



IPv6 DMZ Web Service

Technology Design Guide

August 2014 Series



Table of Contents

Preface	1
CVD Navigator	2
Use Cases	2
Scope	2
Proficiency	2
Introduction	3
Technology Use Cases	3
Use Case: Enable Native IPv6 Access for Network Traffic Between the Internet and a Web Server DMZ Network	3
Use Case: Enable IPv6 Access for Network Traffic Between the Internet and an IPv4-only Web Server DMZ Network	3
Design Overview	4
Domain Name System for IPv6	5
Deployment Details	6
Configuring IPv6 on the Cisco ASA Firewall	8
Configuring Cisco ASA to permit IPv6 web access	13
Configuring IPv6 on the DMZ Web Server	23
Appendix A: Product List	26
Appendix B: CLI Configuration	27
ASA Firewall IE-ASA5545X	27

Preface

Cisco Validated Designs (CVDs) present systems that are based on common use cases or engineering priorities. CVDs incorporate a broad set of technologies, features, and applications that address customer needs. Cisco engineers have comprehensively tested and documented each design in order to ensure faster, more reliable, and fully predictable deployment.

CVDs include two guide types that provide tested design details:

- **Technology design guides** provide deployment details, information about validated products and software, and best practices for specific types of technology.
- **Solution design guides** integrate existing CVDs but also include product features and functionality across Cisco products and sometimes include information about third-party integration.

Both CVD types provide a tested starting point for Cisco partners or customers to begin designing and deploying systems.

CVD Foundation Series

This CVD Foundation guide is a part of the *August 2014 Series*. As Cisco develops a CVD Foundation series, the guides themselves are tested together, in the same network lab. This approach assures that the guides in a series are fully compatible with one another. Each series describes a lab-validated, complete system.

The CVD Foundation series incorporates wired and wireless LAN, WAN, data center, security, and network management technologies. Using the CVD Foundation simplifies system integration, allowing you to select solutions that solve an organization's problems—without worrying about the technical complexity.

To ensure the compatibility of designs in the CVD Foundation, you should use guides that belong to the same release. For the most recent CVD Foundation guides, please visit [the CVD Foundation web site](#).

Comments and Questions

If you would like to comment on a guide or ask questions, please use the [feedback form](#).

CVD Navigator

The CVD Navigator helps you determine the applicability of this guide by summarizing its key elements: the use cases, the scope or breadth of the technology covered, the proficiency or experience recommended, and CVDs related to this guide. This section is a quick reference only. For more details, see the Introduction.

Use Cases

This guide addresses the following technology use cases:

- **Enable Native IPv6 Access for Network Traffic Between the Internet and a Web Server DMZ Network**—Native IPv6 access to web servers in a DMZ requires the full enablement of IPv6 at the Internet edge. The firewall and web servers are configured for IPv6 without the need for any network address translation (NAT).
- **Enable IPv6 Access for Network Traffic Between the Internet and an IPv4-only Web Server DMZ Network**—IPv6 access to IPv4 web servers in a DMZ requires the partial enablement of IPv6 at the Internet edge. Only the outside of the firewall is configured for IPv6 and the web servers run IPv4. Network address translation for IPv6 to IPv4 (NAT64) is configured on the firewall.

For more information, see the “Use Cases” section in this guide.

Scope

This guide covers the following areas of technology and products:

- Cisco ASA 5500-X Series Adaptive Security Appliances for Internet edge firewall security and intrusion prevention

For more information, see the “Design Overview” section in this guide.

Proficiency

This guide is for people with the following technical proficiencies—or equivalent experience:

- **CCNA Routing and Switching**—1 to 3 years installing, configuring, and maintaining routed and switched networks
- **CCNA Security**—1 to 3 years installing, monitoring, and troubleshooting network devices to maintain integrity, confidentiality, and availability of data and devices

Related CVD Guides



Campus Wired LAN
Technology Design Guide



Firewall and IPS Technology
Design Guide

To view the related CVD guides, click the titles or visit [the CVD Foundation web site](#).

Introduction

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 is quickly spreading 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 Use Cases

In many cases, it is straightforward to enable native IPv6 on new or existing web servers. If possible, this method is the recommended approach because it simplifies many configuration details.

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.

Use Case: Enable Native IPv6 Access for Network Traffic Between the Internet and a Web Server DMZ Network

This guide enables the following network and security capabilities:

- **Add IPv6 routing to the outside and web server DMZ network**—Native IPv6 access requires that all IPv6 is enabled end-to-end. Every firewall interface that forwards IPv6 traffic must have an IPv6 address assigned and configured. The firewall must be configured with an IPv6 default route.
- **Permit HTTP/HTTPS access to web server DMZ network**—Similar to an IPv4-only deployment, an IPv6 security policy is created. Only specific traffic types from the Internet that are explicitly permitted are forwarded to the web DMZ network. The firewall inspects each session and implicitly allows the associated return traffic to be forwarded back to the Internet.

Use Case: Enable IPv6 Access for Network Traffic Between the Internet and an IPv4-only Web Server DMZ Network

This guide enables the following network and security capabilities:

- **Enable communication between IPv6 external network addresses and IPv4 internal network addresses by using Network Address Translation 64 (NAT64)**—The firewall must translate the IPv4 web server DMZ network addresses to outside, IPv6 addresses. For two way communications, outside IPv6 source addresses must also be translated by the firewall into IPv4 web server DMZ addresses.
- **Add IPv6 routing to the outside network**—IPv6 access requires that IPv6 is enabled on the outside interface of the firewall configured for NAT64. The firewall must be configured with an IPv6 default route.
- **Permit HTTP/HTTPS access to web server DMZ network**—Similar to IPv4-only and native IPv6 deployments, an IPv6-to-IPv4 security policy is created. Only specific traffic types from the Internet that are explicitly permitted are forwarded to the web DMZ network. The firewall inspects each session and implicitly allows the associated return traffic to be forwarded back to the Internet.

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.

Design Overview

The Cisco Validated Design (CVD) Internet edge design 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. A prerequisite for using this design guide is that you must have already followed the guidance in the [Firewall and IPS Technology Design Guide](#).

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 CVD enterprise 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 IPv6 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.

Deployment Details

How to Read Commands

This guide uses the following conventions for commands that you enter at the command-line interface (CLI).

Commands to enter at a CLI prompt:

```
configure terminal
```

Commands that specify a value for a variable:

```
ntp server 10.10.48.17
```

Commands with variables that you must define:

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

Commands at a CLI or script prompt:

```
Router# enable
```

Long commands that line wrap are underlined.

Enter them as one command:

```
police rate 10000 pps burst 10000  
packets conform-action
```

Noteworthy parts of system output (or of device configuration files) are highlighted:

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

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.

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. At a minimum, you must enable IPv6 on the outside interface(s) of your firewall.

