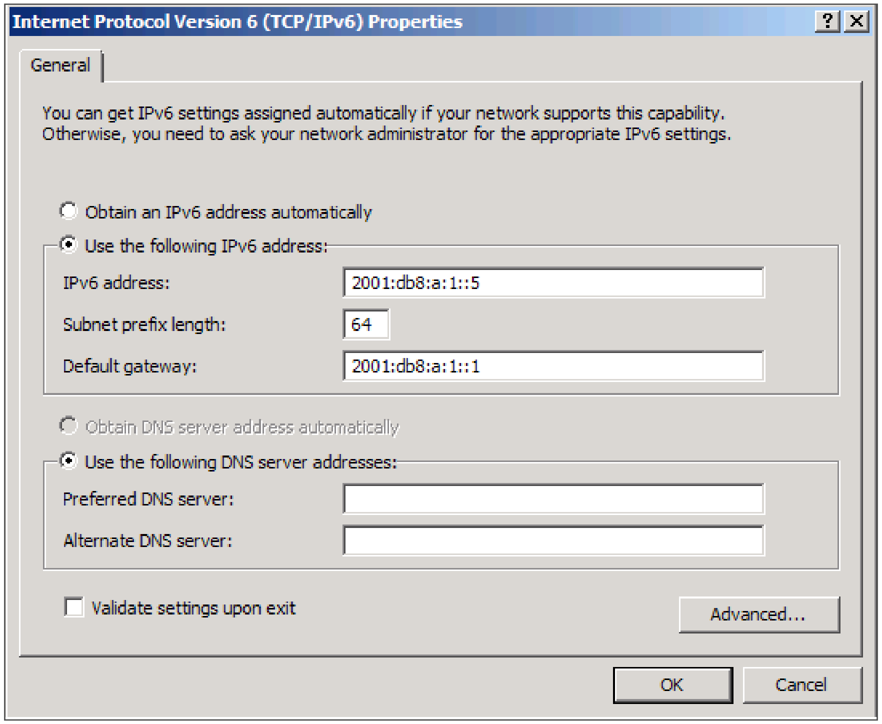
☑ Client for Microsoft Networks
☑ QoS Packet Scheduler
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol Version 6 (TCP/IPv6)
☑ Internet Protocol Version 4 (TCP/IPv4)
☑ Link-Layer Topology Discovery Mapper I/O Driver
☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

Step 6: On 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



Internet Protocol Version 6 (TCP/IPv6) Properties

General

You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

○ Obtain an IPv6 address automatically

● Use the following IPv6 address:

IPv6 address: 2001:db8:a:1::5

Subnet prefix length: 64

Default gateway: 2001:db8:a:1::1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

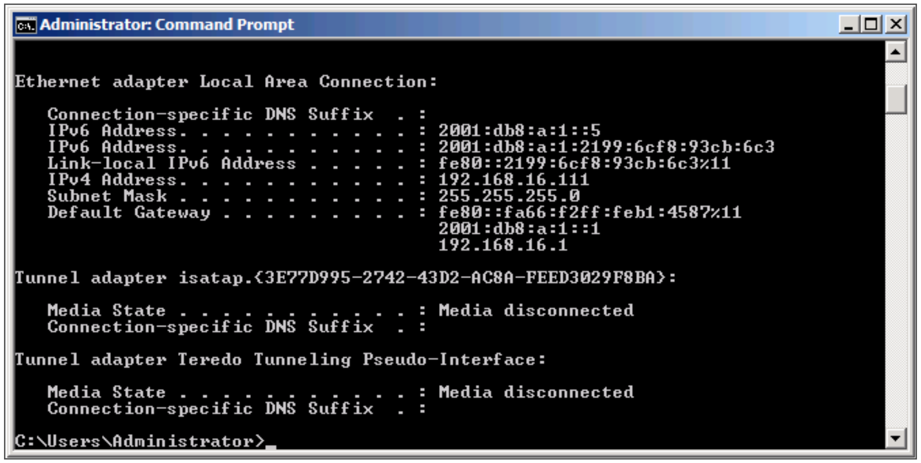
Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

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.



Administrator: Command Prompt

```
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : 2001:db8:a:1::5
   IPv6 Address. . . . . . . . . . . : 2001:db8:a:1:2199:6cf8:93cb:6c3
   Link-local IPv6 Address . . . . . : fe80::2199:6cf8:93cb:6c3%11
   IPv4 Address. . . . . . . . . . . : 192.168.16.111
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::fa66:f2ff:feb1:4587%11
                                       2001:db8:a:1::1
                                       192.168.16.1

Tunnel adapter isatap.{3E77D995-2742-43D2-AC8A-FEED3029F8BA}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

C:\Users\Administrator>_
```

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 9.0(1)1 IPS 7.1(6) 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	7.0(2)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 3750-X Series Stackable 24 Ethernet 10/100/1000 ports	WS-C3750X-24T-S	15.0(1)SE IP Base License
Outside Switch	Cisco Catalyst 2960-S Series 24 Ethernet 10/100/1000 ports and four GbE SFP Uplink ports	WS-C2960S-24TS-L	15.0(1)SE2 LAN Base License

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
!
object network dmz-web-net-v6
 subnet 2001:db8:a:1::/64
object network dmz-webserver-ispa-v6
 host 192.168.16.111
object network oustide-webserver-ispa-v6
 host 2001:db8:a::111
object network dmz-ipv6-natpool
 range 192.168.16.32 192.168.16.63
object network outside-IPv6-all
 subnet ::/0
!
access-list global_access extended permit tcp any6 object dmz-web-net-v6 object-group
access-list global_access extended permit tcp any6 object dmz-webserver-ispa-v6 object-group
object network dmz-webserver-ispa-v6
 nat (dmz-web,outside-16) static oustide-webserver-ispa-v6 net-to-net
object network outside-IPv6-all
 nat (outside-16,dmz-web) dynamic pat-pool dmz-ipv6-natpool round-robin
access-group global_access global
ipv6 route outside-16 ::/0 2001:db8:a::7206
```

Appendix C: Changes

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

- We updated Cisco ASA software to align with current Cisco SBA release.
- We updated screen shots to show current Cisco ASA GUI.
- We added NAT64 option for IPv4-only servers.

Notes

Feedback

Please use the feedback form to send comments and suggestions about this guide.

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.

ALL DESIGNS, SPECIFICATIONS, STATEMENTS, INFORMATION, AND RECOMMENDATIONS (COLLECTIVELY, "DESIGNS") IN THIS MANUAL ARE PRESENTED "AS IS," WITH ALL FAULTS. CISCO AND ITS SUPPLiERS DISCLAIM ALL WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE. IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THE DESIGNS, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THE DESIGNS ARE SUBJECT TO CHANGE WITHOUT NOTICE. USERS ARE SOLELY RESPONSIBLE FOR THEIR APPLICATION OF THE DESIGNS. THE DESIGNS DO NOT CONSTITUTE THE TECHNICAL OR OTHER PROFESSIONAL ADVICE OF CISCO, ITS SUPPLIERS OR PARTNERS. USERS SHOULD CONSULT THEIR OWN TECHNICAL ADVISORS BEFORE IMPLEMENTING THE DESIGNS. RESULTS MAY VARY DEPENDING ON FACTORS NOT TESTED BY CISCO.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.