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).

Prerequisites

Requirements

Esta función se introdujo por primera vez en Cisco IOS Software Release 12.2(4)T. Debe utilizar esta versión o una posterior para esta configuración.

También se probó el software Cisco IOS versión 12.3(5). Sin embargo, los mapas criptográficos basados en DN fallaron debido al ID de bug Cisco CSCed45783 (sólo clientes registrados) .

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). If your network is live, make sure that you understand the potential impact of any command.

Convenciones

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

Antecedentes

Anteriormente, durante la autenticación IKE mediante el método de firma RSA, y después de la validación de la certificación y la comprobación de la lista de revocación de certificados (CRL) opcional, Cisco IOS continuó con la negociación de modo rápido IKE. No proporcionó un método para evitar que los dispositivos VPN remotos se comunicaran con ninguna interfaz cifrada, aparte de las restricciones en la dirección IP del par de cifrado.

Ahora, con el mapa criptográfico basado en DN, el IOS de Cisco puede restringir a los pares VPN remotos para que solo accedan a las interfaces seleccionadas con certificados específicos. En particular, los 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, se utiliza una configuración de red simple para demostrar la función. El router SJhub tiene dos certificados de identidad, uno de la autoridad certificadora Entrust (CA) y otro de Microsoft CA. Consulte Información relacionada.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).