

ASA 8.x: Basic IPv6 Configuration on ASA Using ASDM Configuration Example

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[Background Information](#)

[Configure](#)

[Enable IPv6 on the required interface](#)

[Define the IPv6 access-lists where required](#)

[Specify the IPv6 route information](#)

[Verify](#)

[Troubleshoot](#)

[Related Information](#)

[Introduction](#)

This document describes a basic configuration that enables IPv6 on Cisco Adaptive Security Appliance (ASA) in order to pass the IPv6 packets. This configuration is shown using the Adaptive Security Device Manager (ASDM). Support on Cisco ASA for the IPv6 packets is available from Cisco ASA software version 7.0(1) itself. However, the support to configure through ASDM is available from Cisco ASDM software version 6.2 onwards.

[Prerequisites](#)

[Requirements](#)

There are no specific requirements for this document.

[Components Used](#)

The information in this document is based on these software and hardware versions:

- Cisco ASA with version 8.2
- Cisco ASDM with version 6.3

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Refer to the [Cisco Technical Tips Conventions](#) for more information on document conventions.

Background Information

In order to pass the IPv6 packets through the ASA, complete these high-level steps:

1. [Enable IPv6 on the required interfaces.](#)
2. [Define the IPv6 access-lists where required.](#)
3. [Specify the IPv6 route information.](#)

Configure

Complete these detailed steps.

Enable IPv6 on the required interface

1. Choose **Configuration > Device Setup > Interface**, select the required interface, and click **Edit**.
2. Click the **IPv6** tab in order to specify the related IPv6 settings.
3. Choose the **Enable IPv6** option, then click **Add** in the Interface IPv6 Addresses section.

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

Interface IPv6 Addresses

Link-local address: []

☐ Enable address autoconfiguration

Address	EUI64
---------	-------

[Add] [Edit] [Delete]

Interface IPv6 Prefixes

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

[Add] [Edit] [Delete]

[OK] [Cancel] [Help]

