

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

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Informations connexes](#)

[Introduction](#)

Ce document décrit comment configurer des crypto-cartes basées sur un nom distinctif (DN) pour fournir un contrôle d'accès afin qu'un périphérique VPN puisse établir des tunnels VPN avec un routeur Cisco IOS®. Dans l'exemple de ce document, la signature Rivest, Shamir et Adelman (RSA) est la méthode d'authentification IKE. En plus de la validation de certificat standard, les cartes de chiffrement basées sur DN tentent de faire correspondre l'identité ISAKMP de l'homologue à certains champs de ses certificats, tels que le nom unique X.500 ou le nom de domaine complet (FQDN).

[Conditions préalables](#)

[Conditions requises](#)

Cette fonctionnalité a été introduite pour la première fois dans le logiciel Cisco IOS Version 12.2(4)T. Vous devez utiliser cette version ou une version ultérieure pour cette configuration.

Le logiciel Cisco IOS version 12.3(5) a également été testé. Cependant, les cartes de chiffrement basées sur DN ont échoué en raison de l'ID de bogue Cisco [CSCed45783](#) (clients [enregistrés](#) uniquement).

[Components Used](#)

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

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

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 des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

[Informations générales](#)

Auparavant, lors de l'authentification IKE à l'aide de la méthode de signature RSA, après validation de la certification et vérification facultative de la liste de révocation de certificats (CRL), Cisco IOS a poursuivi la négociation IKE Quick Mode. Il n'a pas fourni de méthode pour empêcher les périphériques VPN distants de communiquer avec des interfaces cryptées, autre que des restrictions sur l'adresse IP de l'homologue de chiffrement.

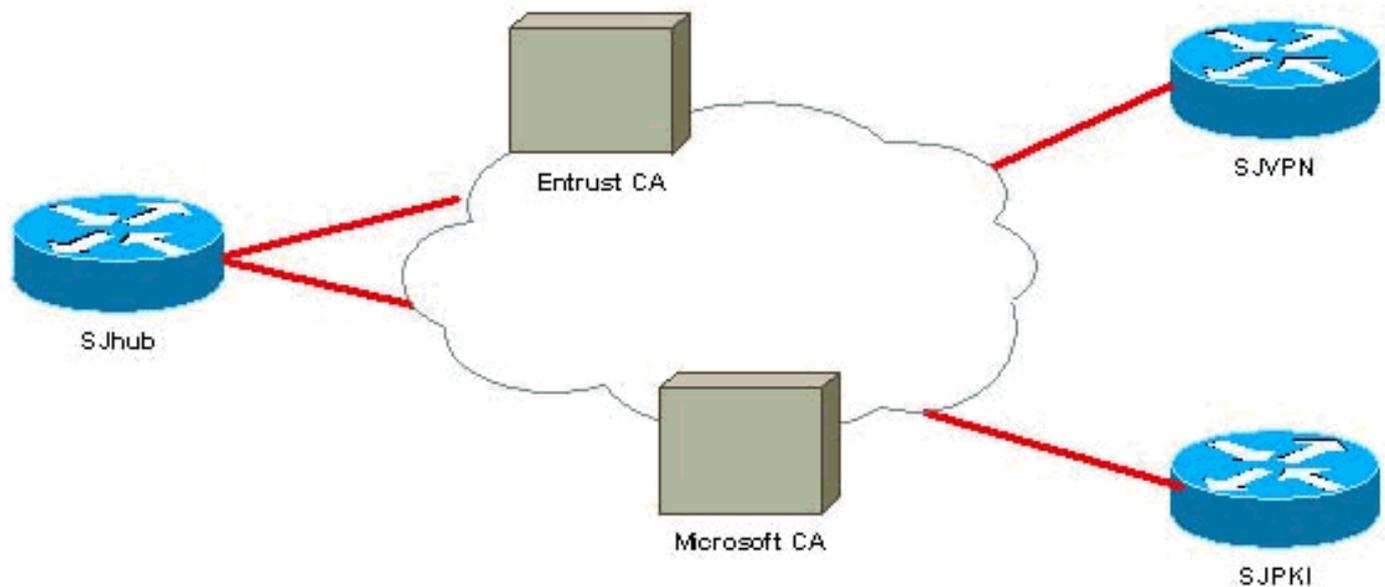
Maintenant avec la carte de chiffrement basée sur DN, Cisco IOS peut restreindre les homologues VPN distants à accéder uniquement à certaines interfaces avec des certificats spécifiques. En particulier, les certificats avec certains DN ou FQDN.

[Configuration](#)

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 démontrer la fonctionnalité. Le routeur SJhub possède deux certificats d'identité, l'un de l'autorité de certification Entrust et l'autre de l'autorité de certification Microsoft. Voir les [informations connexes](#)