Configuration de cartes Crypto basées sur des noms de domaine pour le contrôle d'accès de périphérique VPN

Contenu

Introduction

Ce document décrit comment configurer les crypto map basés sur de nom unique (DN) pour fournir le contrôle d'accès de sorte qu'un périphérique VPN puisse établir des tunnels VPN avec un routeur de Cisco IOS®. Dans l'exemple de ce document, la signature de Rivest, de Shamir, et d'Adelman (RSA) est la méthode pour l'authentification d'IKE. En plus de la validation standard de certificat, de l'essai basé sur dn de crypto map pour apparier l'identité de l'ISAKMP du pair avec certains champs dans ses Certificats, tels que le nom unique X.500 ou le nom de domaine complet (FQDN).

Conditions préalables

Conditions requises

Cette caractéristique a été introduite la première fois dans le Logiciel Cisco IOS version 12.2(4)T. Vous devez cette release ou plus tard pour cette configuration.

La version du logiciel Cisco IOS 12.3(5) a été également testée. Cependant, le DN a basé des crypto map a manqué en raison de l'ID de bogue Cisco CSCed45783 (clients enregistrés seulement).

Composants utilisés

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

- Routeurs de Cisco 7200
- Logiciel Cisco IOS version 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

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 aux Conventions relatives aux conseils techniques Cisco.

Informations générales

Précédemment, pendant l'authentification d'IKE suivre la méthode de signature RSA, et après la validation de certification et le Liste des révocations de certificat (CRL) facultatif vérifiant, le Cisco IOS a continué la négociation rapide de mode d'IKE. Il n'a pas fourni une méthode pour empêcher les périphériques de VPN distant de ne communiquer avec aucune interface chiffrée, autre que des restrictions sur l'adresse IP du pair chiffrant.

Maintenant avec le crypto map basé sur dn, le Cisco IOS peut limiter les homologues VPN distants pour accéder à seulement des interfaces sélectionnées avec les Certificats spécifiques. En particulier, Certificats avec certains dn ou FQDN.

Configurez

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

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.

Configurations

Ce document utilise les configurations indiquées ici.

Dans cet exemple, une configuration réseau simple est utilisée pour expliquer la caractéristique. Le routeur de SJhub a deux certificats d'identité, on de confient à l'Autorité de certification (CA) et l'autre de Microsoft CA. Voyez les informations relatives