The simplest method to enable IPv6 web services is to enable IPv6 on the web DMZ and on the web server. This method does not require the configuration of any address translation.

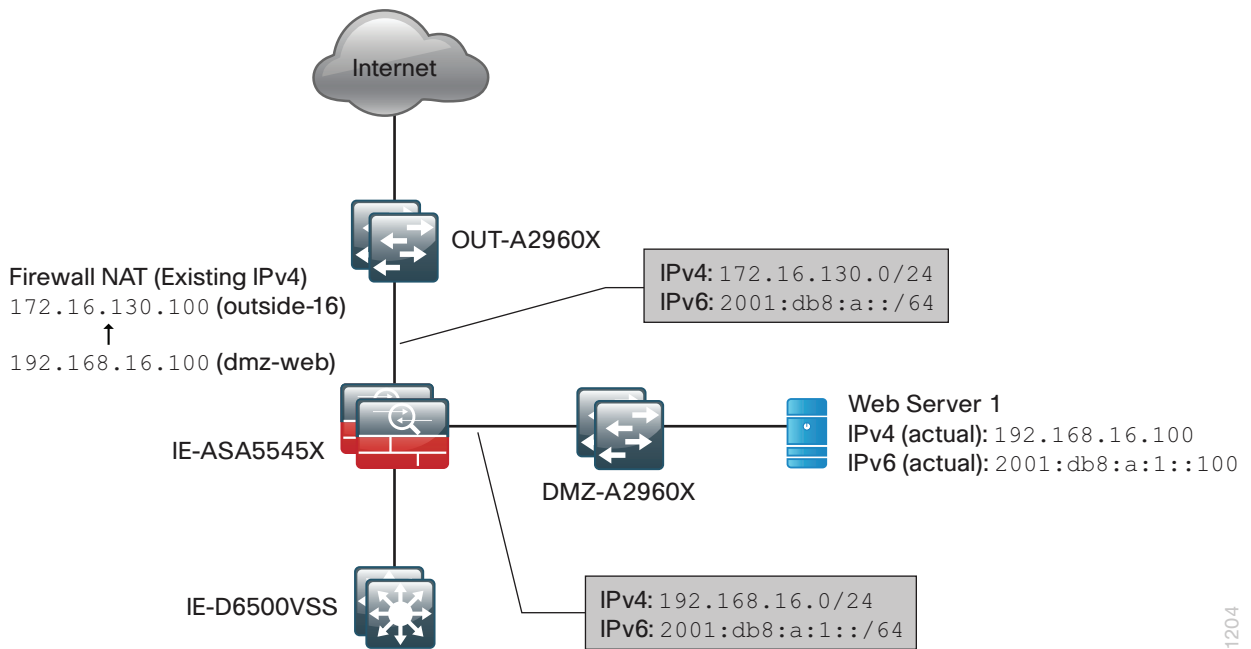


Reader Tip

The IPv4 to IPv4 address translation is shown in the following figures for completeness, but is not required to enable IPv6 web access.

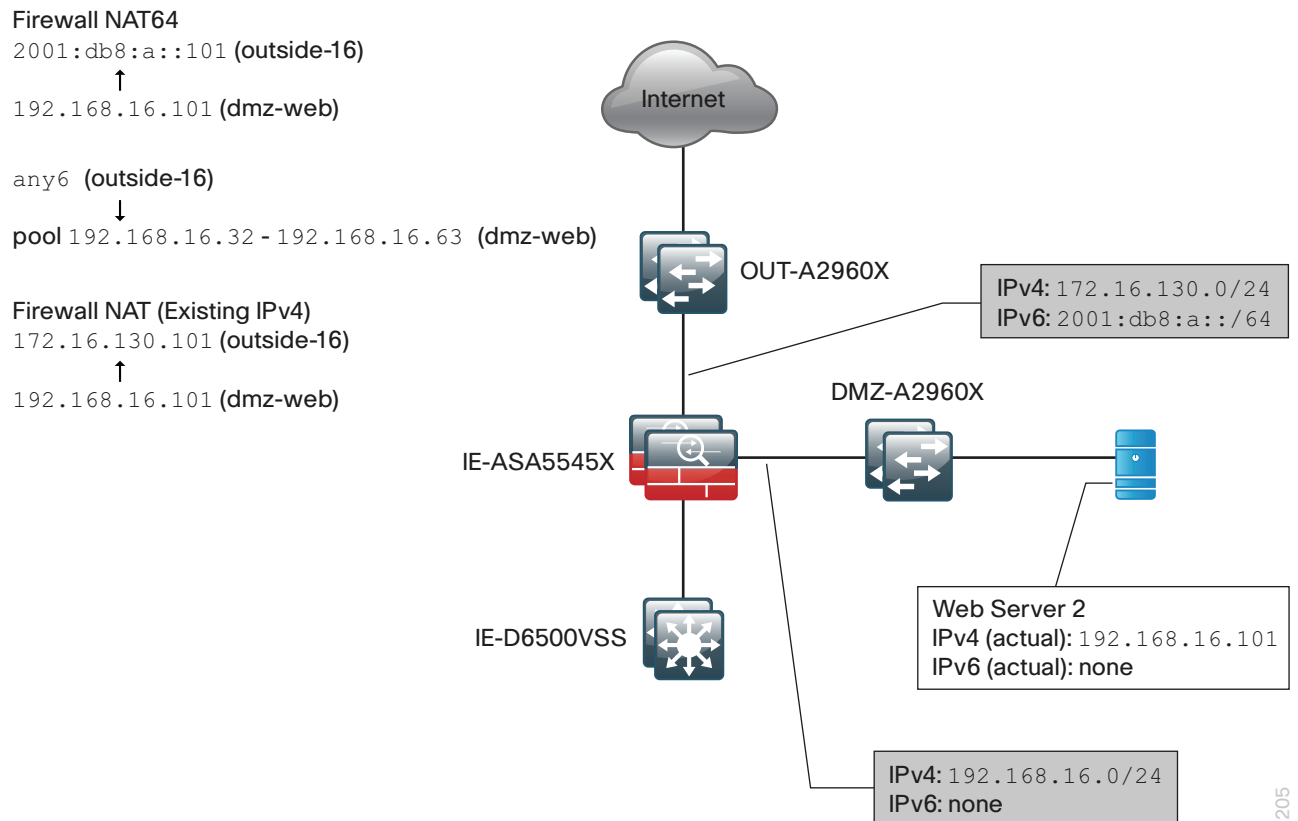
The full procedure to enable IPv4 web access is covered in the [Firewall and IPS Design Guide](#) in the Configuring the Web DMZ process.

Figure 1 - Native IPv6 web server access



If the web server is only running IPv4 and you want to allow IPv6 web clients to access the web server, then you must enable NAT64 on the firewall.

