

ASA 8.x : ASA 8.x : ASDM を使用した ASA での基本的な IPv6 の設定例

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[必要なインターフェイスのイネーブル IPv6](#)

[IPv6 access-list を必要なところに定義して下さい](#)

[IPv6 ルート情報を規定して下さい](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、IPv6 パケットを渡すために Cisco 適応型セキュリティ アプライアンス (ASA) で IPv6 をイネーブルにする基本設定について説明します。この設定では、Adaptive Security Device Manager (ASDM) を使用して示します。IPv6 パケット用の Cisco ASA のサポートは Cisco ASA ソフトウェア バージョン 7.0(1) 自体から使用できます。ただし、ASDM を使用して設定するためのサポートは、Cisco ASDM ソフトウェア バージョン 6.2 以降で使用できません。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- バージョン 8.2 が付いている Cisco ASA
- バージョン 6.3 が付いている Cisco ASDM

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始して

います。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

背景説明

IPv6 パケットを ASA を通して渡すために、これらの高レベル ステップを完了して下さい:

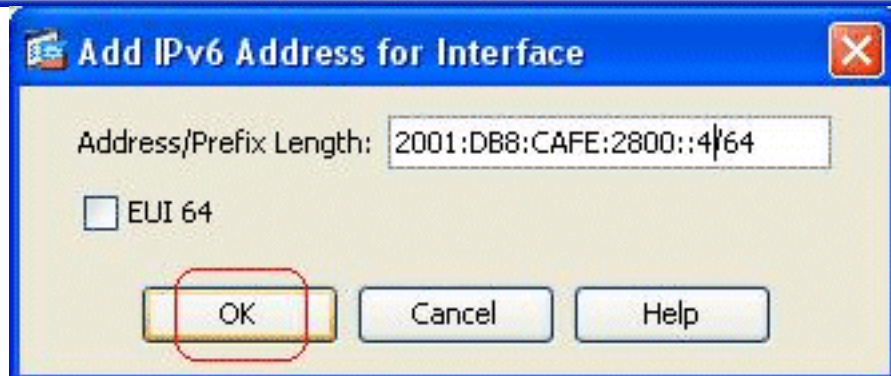
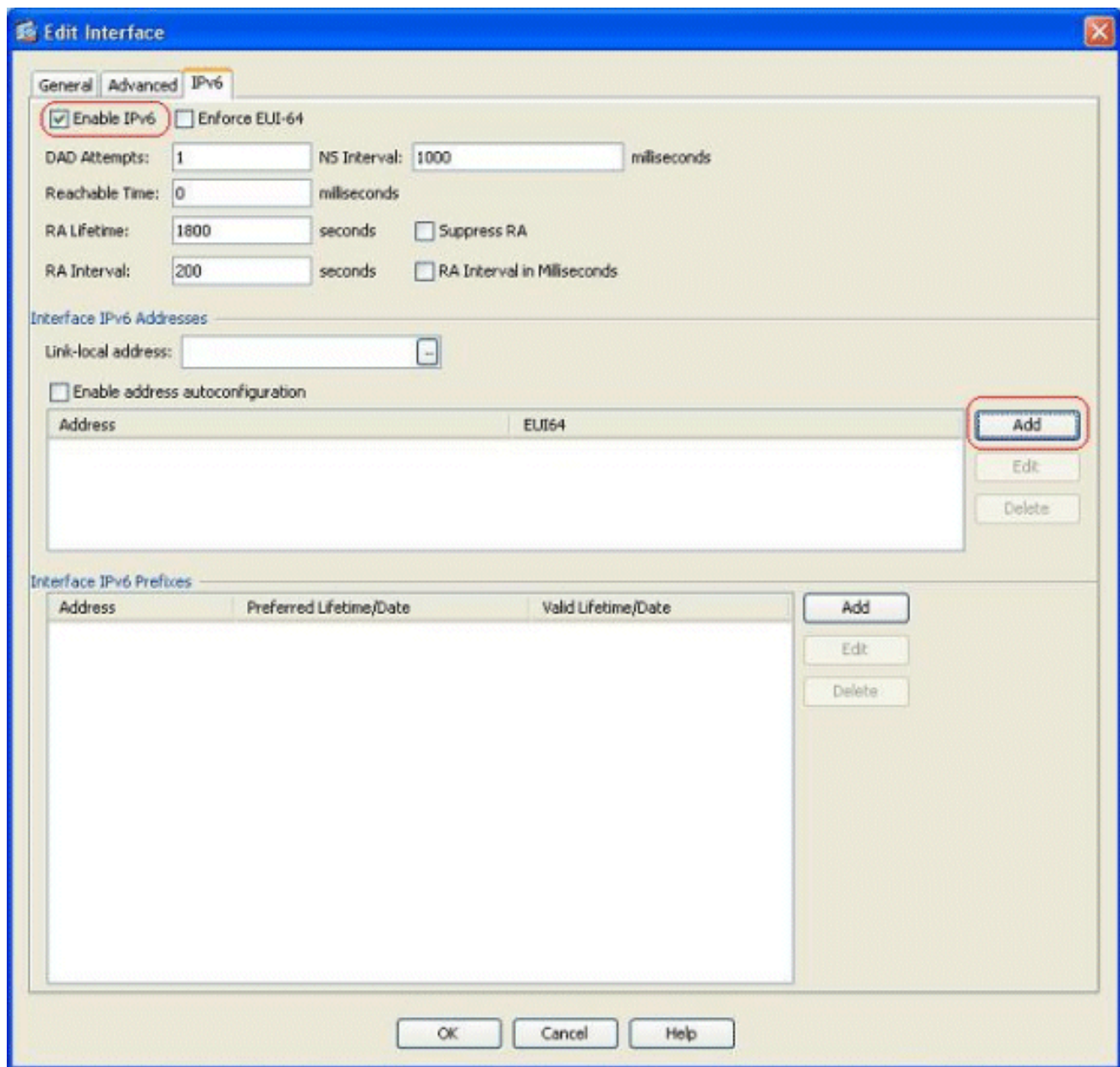
1. [必要なインターフェイスの IPv6 を有効にして下さい。](#)
2. [IPv6 access-list を必要なところに定義して下さい。](#)
3. [IPv6 ルート情報を規定して下さい。](#)