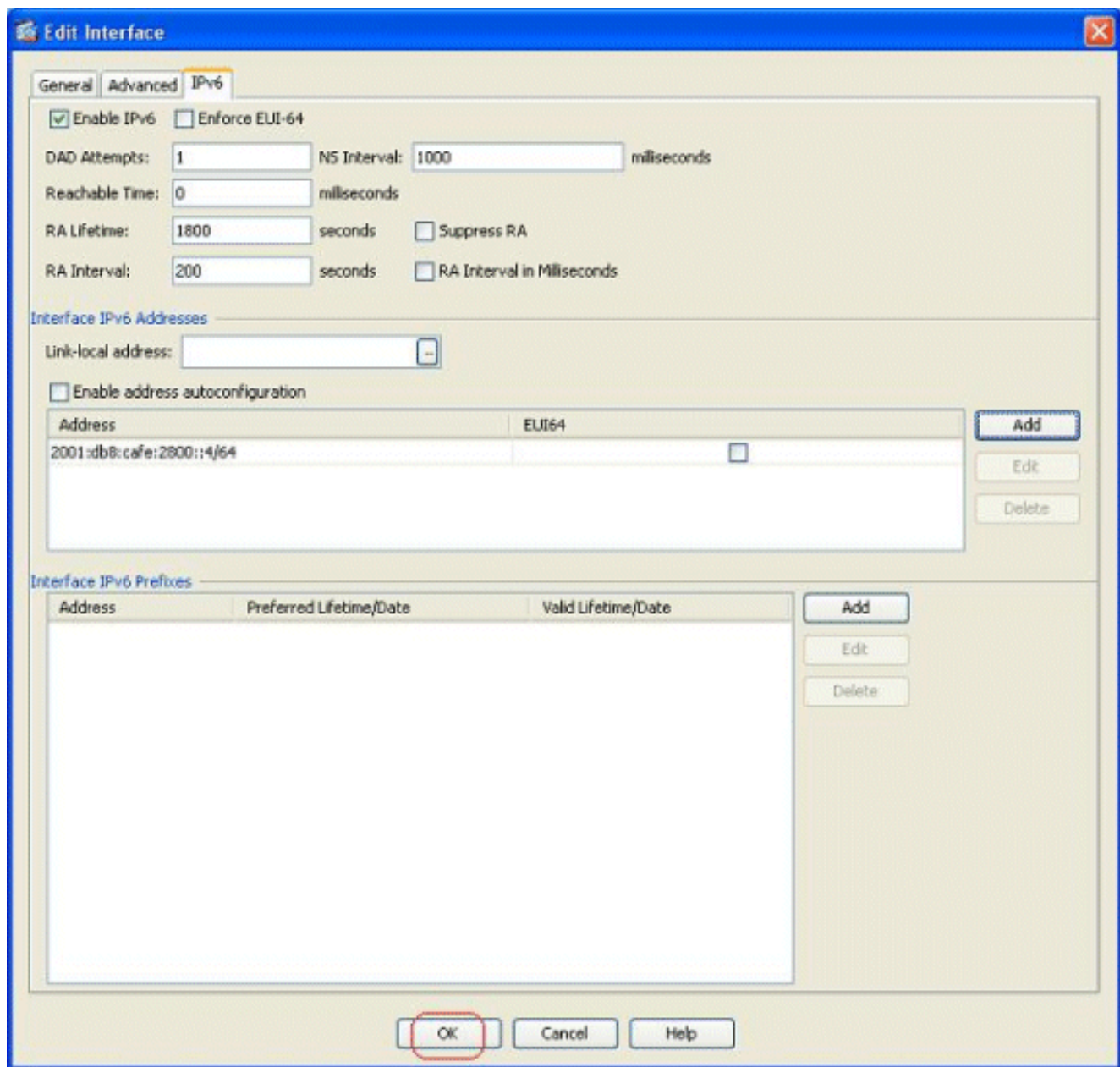
Add IPv6 Address for Interface

Address/Prefix Length: 2001:DB8:CAFE:2800::4/64

☐ EUI 64

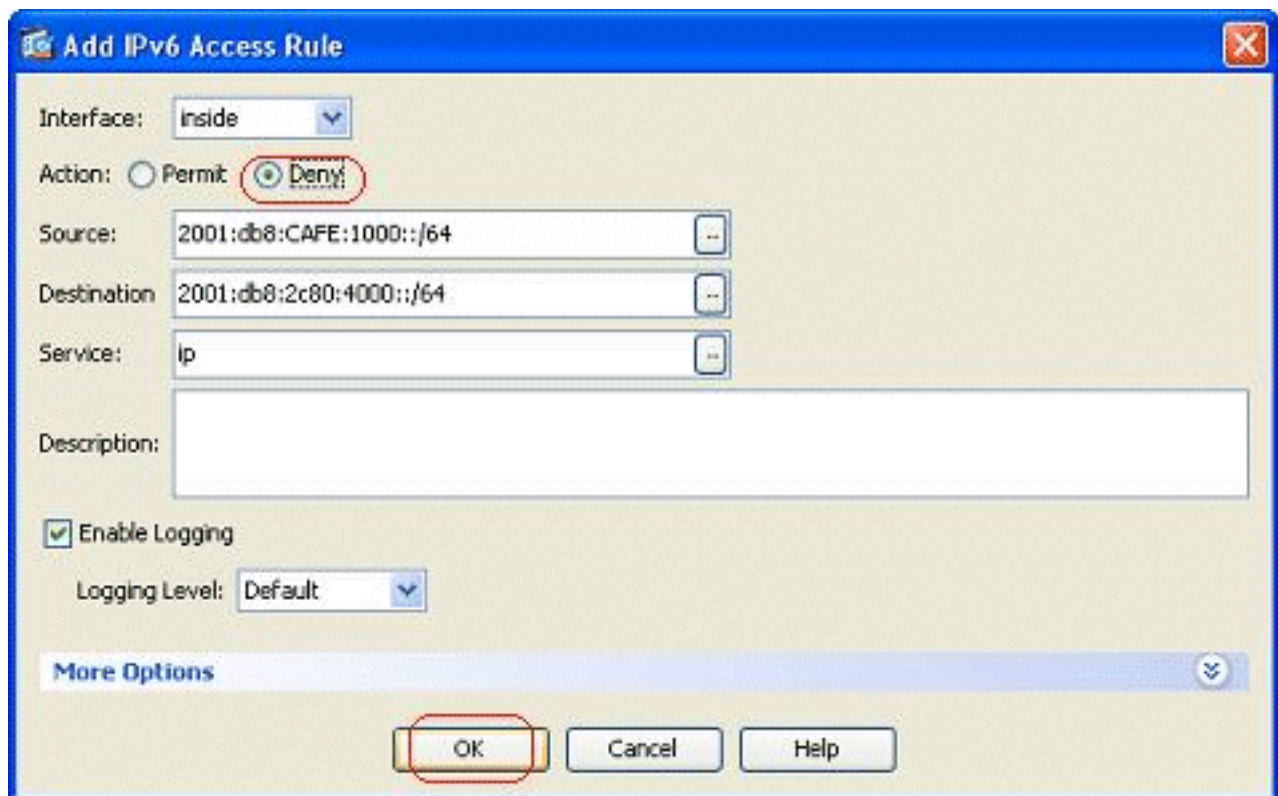
[OK] [Cancel] [Help]