Figure 2 - IPv4 web server access using NAT64



Configuring IPv6 on the Cisco ASA Firewall

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

Procedure 1 Configure IPv6 on Cisco ASA interfaces

Table 1 - Cisco ASA firewall interface IPv6 addresses

Interface	Name	Active IPv6 address	Standby IPv6 address
GigabitEthernet0/3.16	outside-16	2001:db8:a::1/64	2001:db8:a::2
GigabitEthernet0/1.1116	dmz-web	2001:db8:a:1::1/64	2001:db8:a:1::2

Step 1: Connect to Cisco Adaptive Security Device Manager (ASDM) by navigating to <https://10.4.24.30>, and then log in with your username and password.

Step 2: Navigate to **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-email	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
GigabitEthernet0/1.1123	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		Enabled	0			native		Hardware/Management Only

Step 3: Repeat Step 4 through Step 7 for each interface listed in Table 1. If you are configuring NAT64, you need to follow this procedure for the outside interface only.

Step 4: Select the interface, and then click **Edit**. (Example: GigabitEthernet0/3.16)

The Edit Interface dialog box appears.

Step 5: On the Edit Interface dialog box, click the **IPv6** tab, select **Enable IPv6**, and then, under Interface IPv6 Addresses, click **Add**.

The 'Edit Interface' dialog box is shown with the 'IPv6' tab selected. The 'Enable IPv6' checkbox is checked. Below it, there are fields for 'DAD Attempts' (1), 'NS Interval' (1000 milliseconds), 'Reachable Time' (0 milliseconds), 'RA Lifetime' (1800 seconds), and 'RA Interval' (200 seconds). There are also checkboxes for 'Enforce EUI-64', 'Suppress RA', and 'RA Interval in Milliseconds'. At the bottom, there are checkboxes for 'Hosts should use DHCP for address config' and 'Hosts should use DHCP for non-address config'. The 'Interface IPv6 Addresses' section has a 'Link-local address' field and an 'Enable address autoconfiguration' checkbox. Below this is a table with columns 'Address' and 'EUI64'. To the right of the table are 'Add', 'Edit', and 'Delete' buttons. The 'Interface IPv6 Prefixes' section has a table with columns 'Address', 'Preferred Lifetime/Date', and 'Valid Lifetime/Date'. To the right of the table are 'Add', 'Edit', and 'Delete' buttons. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Step 6: In the Address/Prefix Length box, enter the active IPv6 address, and then click **OK**. (Example: 2001:db8:a::1/64)

The 'Add IPv6 Address for Interface' dialog box is shown. It has a single text field labeled 'Address/Prefix Length:' containing the text '2001:db8:a::1/64'. Below the field is a checkbox labeled 'EUI 64'. At the bottom are 'OK', 'Cancel', and 'Help' buttons.

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

Edit Interface

General Advanced **IPv6**

☒ 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	<input type="checkbox"/>

Interface IPv6 Prefixes

Address	Preferred Lifetime/Date	Valid Lifetime/Date
---------	-------------------------	---------------------

OK Cancel Help

Step 7: Click OK to close the window.

Step 8: After adding all of the active IPv6 addresses listed in Table 1, on the **Configuration > Device Setup > Interfaces** pane, click **Apply**.

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::1/64	255.255.255.0 64	vlan1116		Logical
GigabitEthernet0/1.1117	dmz-email	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
GigabitEthernet0/1.1123	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::1/64	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		Enabled	0			native		Hardware/Management Only

Add Edit Delete

Step 9: Navigate to **Configuration > Device Management > High Availability and Scalability > Failover**. Click the **Interfaces** tab. The interfaces configured for IPv4 and IPv6 are displayed.

Configuration > Device Management > High Availability and Scalability > Failover

Setup Interfaces Criteria MAC Addresses

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	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	<input checked="" type="checkbox"/>
		2001:db8:a::1	64		
GigabitEthernet0/1.1117	dmz-email	192.168.17.1	255.255.255.0	192.168.17.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1118	dmz-dmvpn	192.168.18.1	255.255.255.0	192.168.18.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1119	dmz-wlc	192.168.19.1	255.255.255.0	192.168.19.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1128	dmz-guests	192.168.28.1	255.255.252.0	192.168.28.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
		2001:db8:a::1	64		
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	<input checked="" type="checkbox"/>

Step 10: For each interface listed in Table 1, select the IPv6 interface (example: outside-16), double-click the empty **Standby IP Address** field, enter the standby IPv6 address as listed in Table 1, and then press **Enter**. (Example: 2001:db8:a::2)

GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
		2001:db8:a::1	64	2001:db8:a::2	<input type="checkbox"/>

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

Configuration > Device Management > High Availability and Scalability > Failover

Setup Interfaces Criteria MAC Addresses

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	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1116	dmz-web	192.168.16.1	255.255.255.0	192.168.16.2	<input checked="" type="checkbox"/>
		2001:db8:a::1	64	2001:db8:a::2	
GigabitEthernet0/1.1117	dmz-email	192.168.17.1	255.255.255.0	192.168.17.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1118	dmz-dmvpn	192.168.18.1	255.255.255.0	192.168.18.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1119	dmz-wlc	192.168.19.1	255.255.255.0	192.168.19.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1123	dmz-management	192.168.23.1	255.255.255.0	192.168.23.2	<input checked="" type="checkbox"/>
GigabitEthernet0/1.1128	dmz-guests	192.168.28.1	255.255.252.0	192.168.28.2	<input checked="" type="checkbox"/>
GigabitEthernet0/3.16	outside-16	172.16.130.124	255.255.255.0	172.16.130.123	<input checked="" type="checkbox"/>
		2001:db8:a::1	64	2001:db8:a::2	
GigabitEthernet0/3.17	outside-17	172.17.130.124	255.255.255.0	172.17.130.123	<input checked="" type="checkbox"/>

Procedure 2 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**.

Configuration > Device Setup > Routing > Static Routes

Specify static routes.

