

ASA 8.x : Configuration de base d'IPv6 sur l'ASA utilisant l'exemple de configuration ASDM

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurez](#)

[IPv6 d'enable sur l'interface requise](#)

[Définissez les Listes d'accès d'IPv6 si nécessaire](#)

[Spécifiez les informations d'ipv6 route](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit une configuration de base cet IPv6 d'enable sur l'appliance de sécurité adaptable Cisco (ASA) afin de passer les paquets d'IPv6. Cette configuration est affichée utilisant Adaptive Security Device Manager (ASDM). Le support sur Cisco ASA pour les paquets d'IPv6 est fourni par la version de logiciel de Cisco ASA 7.0(1) elle-même. Cependant, le support à configurer par l'ASDM est fourni par la version de logiciel 6.2 de Cisco ASDM en avant.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco ASA avec la version 8.2
- Cisco ASDM avec la version 6.3

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont

démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

[Conventions](#)

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

[Informations générales](#)

Afin de passer les paquets d'IPv6 par l'ASA, terminez-vous ces étapes de haut niveau :

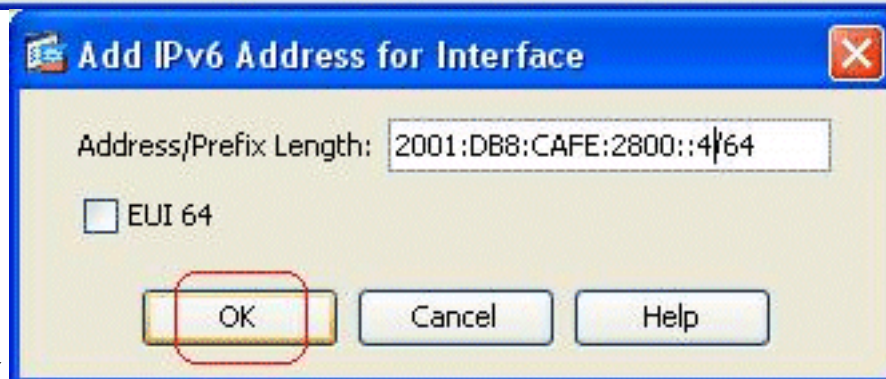
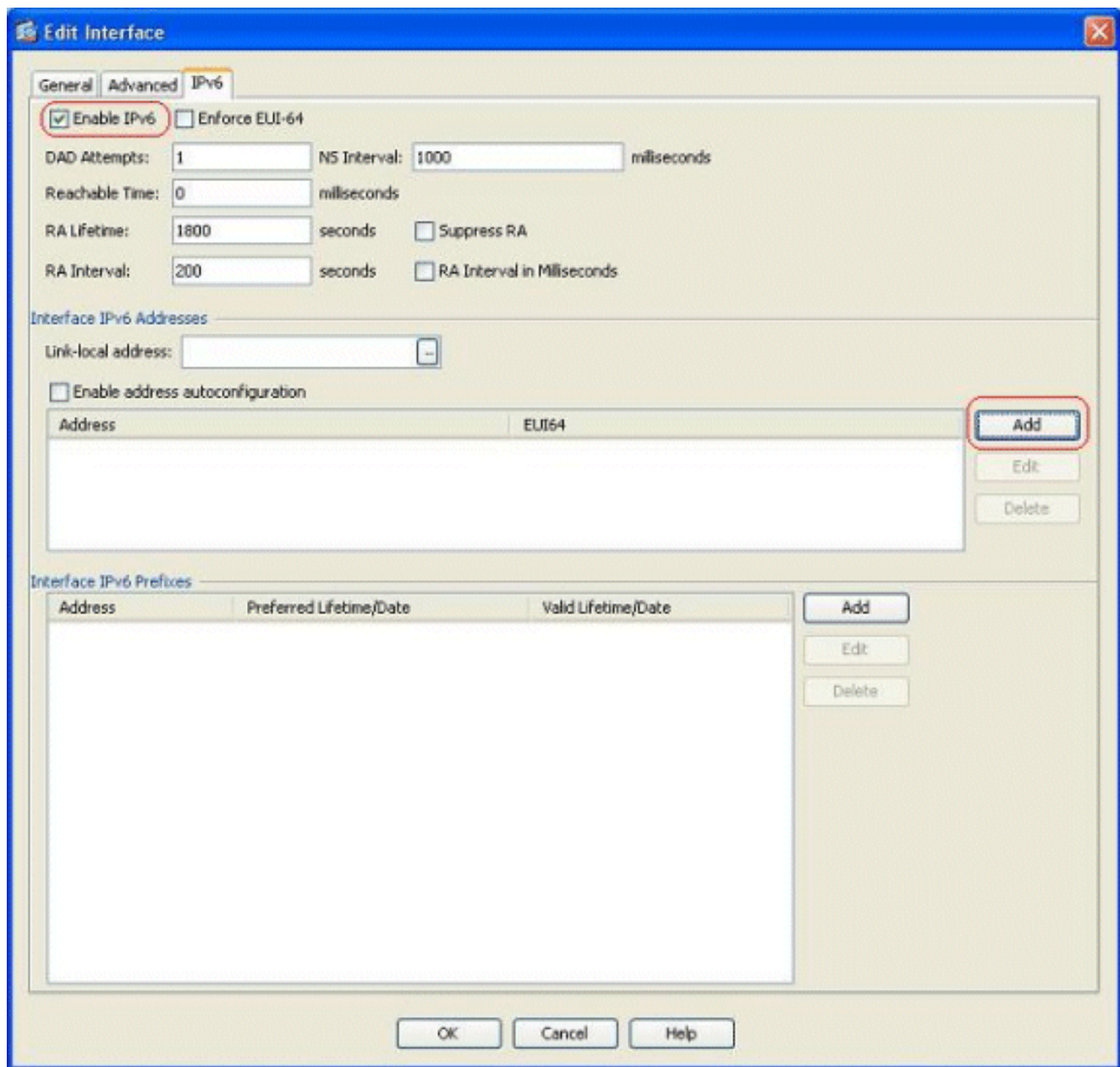
1. [IPv6 d'enable sur les interfaces requises](#).
2. [Définissez les Listes d'accès d'IPv6 si nécessaire](#).
3. [Spécifiez les informations d'ipv6 route](#).