4. Click **OK**.
5. Click **OK** in order to revert back to the Interfaces pane.



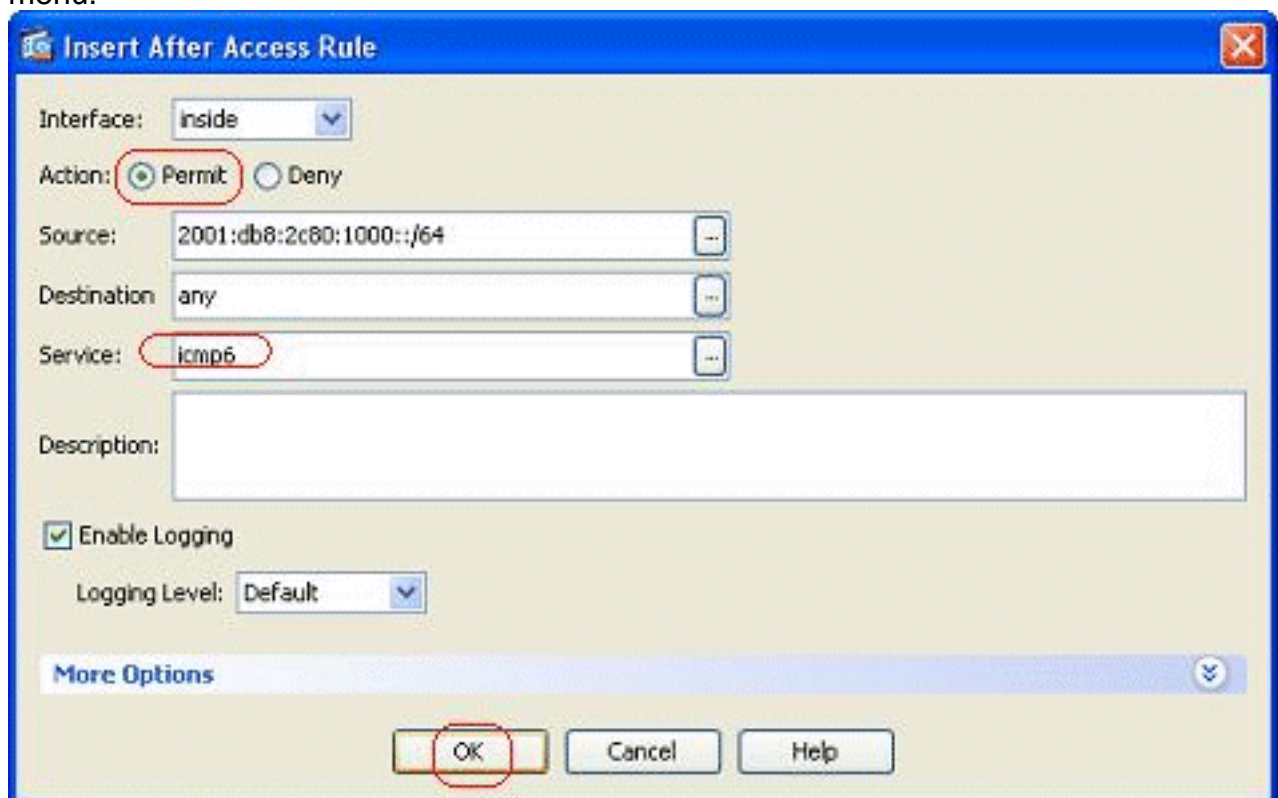
Define the IPv6 access-lists where required

