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.

General Advance	d IPv6		
(man in man)			
Enable IPv6	Enforce EUI-	64	
DAD Attempts:	1	N5 Interval:	1000 miliseconds
Reachable Time:	0	miliseconds	
RA Lifetime:	1800	seconds	Suppress RA
RA Interval:	200	seconds	RA Interval in Miliseconds
nterface IPv6 Add	resses		
Link-local address			G
Enable addre	ss autoconfigurati	ion	_
Address			EUI64 Add
			Delete
			Delete
		[OK Cancel Help
	Add IPv	(6 Addres	OK Cancel Heb
	Add IP v Address/P	(<mark>6 Addres</mark> Prefix Lengt	OK Cancel Heb s for Interface h: 2001:DB8:CAFE:2800::4¥64

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

eneral Advance	d IPv6						
Enable IPv6	Enforce EU	1-64					
DAD Attempts:	1	N5 Interval:	1000		miliseconds		
Reachable Time:	0	miliseconds					
RA Lifetime:	1800	seconds	Suppress R/	A			
RA Interval:	200	seconds	RA Interval	in Milliseconds			
erface IPv6 Addr	ACCAC						
ink-local address:			-				
Enable addres	s autoconfigura	ation					
Address			1	EUI64			Add
2001:db8:cafe:28	800::4/64						Edit
2001:db8:caře:26	800::4/64						Edk Delete
erface IPv6 Prefo Address	800::4/64 xes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add	Edt
erface IPv6 Prefo Address	800::4/64 Kes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add	Edt Delete
erface JPv6 Prefo Address	800:::4/64 xes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt
erface IPv6 Prefix Address	800::4/64 xes Pref	erred Lifetime/Date		Valid Lifetim	e/Date	Add Edit Delete	Edt
erface IPv6 Prefo Address	800::4/64 Kes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt
erface IPv6 Prefo Address	800:::4/64 xes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt
erface IPv6 Prefo Address	800::4/64 xes Pref	'erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt
erface IPv6 Prefo Address	800::4/64 xes Pref	erred Lifetime/Date	2 2 2 2 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	Valid Lifetim	e/Date	Add Edt Delete	Edt
erface IPv6 Prefo Address	800:::4/64 xes Pref	erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt
2001:db8:cafe:28	800::4/64 xes Pref	'erred Lifetime/Date	8	Valid Lifetim	e/Date	Add Edit Delete	Edt

Define the IPv6 access-lists where required

 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:

🔂 Add IPv	6 Access Rule	X
Interface: Action: 🔿	Inside V	
Source:	2001:db8:CAFE:1000::/64	
Destination	2001:db8:2c80:4000::/64	
Service:	lp	
Description:		
Enable L	ogging	
Logging	Level: Default 💌	
More Opt	ions	*
	OK Cancel Help	

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

🕼 Insert /	After Access Rule	X
Interface: Action:	Permit O Deny	
Source:	2001:db8:2c80:1000::/64	
Destination	any	
Service: 🤇	icmp6	
Description:		
C Enable I	Logging	
Logging	Level: Default	
More Op	tions	۲

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

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time	Descript
a 🚚 d	mz IPv6 (1 im	plicit incoming rule)							
1		any	Any less secure ne	🗶 ip	🖌 Permit				Implicit ru
3.50 in	nside IPv6 (2	incoming rules)							
1		2001:db8:cafe:10	2001:db8:2c80:40	3P lp	3 Deny				
2	v	2001:db8:2c80:10	 any 	icmp6	🖌 Permit				
	ngmt IPv6 (0 i	mplicit incoming rules)							
	utside IPv6 (0 implicit incoming rules)							
- P	artner-dmz I	Pv6 (1 implicit incoming rule)							
1		i any	Any less secure ne	🕑 ip	🖌 Permit				Implicit ru
🚽 👎 G	ilobal IPv6 (1	implicit rule)							
1		any	any	<u>ae</u> ∕ip	3 Deny				Implicit ru

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

Incenace:	inside	~			
IP Address:	2001:db8:2c80:	:1000:: 🔄	Prefix Length:	64	
Gateway IP:	2001:db8:CAFE	:2800::9	Distance:	1	
otions					
 None 					
	(Default tunnel)	gateway for VP	N traffic)		
O Tracked					
Track ID:		Track IP Ad	iress:		
SLA ID:		Target Inter	face: dmz		
Monitor	ing Options				
Enabling th	ie tracked option	starts a job for	monitoring th	e state of the	route
	the track address	s provided.			

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

figuration	> Device Setup > Rou routes.	ting > Static Ro	<u>utes</u>			
Filter: O Bo	th OIPv4 only OIP	v6 only				
Interface	IP Address	Netmask/ Prefix Length	Gateway IP	Metric/ Distance	Options	
No. of Concession, Name	2001-db8-2-80-1000	64	2001:db8:cafe:2800:	seway IP	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
- <u>Configuring IPv6 Addressing</u>
- <u>Technical Support & Documentation Cisco Systems</u>