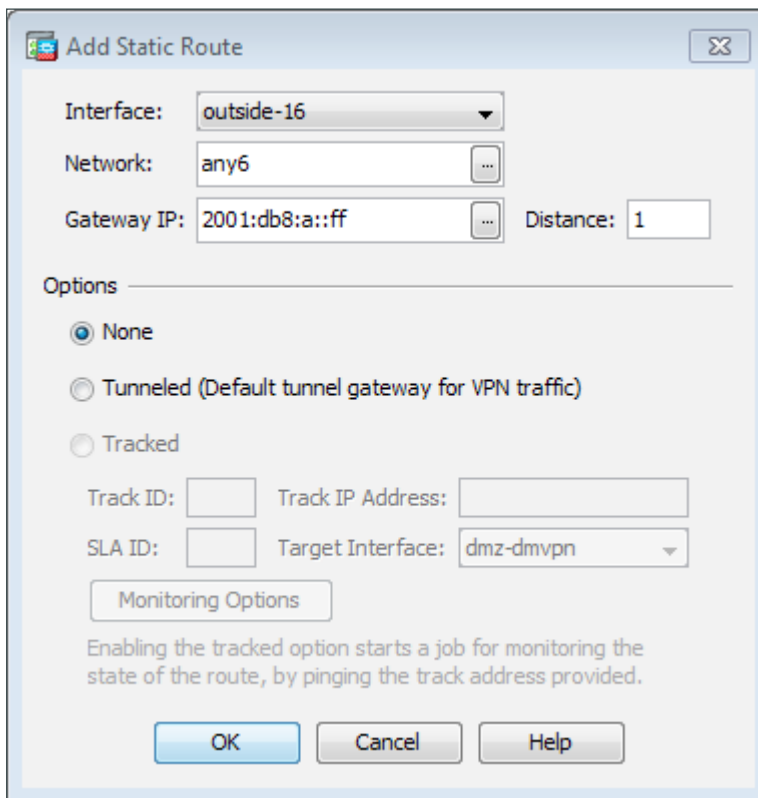
Filter: ☐ Both ☐ IPv4 only ☒ IPv6 only

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

Add Edit Delete

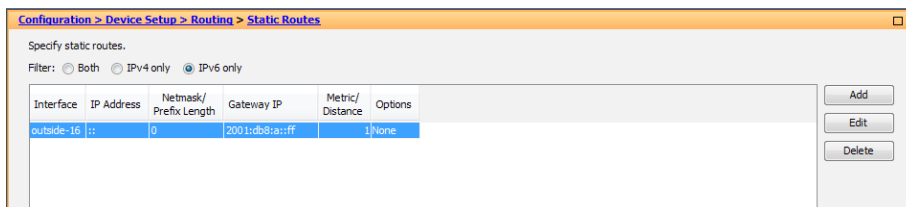
Step 2: Click **Add**. In the Add Static Route dialog box, enter the values below, and then click **OK**.

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



The 'Add Static Route' dialog box is shown. It has a title bar with a close button. The 'Interface' dropdown is set to 'outside-16'. The 'Network' text box contains 'any6'. The 'Gateway IP' text box contains '2001:db8:a::ff' and the 'Distance' text box contains '1'. Under the 'Options' section, the 'None' radio button is selected. There are also fields for 'Track ID', 'Track IP Address', 'SLA ID', and 'Target Interface' (set to 'dmz-dmvpn'). A 'Monitoring Options' button is below these fields. A note states: 'Enabling the tracked option starts a job for monitoring the state of the route, by pinging the track address provided.' At the bottom are 'OK', 'Cancel', and 'Help' buttons.

The static route table reflects the new values.



The 'Static Routes' configuration pane is shown. It has a title bar with the breadcrumb 'Configuration > Device Setup > Routing > Static Routes'. Below the title bar, it says 'Specify static routes.' and has a filter: 'Filter: Both IPv4 only IPv6 only' (with 'IPv6 only' selected). A table lists the static routes. The table has columns: Interface, IP Address, Netmask/Prefix Length, Gateway IP, Metric/Distance, and Options. There is one row with the following values: Interface: outside-16, IP Address: ::, Netmask/Prefix Length: 0, Gateway IP: 2001:db8:a::ff, Metric/Distance: 1, Options: None. To the right of the table are 'Add', 'Edit', and 'Delete' buttons.

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

Step 3: On the **Configuration > Device Setup > Routing > Static Routes** pane, click **Apply**.

Configuring Cisco ASA to permit IPv6 web access

1. Add a rule to permit HTTP/HTTPS traffic for native IPv6
2. Configure IPv6 to IPv4 Static Translation (NAT64)
3. Configure IPv6 Source Address Translation
4. Permit HTTP/HTTPS to the NATed Server

The [Firewall and IPS Technology Design Guide](#) includes the recommended procedures for deploying a pair of IPv4 web servers in a web DMZ. Only the additional steps to permit IPv6 access to the existing web DMZ are included here.

In the following procedures, Web Server 1 is configured for native IPv6 support end to end and does not require any NAT configuration. Web Server 2 is only configured for native IPv4 and the firewall is configured for NAT64 to provide IPv6 access.

Table 2 - Web server addresses

Host	IPv4 address	IPv6 address	NAT64 address
Web Server 1	192.168.16.100	2001:db8:a:1::100/64	NAT64 not required
Web Server 2	192.168.16.101	None	2001:db8:a::101/64

Procedure 1 Add a rule to permit HTTP/HTTPS traffic for native IPv6

This procedure is only required for a web server running native IPv6. If you are configuring NAT64, you may skip to Procedure 2.

Step 1: Navigate to **Configuration > Firewall > Access Rules**.



Tech Tip

Cisco ASA software 8.3(1) and later has the concept of Real IP. When you use 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.

Table 3 - Firewall policy rules for IPv6 web DMZ

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	any6	dmz-web-network6	tcp/http, tcp/https	Allow anyone to access the web servers in the DMZ using IPv6	Selected / Default

Step 2: Click the rule that permits traffic from **any4** to **dmz-web-network/24**.

6	<input checked="" type="checkbox"/>	any4			dmz-web-network/24		tcp http tcp https	<input checked="" type="checkbox"/> Permit
---	-------------------------------------	------	--	--	--------------------	--	-----------------------	--

Step 3: Click **Add > Insert After**.

The Add Access Rule dialog box appears.

Step 4: For Step 5 through Step 12, use the values listed in Table 3.

Step 5: In the **Interface** list, choose the interface. (Example: Any)

Step 6: For the **Action** option, select the action. (Example: Permit)

Step 7: In the **Source** box, select the source. (Example: any6)

Step 8: In the **Destination** box, select the destination. (Example: dmz-web-network6)

Step 9: In the **Service** box, enter the services. (Example: tcp/http, tcp/https)

Step 10: In the **Description** box, enter a useful description. (Example: Allow anyone to access the web servers in the DMZ using IPv6)

Step 11: Select or clear **Enable Logging**. (Example: Selected)

Step 12: In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

Insert After Access Rule

Interface: -- Any --

Action: ☒ Permit ☐ Deny

Source Criteria

Source: any6

User:

Security Group:

Destination Criteria

Destination: dmz-web-network6/64

Security Group:

Service: tcp/http, tcp/https

Description: Allow anyone to access the web servers in the DMZ using IPv6

☒ Enable Logging

Logging Level: Default

[More Options](#)

OK Cancel Help

The rule that you created appears in the Global rule table.

