

# ASDM 6.4 : Exemple de configuration d'un tunnel VPN site à site avec IKEv2

## Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Configurer](#)

[Diagramme du réseau](#)

[Configuration ASDM sur HQ-ASA](#)

[Vérifier](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

## Introduction

Ce document décrit comment configurer un tunnel VPN de site à site entre deux dispositifs de sécurité adaptable Cisco (ASA) utilisant la version 2 d'échange de clés Internet (IKE). Il décrit les étapes utilisées pour configurer le tunnel VPN utilisant un assistant d'interface utilisateur d'Adaptive Security Device Manager (ASDM).

## Conditions préalables

### Exigences

Assurez-vous que Cisco ASA a été configuré avec les [paramètres](#) de [base](#).

### Composants utilisés

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

- Appareils de sécurité adaptatifs de la gamme Cisco ASA 5500 exécutant le logiciel version 8.4 et ultérieure
- Logiciel Cisco ASDM versions 6.4 et ultérieures

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

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

## Informations générales

IKEv2, est une amélioration du protocole IKEv1 existant qui inclut les avantages suivants :

- Moins d'échanges de messages entre homologues IKE
- Méthodes d'authentification unidirectionnelle
- Prise en charge intégrée de Dead Peer Detection (DPD) et NAT-Traversal
- Utilisation du protocole EAP (Extensible Authentication Protocol) pour l'authentification
- Élimine le risque d'attaques DoS simples en utilisant des cookies anti-colmatage

## Configurer

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Utilisez l'outil de recherche de commandes (clients enregistrés seulement) pour en savoir plus sur les commandes employées dans cette section.

## Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ce document montre la configuration du tunnel VPN site à site sur HQ-ASA. La même chose pourrait être suivie comme un miroir sur le BQ-ASA.

## Configuration ASDM sur HQ-ASA

Ce tunnel VPN peut être configuré à l'aide d'un assistant d'interface utilisateur graphique facile à utiliser.

Procédez comme suit :

1. Connectez-vous à l'ASDM et accédez à Wizards > VPN Wizards > Site-to-site VPN Wizard.
2. Une fenêtre de configuration de connexion VPN de site à site s'affiche. Cliquez sur Next

(Suivant).

3. Spécifiez l'adresse IP de l'homologue et l'interface d'accès VPN. Cliquez sur Next (Suivant).
4. Sélectionnez les deux versions IKE, puis cliquez sur Next.

Remarque : les deux versions d'IKE sont configurées ici, car l'initiateur peut avoir une sauvegarde d'IKEv2 vers IKEv1 en cas de défaillance d'IKEv2.

5. Spécifiez le réseau local et le réseau distant de sorte que le trafic entre ces réseaux soit chiffré et passé par le tunnel VPN. Cliquez sur Next (Suivant).
6. Spécifiez les clés prépartagées pour les deux versions d'IKE.

La principale différence entre les versions 1 et 2 d'IKE réside dans la méthode d'authentification qu'elles autorisent. IKEv1 n'autorise qu'un seul type d'authentification aux deux extrémités VPN (c'est-à-dire, clé pré-partagée ou certificat). Cependant, IKEv2 permet de configurer des méthodes d'authentification asymétriques (c'est-à-dire une authentification par clé pré-partagée pour l'émetteur, mais une authentification par certificat pour le répondeur) à l'aide d'interfaces de ligne de commande d'authentification locales et distantes distinctes.

En outre, vous pouvez avoir différentes clés pré-partagées aux deux extrémités. La clé pré-partagée locale du côté HQ-ASA devient la clé pré-partagée distante du côté BQ-ASA. De même, la clé pré-partagée distante du côté HQ-ASA devient la clé pré-partagée locale du côté BQ-ASA.

7. Spécifiez les algorithmes de chiffrement pour les versions 1 et 2 d'IKE. Ici, les valeurs par défaut sont acceptées :
8. Cliquez sur Manage... afin de modifier la stratégie IKE.

Remarque :

- La stratégie IKE dans IKEv2 est synonyme de la stratégie ISAKMP dans IKEv1.
- La proposition IPsec dans IKEv2 est synonyme du jeu de transformation dans IKEv1.

9. Ce message s'affiche lorsque vous essayez de modifier la stratégie existante :

Cliquez sur OK afin de continuer.

10. Sélectionnez la stratégie IKE spécifiée, puis cliquez sur Edit.
11. Vous pouvez modifier les paramètres tels que Priorité, Chiffrement, Groupe D-H, Hachage d'intégrité, Hachage PRF et Valeurs de durée de vie. Cliquez sur OK lorsque vous avez terminé.

IKEv2 permet de négocier l'algorithme Integrity séparément de l'algorithme PRF (fonction pseudo-aléatoire). Cela peut être configuré dans la stratégie IKE avec les options

disponibles actuelles SHA-1 ou MD5.

Vous ne pouvez pas modifier les paramètres de proposition IPsec définis par défaut. Cliquez sur Select à côté du champ IPsec Proposal afin d'ajouter de nouveaux paramètres. La principale différence entre IKEv1 et IKEv2, en termes de propositions IPsec, est que IKEv1 accepte l'ensemble de transformation en termes de combinaisons d'algorithmes de chiffrement et d'authentification. IKEv2 accepte les paramètres de cryptage et d'intégrité individuellement, et effectue enfin toutes les combinaisons OU possibles de ces paramètres. Vous pouvez les afficher à la fin de cet Assistant, dans la diapositive Résumé.

12. Cliquez sur Next (Suivant).

13. Spécifiez les détails, tels que l'exemption NAT, PFS et le contournement de l'ACL d'interface. Sélectionnez Suivant.

14. Un résumé de la configuration est disponible ici :

Cliquez sur Finish afin de terminer l'assistant de tunnel VPN de site à site. Un nouveau profil de connexion est créé avec les paramètres configurés.

## Vérifier

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

- [show crypto ikev2 sa](#) - Affiche la base de données SA d'exécution IKEv2.
- [show vpn-sessiondb detail I2I](#) - Affiche les informations sur les sessions VPN site à site.

## Dépannage

### Dépannage des commandes

L'[Outil Interpréteur de sortie \(clients enregistrés uniquement\) \(OIT\) prend en charge certaines commandes show](#). Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .

Remarque : Consulter les [renseignements importants sur les commandes de débogage](#) avant d'utiliser les commandes de débogage.

- [debug crypto ikev2](#) - Affiche les messages de débogage pour IKEv2.

## Informations connexes

- [Assistance technique pour les appareils Cisco ASA 5500](#)
- [Assistance et documentation techniques - Cisco Systems](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.