設定

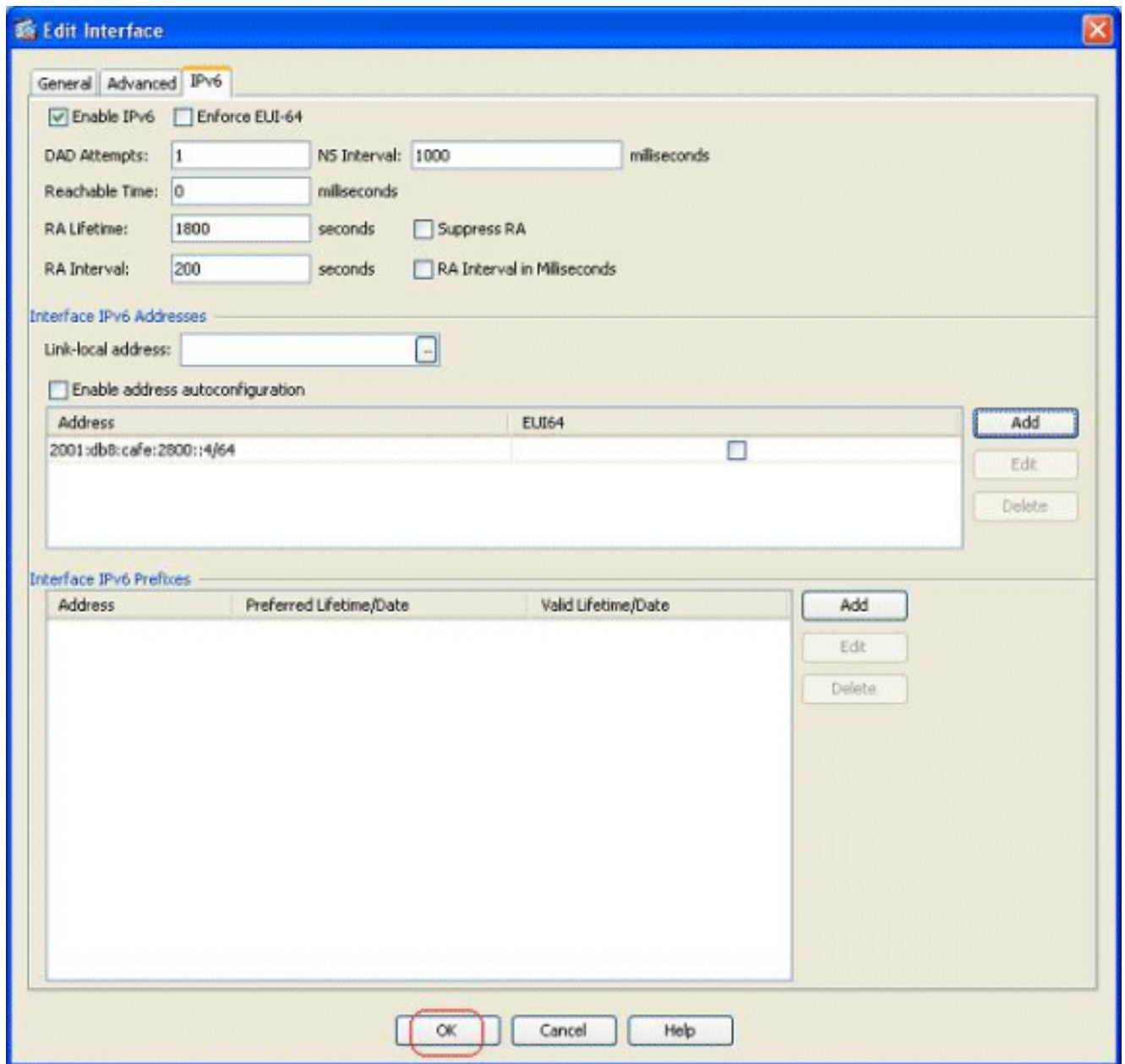
これらの詳細なステップを完了して下さい。

[必要なインターフェイスの IPv6 を有効にして下さい](#)

1. >デバイス セットアップ> インターフェイス 『Configuration』 を選択し、必要なインターフェイスを選択し、『Edit』 をクリックして下さい。
2. 関連 IPv6 設定を規定するために IPv6 タブをクリックして下さい。
3. イネーブル IPv6 オプションを選択し、そしてインターフェイス IPv6 アドレス セクションで 『Add』 をクリックして下さい。



4. [OK] をクリックします。
5. インターフェイス ペインに戻るために『OK』 をクリックして下さい。



IPv6 access-list を必要なところに定義して下さい

1. >ファイアウォール>アクセス規則『Configuration』を選択し、追加 IPv6 アクセス規則オプションを選択するために追加ダウン ボタンをクリックして下さい。New ウィンドウは現われます

Add IPv6 Access Rule

Interface:

Action: Permit Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

More Options

OK Cancel Help

- 『OK』 をクリックした、追加ドロップダウン メニューから別のアクセス規則オプションを追加するために後『Insert』 をクリックして下さい。

Insert After Access Rule

Interface:

Action: Permit Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

More Options

OK Cancel Help

- [OK] をクリックします。設定されたアクセス ルールはここに見られる場合があります
:

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 checked="" type="checkbox"/>	any	any	ip	Deny				Implicit rule

4. IPv6 アクセス規則オプションだけ選択して下さい。

IPv6 ルート情報を規定して下さい

1. >デバイスセットアップ>ルーティング>スタティック・ルート『Configuration』を選択し、ルートを追加するために『Add』をクリックして下さい。
2. スタティック・ルートペインに戻るために『OK』をクリックして下さい。

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.

3. 設定されたルートしか表示しないために IPv6 ルーティングを選択して下さい。

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:2800...	1	None

ASA が IPv6 パケットをルーティングすることができるようにこれが必要な基本設定を完了します。

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

関連情報

- [ASA の設定例およびテクニカル ノート](#)
- [IPv6 当たることの設定](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)