[Configurez](#)

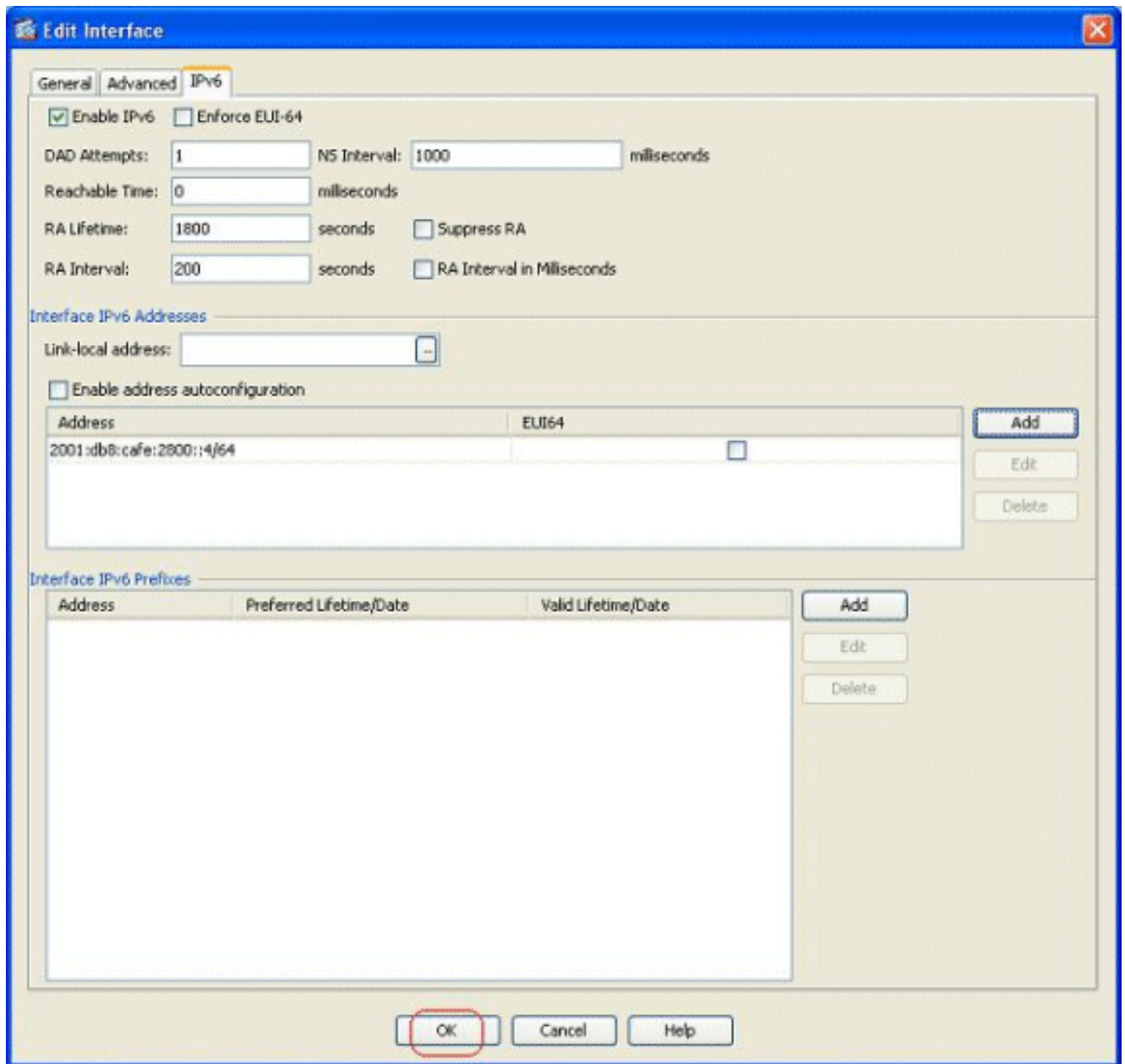
Terminez-vous ces étapes détaillées.

[IPv6 d'enable sur l'interface requise](#)

1. Choisissez la **configuration** > l'**installation de périphérique** > l'**interface**, sélectionnez l'interface requise, et cliquez sur Edit.
2. Cliquez sur l'onglet d'**IPv6** afin de spécifier les configurations relatives d'IPv6.
3. Choisissez l'option d'**IPv6 d'enable**, puis cliquez sur Add dans la section d'adresses d'IPv6 d'interface.



4. Cliquez sur **OK**.
5. Cliquez sur **OK** afin de revenir au volet d'interfaces.



Définissez les Listes d'accès d'IPv6 si nécessaire

1. Choisissez la **configuration** > le **Pare-feu** > les **règles d'accès**, et cliquez sur en fonction le bouton de déroulant d'**ajouter** afin de sélectionner l'option de **règle d'accès d'IPv6 d'ajouter**. Une nouvelle fenêtre apparaît

Add IPv6 Access Rule

Interface:

Action: Permit Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

More Options

2. Cliquez sur OK, et cliquez sur l'insertion après qu'afin d'ajouter une autre option de règle d'accès du menu déroulant d'ajouter.

Insert After Access Rule

Interface:

Action: Permit Deny

Source:

Destination:

Service:

Description:

Enable Logging

Logging Level:

More Options

3. Cliquez sur OK. Les règles d'accès configurées peuvent être vues ici

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. Choisissez l'option de règles d'accès d'IPv6 seulement.

Spécifiez les informations d'ipv6 route

1. Choisissez la configuration > l'installation de périphérique > le routage > les artères statiques, et cliquez sur Add afin d'ajouter une artère.
2. Cliquez sur OK afin de revenir au volet statique

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.

d'artères.

3. Choisissez les artères d'IPv6 afin de visualiser seulement l'artère configurée.



Ceci conclut la configuration de base exigée pour que l'ASA conduise les paquets d'IPv6.

Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

Informations connexes

- [Exemples et TechNotes de configuration ASA](#)
- [Configurer l'adressage d'IPv6](#)
- [Support et documentation techniques - Cisco Systems](#)