Configuración de mapas de encripción basados en DN para el control de acceso al dispositivo VPN

Contenido

Introducción

Este documento describe cómo configurar los mapas de encripción basados en Nombres distinguidos (DN) con el objeto de proporcionar control de acceso de modo que un dispositivo VPN pueda establecer túneles VPN con un router del IOS® de Cisco. En el ejemplo de este documento, la firma Rivest, Shamir y Adelman (RSA) es el método para la autenticación IKE. Además de la validación de certificados estándar, los mapas de criptografía basados en DN intentan hacer coincidir la identidad ISAKMP del par con ciertos campos de sus certificados, como el nombre distintivo X.500 o el nombre del dominio aprobado (FQDN).

prerrequisitos

Requisitos

Esta característica primero fue introducida en el Cisco IOS Software Release 12.2(4)T. Usted debe esta versión o más adelante para esta configuración.

El Cisco IOS Software Release 12.3(5) también fue probado. Sin embargo, el DN basó fallada las correspondencias de criptografía debido al Id. de bug Cisco CSCed45783 (clientes registrados solamente).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Routers Cisco 7200
- Versión de software del IOS de Cisco 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Previamente, durante la autenticación IKE usando el método de firma RSA, y después de la validación de la certificación y del Listas de revocación de certificados (CRL) opcional que marcaban, el Cisco IOS continuó la negociación del Quick Mode IKE. No proporcionó un método para evitar que los dispositivos VPN remotos comuniquen con ninguna interfaces encriptadas, con excepción de las restricciones en la dirección IP del par que cifraba.

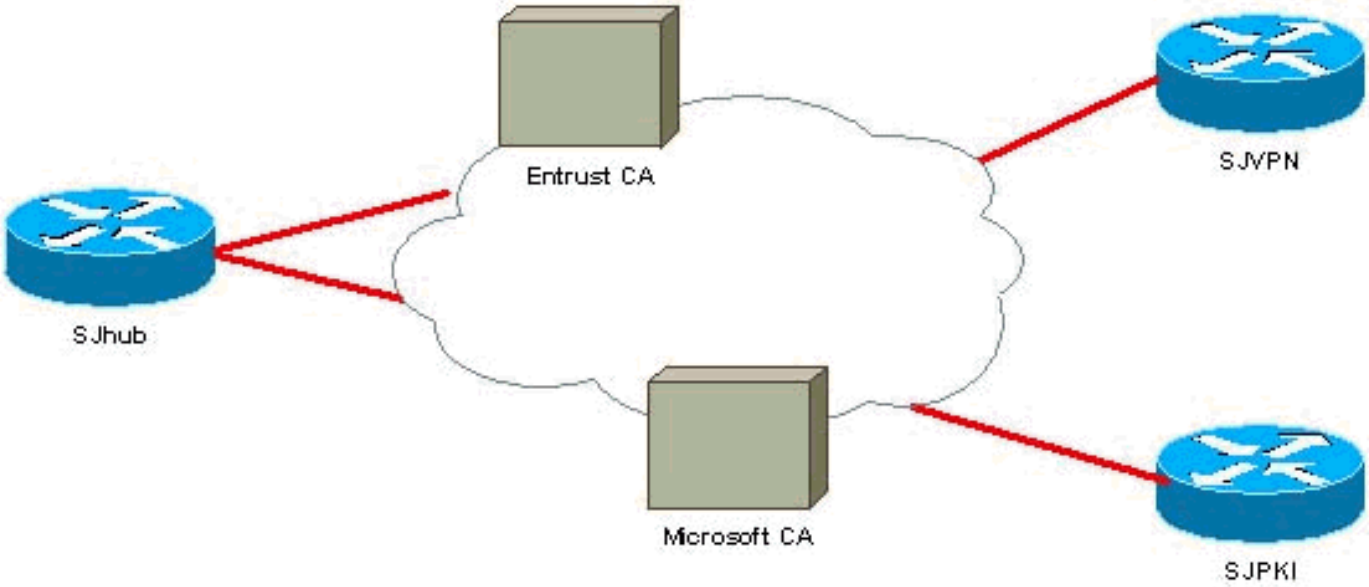
Ahora con correspondencia de criptografía basada en DN, el Cisco IOS puede restringir a los pares remotos VPN para acceder solamente las interfaces seleccionadas con los Certificados específicos. Particularmente, Certificados con ciertos DN o FQDN.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuraciones

Este documento usa las configuraciones detalladas aquí.

En este ejemplo, una configuración de la red simple se utiliza para demostrar la característica. El router SJhub tiene dos certificados de identidad, uno de la autoridad certificadora Entrust (CA) y otro de Microsoft CA. Vea la información relacionada