6	<input checked="" type="checkbox"/>	any4		dmz-web-network/24	tcp http tcp https	Permit
7	<input checked="" type="checkbox"/>	any6		dmz-web-network6/64	tcp http tcp https	Permit

Step 13: Click **Apply** on the Access Rules pane.

Step 14: If you are using native IPv6 to access your web server, you may skip Procedure 2 through Procedure 4.

Procedure 2 Configure IPv6 to IPv4 Static Translation (NAT64)

In this procedure, you map an outside IPv6 static address to the IPv4 address of the server in the web DMZ. This uses NAT64 to translate the destination address of the client connection from the Internet to the real IPv4 address on the server.

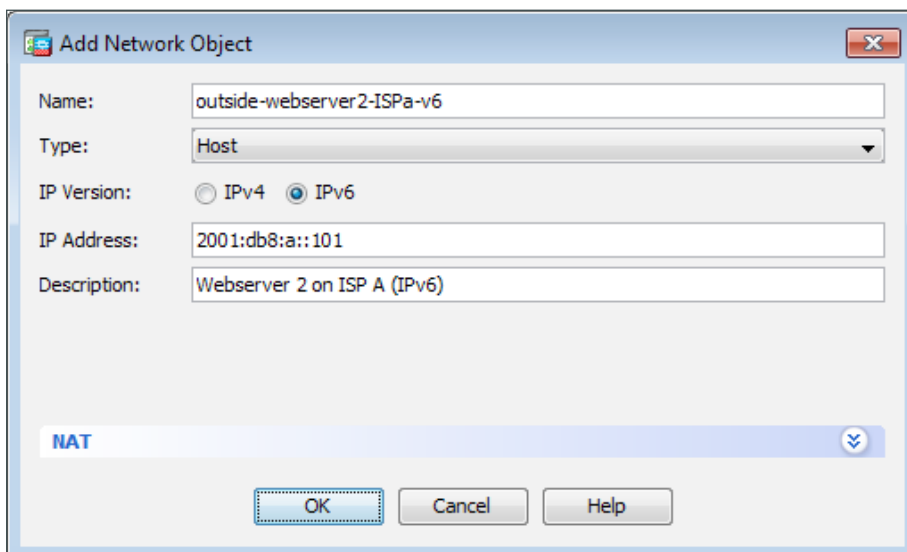
Tech Tip

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

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—**outside-webserver2-ISPa-v6**
- Type—**Host**
- IP Version—**IPv6**
- IP Address—**2001:db8:a::101**



The image shows the 'Add Network Object' dialog box with the following fields and values:

- Name:** outside-webserver2-ISPa-v6
- Type:** Host
- IP Version:** IPv4 (unselected), IPv6 (selected)
- IP Address:** 2001:db8:a::101
- Description:** Webserver 2 on ISP A (IPv6)
- NAT:** (dropdown menu)
- Buttons:** OK, Cancel, Help

Step 3: Click **Add**, and then select **Network Object**. The Add Network Object dialog box appears.

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

- Name—**dmz-webserver2-ISP-a-v6**
- Type—**Host**
- IP Version—**IPv4**
- IP Address—**192.168.16.101**

Step 5: Click the two down arrows. The NAT pane expands.

Step 6: Select **Add Automatic Address Translation Rules**.

Step 7: In the **Translated Addr** list, choose the network object created in Step 2.

Step 8: Select **Use one-to-one address translation**.

The screenshot shows the 'Add Network Object' dialog box. The top section contains fields for Name, Type, IP Version, IP Address, and Description. The 'NAT' pane is expanded below, showing options for adding automatic address translation rules. The 'Type' is set to 'Static', and the 'Translated Addr' is set to 'outside-webserver2-ISP-a-v6'. The 'Use one-to-one address translation' checkbox is checked. Other options like 'PAT Pool Translated Address', 'Round Robin', 'Extend PAT uniqueness', 'Translate TCP and UDP ports', 'Fall through to interface PAT', and 'Use IPv6 for interface PAT' are unchecked. An 'Advanced...' button is at the bottom of the NAT pane. At the very bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

Add Network Object

Name:

Type:

IP Version: ☒ IPv4 ☐ IPv6

IP Address:

Description:

NAT

☒ Add Automatic Address Translation Rules

Type:

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

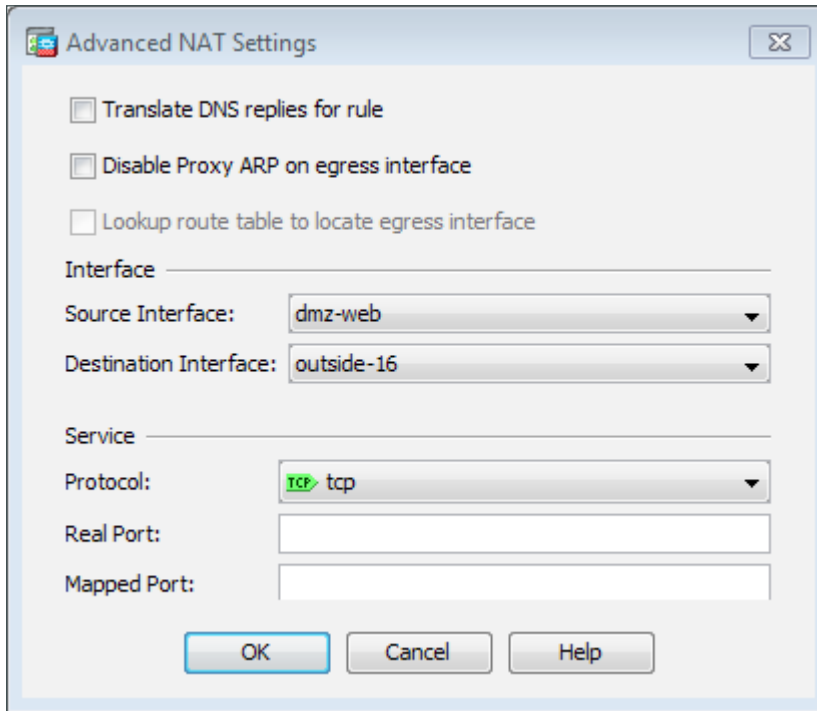
☐ Fall through to interface PAT(dest intf):

☐ Use IPv6 for interface PAT

Step 9: Click **Advanced**, the Advanced NAT Settings dialog box appears.

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

Step 11: On the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose **outside-16**, and then click **OK**.



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

Step 13: On the Network Objects/Groups pane, click **Apply**.

Now all traffic destined for **2001:db8:a::101** will be translated to **192.168.16.101**.