1. Choose **Configuration > Firewall > Access Rules**, and click on the **Add** drop-down button in order to select the **Add IPv6 Access Rule** option. A new window appears:



The 'Add IPv6 Access Rule' dialog box is shown. It has a blue title bar with a close button. The interface includes a dropdown for 'Interface' set to 'inside'. The 'Action' section has two radio buttons: 'Permit' and 'Deny', with 'Deny' selected and circled in red. Below are text fields for 'Source' (2001:db8:CAFE:1000::/64), 'Destination' (2001:db8:2c80:4000::/64), and 'Service' (ip), each with a browse button (...). A large text area for 'Description' is empty. There is a checked checkbox for 'Enable Logging' and a dropdown for 'Logging Level' set to 'Default'. A 'More Options' section is collapsed. At the bottom are 'OK', 'Cancel', and 'Help' buttons, with 'OK' circled in red.

2. Click **OK**, and click **Insert After** in order to add another access rule option from the **Add** drop-down menu.



The 'Insert After Access Rule' dialog box is shown. It has a blue title bar with a close button. The interface includes a dropdown for 'Interface' set to 'inside'. The 'Action' section has two radio buttons: 'Permit' and 'Deny', with 'Permit' selected and circled in red. Below are text fields for 'Source' (2001:db8:2c80:1000::/64), 'Destination' (any), and 'Service' (icmp6), each with a browse button (...). A large text area for 'Description' is empty. There is a checked checkbox for 'Enable Logging' and a dropdown for 'Logging Level' set to 'Default'. A 'More Options' section is collapsed. At the bottom are 'OK', 'Cancel', and 'Help' buttons, with 'OK' circled in red.

3. Click **OK**. The configured access rules can be seen here:

Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Description
dmz IPv6 (1 implicit incoming rule)									
1	<input checked="" type="checkbox"/>	any	Any less secure ne...	ip	Permit				Implicit rule
inside IPv6 (2 incoming rules)									
1	<input type="checkbox"/>	2001:db8:cafe:10...	2001:db8:2c80:40...	ip	Deny				
2	<input checked="" type="checkbox"/>	2001:db8:2c80:10...	any	icmp6	Permit				
mgmt IPv6 (0 implicit incoming rules)									
outside IPv6 (0 implicit incoming rules)									
partner-dmz IPv6 (1 implicit incoming rule)									
1	<input checked="" type="checkbox"/>	any	Any less secure ne...	ip	Permit				Implicit rule
Global IPv6 (1 implicit rule)									
1	<input type="checkbox"/>	any	any	ip	Deny				Implicit rule

4. Choose the **IPv6 access rules only** option.

Specify the IPv6 route information

1. Choose **Configuration > Device Setup > Routing > Static Routes**, and click **Add** in order to add a route.
2. Click **OK** in order to revert back to the Static Routes

Add Static Route

Interface:

IP Address: Prefix Length:

Gateway IP: Distance:

Options

☒ None

☐ Tunneled (Default tunnel gateway for VPN traffic)

☐ Tracked

Track ID: Track IP Address:

SLA ID: Target Interface:

Monitoring Options

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

pane.

3. Choose **IPv6 Routes Only** in order to view the configured route.

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
inside	2001:db8:2c80:1000::	64	2001:db8:cafe:2600::	1	None

This concludes the basic configuration required in order for the ASA to route the IPv6 packets.

[Verify](#)

There is currently no verification procedure available for this configuration.

[Troubleshoot](#)

There is currently no specific troubleshooting information available for this configuration.

[Related Information](#)

- [ASA Configuration Examples and TechNotes](#)
- [Configuring IPv6 Addressing](#)
- [Technical Support & Documentation - Cisco Systems](#)