ASDM 6.4 : Tunnel VPN de site à site avec l'exemple de la configuration IKEv2

Contenu

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

Conditions requises

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 :

- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 exécutant la version de logiciel 8.4 et plus tard
- Version de logiciel 6.4 de Cisco ASDM et plus tard

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

IKEv2, est une amélioration au protocole IKEv1 existant qui inclut ces avantages :

- Moins échanges de message entre les pairs d'IKE
- Méthodes d'authentification unidirectionnelle
- Prise en charge intégrée pour Dead Peer Detection (DPD) et le NAT-Traversal
- Utilisation de Protocole EAP (Extensible Authentication Protocol) pour l'authentification
- Élimine le risque d'attaques DoS simples utilisant les Témoins anticolmatants

Configurez

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

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Ce document affiche la configuration du tunnel VPN de site à site sur HQ-ASA. Les mêmes ont pu être suivis comme miroir sur le BQ-ASA.

Configuration ASDM sur HQ-ASA

Ce tunnel VPN a pu être configuré utilisant un assistant facile à utiliser GUI.

Procédez comme suit :

1. Ouvrez une session à l'ASDM, et allez aux **assistants** > aux **assistants VPN** > à l'**assistant du site à site VPN**.
2. Une fenêtre d'installation de connexion VPN de site à site apparaît. Cliquez sur **Next** (Suivant).
3. Spécifiez l'interface d'adresse IP et d'accès VPN de pair. Cliquez sur **Next** (Suivant).
4. Sélectionnez les deux versions d'IKE, et cliquez sur Next.**Remarque:** Les deux versions d'IKE sont configurées ici parce que le demandeur pourrait avoir une sauvegarde d'IKEv2 à IKEv1 quand IKEv2 échoue.

5. Spécifiez le réseau local et le réseau distant de sorte que le trafic entre ces réseaux soient chiffrés et avez traversé le tunnel VPN. Cliquez sur **Next** (Suivant).
6. Spécifiez les clés pré-partagées pour les deux versions d'IKE.La difference majeure entre les versions 1 et 2 d'IKE se trouve en termes de méthode d'authentification qu'ils permettent. IKEv1 permet seulement un type d'authentification aux deux extrémités VPN (c'est-à-dire, l'un ou l'autre de clé ou de certificat pré-partagée). Cependant, IKEv2 permet des méthodes d'authentification asymétriques à configurer (c'est-à-dire, authentification de pre-shared-key pour le créateur, mais authentification de certificat pour le responder) utilisant les gens du pays distincts et l'authentification à distance CLIs.De plus, vous pouvez avoir différentes clés pré-partagées aux deux extrémités. La clé pré-partagée locale à l'extrémité HQ-ASA devient la clé pré-partagée distante à l'extrémité BQ-ASA. De même, la clé pré-partagée distante à l'extrémité HQ-ASA devient la clé pré-partagée locale à l'extrémité BQ-ASA.
7. Spécifiez les algorithmes de chiffrement pour les deux versions 1 et 2 d'IKE. Ici, les valeurs par défaut sont reçues :
8. Le clic **parviennent…** afin de modifier la stratégie IKE.**Remarque: La stratégie IKE** dans IKEv2 est synonyme à la **stratégie ISAKMP** dans IKEv1.**La proposition d'IPsec** dans IKEv2 est synonyme au **jeu de transformations** dans IKEv1.
9. Ce message apparaît quand vous essayez de modifier la stratégie existante :Cliquez sur OK afin de poursuivre.
10. Sélectionnez la stratégie IKE spécifiée, et cliquez sur Edit.
11. Vous pouvez modifier les paramètres des valeurs tels que la priorité, le cryptage, le groupe de D-H, les informations parasites d'intégrité, PRF informations parasites, et vie. Cliquez sur OK une fois terminé.IKEv2 tient compte pour que l'algorithme d'intégrité soit négocié séparément du pseudo algorithme aléatoire de la fonction (PRF). Ceci a pu être configuré dans la stratégie IKE avec des options disponibles en cours étant SHA-1 ou MD5.Vous ne pouvez pas modifier les paramètres de proposition d'IPsec qui sont définis par défaut. Clic **choisi** à côté du champ de proposition d'IPsec afin d'ajouter de nouveaux paramètres. La difference majeure entre IKEv1 et IKEv2, en termes de propositions d'IPsec, est qu'IKEv1 reçoit le jeu de transformations en termes de combinaisons des algorithmes de cryptage et d'authentification. IKEv2 reçoit les paramètres de cryptage et d'intégrité individuellement, et fait finalement tout le possible OU combinaisons de ces derniers. Vous pourriez visualiser ces derniers à l'extrémité de cet assistant, dans la glissière récapitulative.
12. Cliquez sur **Next** (Suivant).
13. Spécifiez les détails, sauter tels que le nat exemption, le PFS, et d'interface ACL. Choisissez **ensuite**.
14. Un résumé de la configuration peut être vu ici :Cliquez sur Finish afin de se terminer l'assistant de tunnel VPN de site à site. Un nouveau profil de connexion est créé avec les paramètres configurés.

Vérifiez

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** .

- **affichez cryptos ikev2 SA** - Affiche la base de données d'exécution SA IKEv2.

- affichez le détail l2l de VPN-sessiondb - Affiche les informations sur des sessions VPN de site à site.

Dépannez

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: Référez-vous aux informations importantes sur les commandes de débogage avant d'utiliser les commandes de **débogage**.

- debug crypto ikev2 - Affiche des **messages de débogage** pour IKEv2.

Informations connexes

- Soutien technique d'appareils de gamme de Cisco ASA 5500
- Support et documentation techniques - Cisco Systems