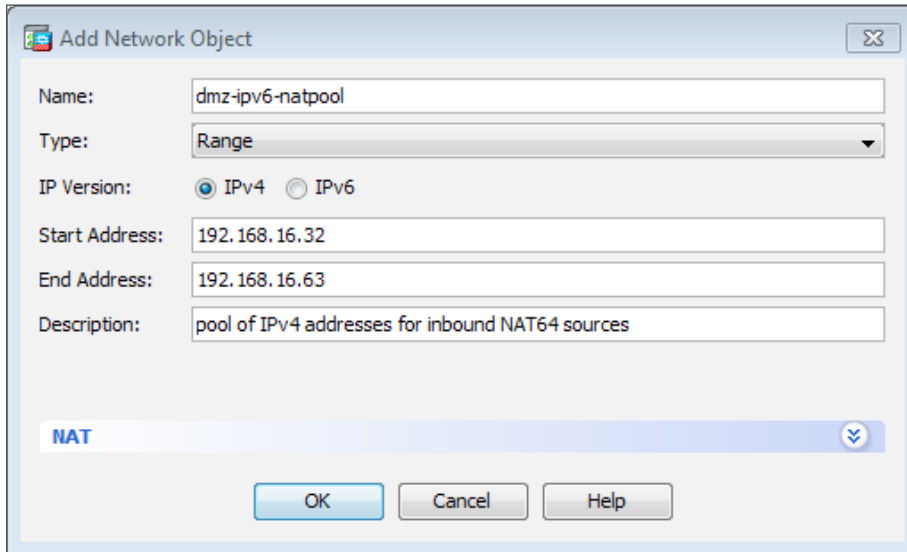
Procedure 3 Configure IPv6 Source Address Translation

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 client's 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 web 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**



Step 3: On the **Network Objects/Groups** pane, click **Apply**.

Step 4: Navigate to **Configuration > Firewall > NAT Rules**, and click **Add > Add “Network Object” Nat Rule**. The Add Network Object dialog box appears.

Step 5: 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 6: On the Add Network Object dialog box, in the NAT section, in **Type** list, choose **Dynamic**.

Step 7: 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 8: On the Browse PAT Pool Translated Address dialog box, locate the object (Example: dmz-ipv6-natpool) created in Step 2 of Procedure 2, “Configure IPv6 to IPv4 Static Translation (NAT64),” double-click the object, and then click **OK**.

Step 9: In the PAT Pool Translated Address list, choose Round Robin.

The image shows the 'Add Network Object' dialog box. The 'Name' field is 'outside-IPv6-all', 'Type' is 'Network', 'IP Version' is 'IPv6', 'IP Address' is '::', 'Prefix Length' is '0', and 'Description' is 'Any IPv6 address'. The 'NAT' section is expanded, showing 'Add Automatic Address Translation Rules' checked, 'Type' is 'Dynamic', 'Translated Addr' is empty, 'Use one-to-one address translation' is unchecked, 'PAT Pool Translated Address' is 'dmz-ipv6-natpool', 'Round Robin' is checked, 'Extend PAT uniqueness to per destination instead of per interface' is unchecked, 'Translate TCP and UDP ports into flat range 1024-65535' is unchecked, 'Include range 1-1023' is unchecked, 'Fall through to interface PAT(dest intf)' is 'dmz-dmvpn', and 'Use IPv6 for interface PAT' is unchecked. An 'Advanced...' button is at the bottom of the NAT section. The main dialog has 'OK', 'Cancel', and 'Help' buttons at the bottom.

Add Network Object

Name: outside-IPv6-all

Type: Network

IP Version: ☐ IPv4 ☒ IPv6

IP Address: ::

Prefix Length: 0

Description: Any IPv6 address

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): dmz-dmvpn

☐ Use IPv6 for interface PAT

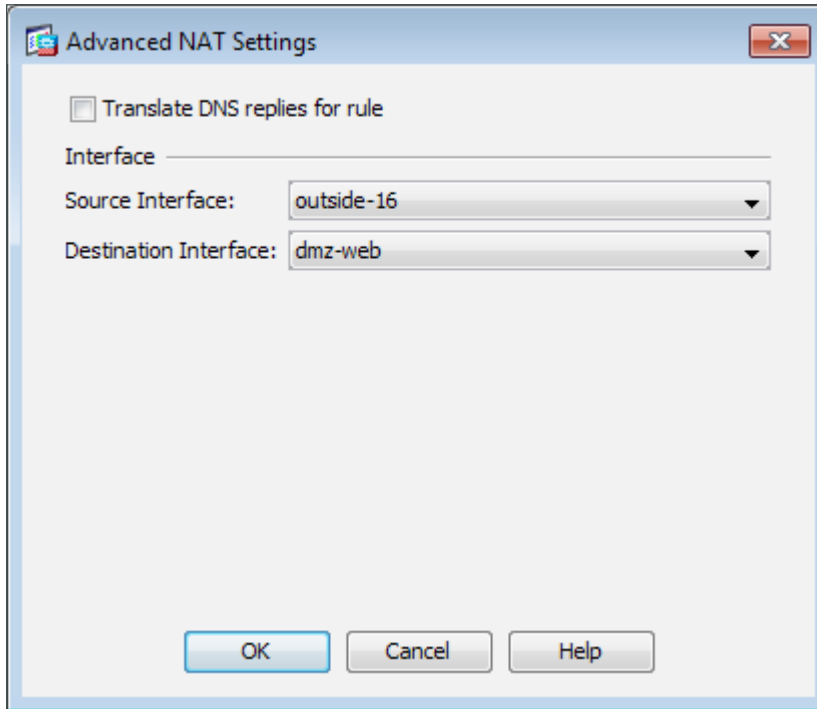
Advanced...

OK Cancel Help

Step 10: On the Add Network Object dialog box, click **Advanced**. The Advanced NAT Settings dialog box appears.

Step 11: On the Advanced NAT Settings dialog box, in the **Source Interface** list, choose **outside-16**.

Step 12: On the Advanced NAT Settings dialog box, in the **Destination Interface** list, choose **dmz-web**, and then click **OK**.



Step 13: On the Add Network Object dialog box, click **OK**.

Step 14: On the **Network Objects/Groups** pane, click **Apply**.

14	outside-16	dmz-web	outside-IPv6-all	any	any	dmz-ipv6-natpool (D) [PP,RR]	-- Original --	-- Original --
----	------------	---------	------------------	-----	-----	------------------------------	----------------	----------------

All client IPv6 source addresses are 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, and 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 4 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**.

Tech Tip

Cisco ASA software 8.3(1) and later has the concept of Real IP. When you use 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.

Table 4 - Firewall policy rules for IPv6 web DMZ

Interface	Action	Source	Destination	Service	Description	Logging Enable / Level
Any	Permit	any6	dmz-web-network/24	tcp/http, tcp/https	Allow anyone to access the IPv4 web servers in the DMZ using IPv6	Selected / Default

Click the rule that permits traffic from **any4** to **dmz-web-network**.

6		 any4		 dmz-web-network/24		 tcp http  tcp https	 Permit
---	---	--	--	--	--	--	--

Step 2: Click **Add > Insert After**.

The Add Access Rule dialog box appears.

Step 3: For Step 5 through Step 12, use the values listed in Table 4.

Step 4: In the **Interface** list, choose the interface. (Example: Any)

Step 5: For the **Action** option, select the action. (Example: Permit)

Step 6: In the **Source** box, select the source. (Example: any6)

Step 7: In the **Destination** box, select the destination. (Example: dmz-web-network/24)

Step 8: In the **Service** box, enter the services. (Example: tcp/http, tcp/https)

Step 9: In the **Description** box, enter a useful description. (Example: Allow anyone to access the IPv4 web servers in the DMZ using IPv6)

Step 10: Select or clear **Enable Logging**. (Example: Selected)

Step 11: In the **Logging Level** list, choose the logging level value, and then click **OK**. (Example: Default)

Insert After Access Rule

Interface:

-- Any --

Action:

☒ Permit

☐ Deny

Source Criteria

Source:

any6

User:

Security Group:

Destination Criteria

Destination:

dmz-web-network/24

Security Group:

Service:

tcp/http, tcp/https

Description:

Allow anyone to access the IPv4 web servers in the DMZ using IPv6

☒ Enable Logging

Logging Level:

Default

More Options

OK

Cancel

Help

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

6	<input checked="" type="checkbox"/>	<div>any4</div>		<div>dmz-web-network/24</div>	<div><div>tcp http</div><div>tcp https</div></div>
7	<input checked="" type="checkbox"/>	<div>any6</div>		<div>dmz-web-network5/64</div>	<div><div>tcp http</div><div>tcp https</div></div>
8	<input checked="" type="checkbox"/>	<div>any6</div>		<div>dmz-web-network/24</div>	<div><div>tcp http</div><div>tcp https</div></div>

Step 12: After adding all of the rules in Table 4, in the order listed, click **Apply** on the Access Rules pane.

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

Configuring IPv6 on the DMZ Web Server

1. Configure IPv6 on a Windows 2008 server

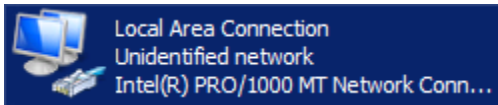
Procedure 1

Configure IPv6 on a Windows 2008 server

In this procedure, you configure the web server DMZ network interface on a Windows 2008 server to support IPv6. This is used for direct untranslated access to the server from IPv6 clients. This procedure is not required if you are configuring NAT64.

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.

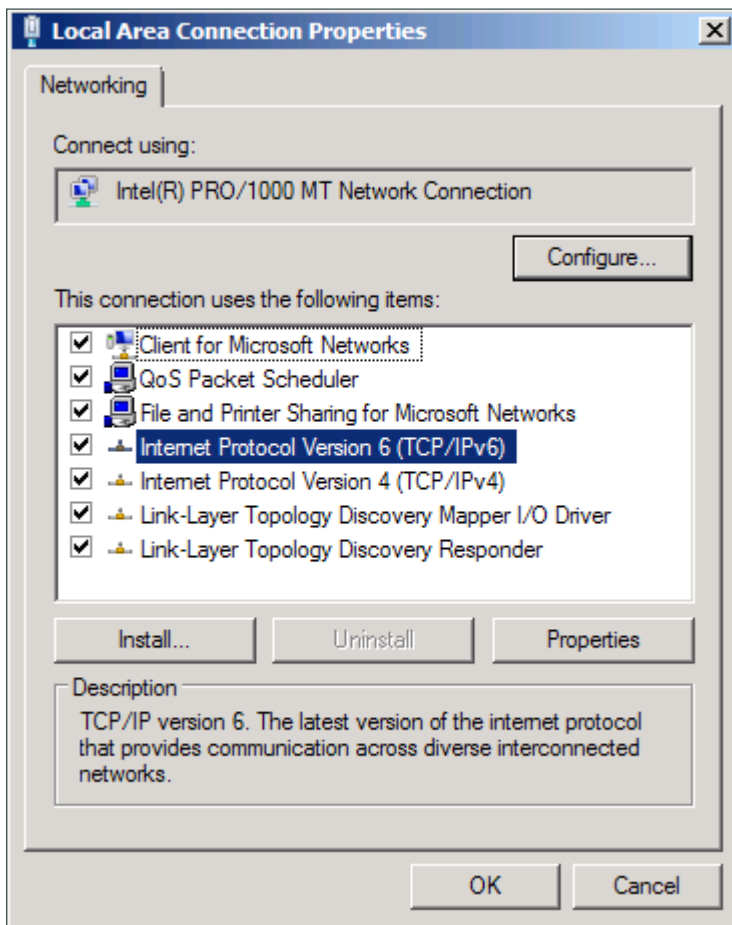
If the **Internet Protocol Version 6 (TCP/IPv6)** check box is selected, proceed to the following step.



Tech Tip

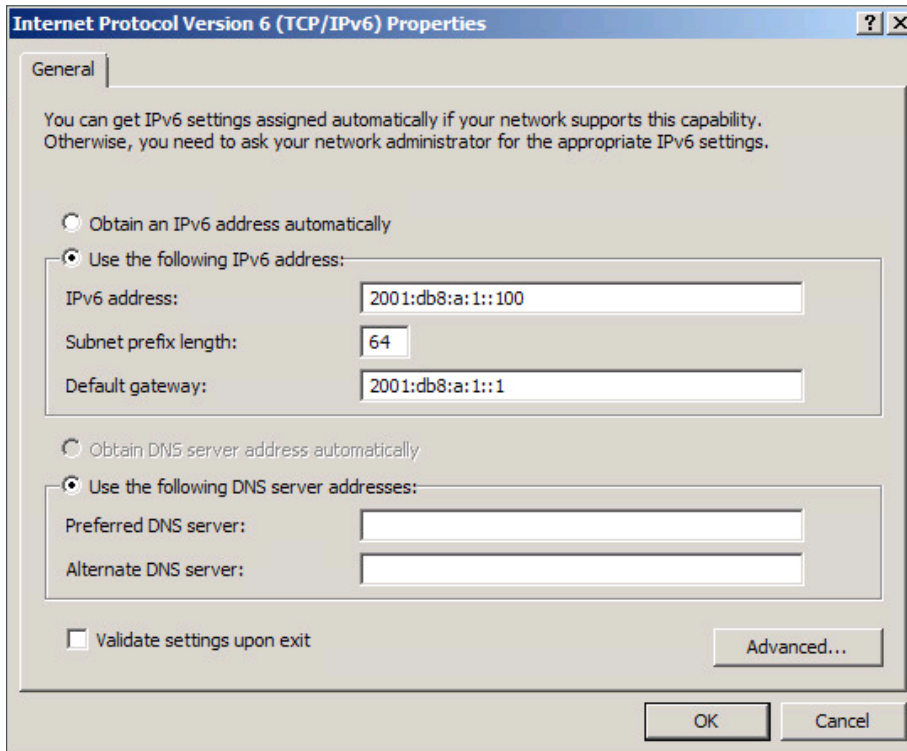
If you do not close and reopen the page the first time you enable IPv6, you will get an error and be unable to provision an IPv6 address.

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



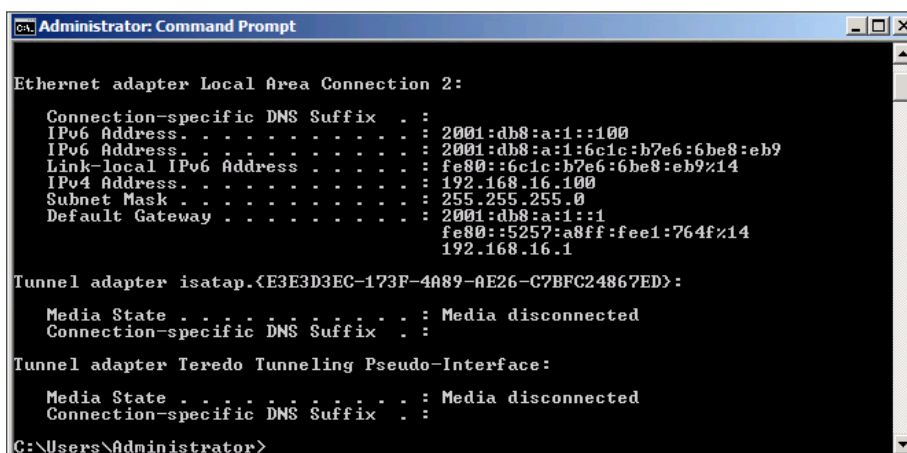
Step 6: On the Internet Protocol Version 6 (TCP/IPv6) Properties dialog box, select **Use the following IPv6 address**, enter the following values, and then click **OK**.

- IPv6 Address—**2001:db8:a:1::100**
- 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.



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 9.1(5) IPS 7.1(8p2)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 ASA 5512-X Security Plus license	ASA5512-SEC-PL	
	Firewall Management	ASDM	7.1(6)

Internet Edge LAN

Functional Area	Product Description	Part Numbers	Software
DMZ Switch	Cisco Catalyst 2960-X Series 24 10/100/1000 PoE and 2 SFP+ Uplink	WS-C2960X-24PS	15.0(2)EX5 LAN Base feature set
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	
Outside Switch	Cisco Catalyst 2960-X Series 24 10/100/1000 PoE and 2 SFP+ Uplink	WS-C2960X-24PS	15.0(2)EX5 LAN Base feature set
	Cisco Catalyst 2960-X FlexStack-Plus Hot-Swappable Stacking Module	C2960X-STACK	

Appendix B: CLI Configuration

ASA Firewall IE-ASA5545X

```
ASA Version 9.1(5)
!
hostname IE-ASA5545X
domain-name cisco.local
!
interface GigabitEthernet0/1.1116
  description Web DMZ server connection in VLAN 1116
  vlan 1116
  nameif dmz-web
  security-level 50
  ip address 192.168.16.1 255.255.255.0 standby 192.168.16.2
  ipv6 address 2001:db8:a:1::1/64 standby 2001:db8:a:1::2
  ipv6 enable
!
interface GigabitEthernet0/3.16
  description Primay internet connection on VLAN 16
  vlan 16
  nameif outside-16
  security-level 0
  ip address 172.16.130.124 255.255.255.0 standby 172.16.130.123
  ipv6 address 2001:db8:a::1/64 standby 2001:db8:a::2
  ipv6 enable
!
object network outside-webserver1-ISPa
  host 172.16.130.100
  description Webserver1 on ISP A
object network dmz-webserver1-ISPa
  host 192.168.16.100
  description NAT webserver1 in the DMZ to the outside address on ISP A
object network outside-webserver1-ISPb
  host 172.17.130.100
  description Webserver1 on ISP B
object network dmz-webserver1-ISPb
  host 192.168.16.100
  description NAT webserver1 in the DMZ to the outside address on ISP B
object network outside-webserver2-ISPa
  host 172.16.130.101
  description Webserver2 on ISP A
object network outside-webserver2-ISPb
  host 172.17.130.101
```

```

description Webserver2 on ISP B
object network dmz-webserver2-ISPa
  host 192.168.16.101
description NAT webserver2 in the DMZ to the outside address on ISP A
object network dmz-webserver2-ISPb
  host 192.168.16.101
description NAT webserver2 in the DMZ to the outside address on ISP B
object network dmz-ipv6-natpool
  range 192.168.16.32 192.168.16.63
description pool of IPv4 addresses for inbound NAT64 sources
object network dmz-webserver2-ISPa-v6
  host 192.168.16.101
description NAT IPv4 webserver 2 in the DMZ to the outside IPv6 address on ISP A
object network outside-webserver2-ISPa-v6
  host 2001:db8:a::101
description Webserver 2 on ISP A (IPv6)
object network outside-IPv6-all
  subnet ::/0
description Any IPv6 address
!
object-group service DM_INLINE_TCP_1 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_TCP_4 tcp
  port-object eq www
  port-object eq https
object-group service DM_INLINE_TCP_5 tcp
  port-object eq www
  port-object eq https
!
access-list global_access remark Allow anyone to access the webserver in the DMZ
access-list global_access extended permit tcp any4 192.168.16.0 255.255.255.0 object-
group DM_INLINE_TCP_1
access-list global_access remark Allow anyone to access the webserver in the DMZ using
IPv6
access-list global_access extended permit tcp any6 2001:db8:a:1::/64 object-group
DM_INLINE_TCP_4
access-list global_access remark Allow anyone to access the IPv4 webserver in the DMZ
using IPv6
access-list global_access extended permit tcp any6 192.168.16.0 255.255.255.0 object-
group DM_INLINE_TCP_5
!
object network dmz-webserver1-ISPa
  nat (any,outside-16) static outside-webserver1-ISPa
object network dmz-webserver1-ISPb
  nat (any,outside-17) static outside-webserver1-ISPb
object network dmz-webserver2-ISPa

```

```

    nat (any,outside-16) static outside-webserver2-ISPa
object network dmz-webserver2-ISPb
    nat (any,outside-17) static outside-webserver2-ISPb
object network dmz-webserver2-ISPa-v6
    nat (dmz-web,outside-16) static outside-webserver2-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::ff
!
: end

```

Feedback

Please use the [feedback form](#) to send comments and suggestions about this guide.



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.

© 2014 Cisco Systems, Inc. All rights reserved.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)