Configuring DN-Based Crypto Maps for VPN Device Access Control

Contents

Introduction

Este documento descreve como configurar mapas de criptografia com base em Nomes distintos (DN) para fornecer controle de acesso, de modo que um dispositivo VPN possa estabelecer túneis VPN com um roteador Cisco IOS®. No exemplo deste documento, a assinatura Rivest, Shamir e Adelman (RSA) é o método de autenticação IKE. Além da validação de certificado padrão, os mapas de criptografia baseados em DN tentam fazer a correspondência da identidade de ISAKMP do peer com determinados campos em seus certificados, tais como o nome distinto do X.500 ou o nome de domínio completo (FQDN).

Prerequisites

Requirements

Este recurso foi introduzido pela primeira vez no Cisco IOS Software Release 12.2(4)T. Esta versão ou posterior deve ser usada para esta configuração.

O Cisco IOS Software Release 12.3(5) também foi testado. No entanto, os mapas de criptografia baseados em DN falharam devido à ID de bug da Cisco CSCed45783 (somente clientes registrados) .

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 7200 routers
- Versão do software Cisco IOS 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

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

Anteriormente, durante a autenticação IKE usando o método de assinatura RSA e após a validação da certificação e a verificação opcional de lista de revogação de certificados (CRL), o Cisco IOS continuou a negociação do modo rápido IKE. Ele não forneceu um método para impedir que os dispositivos VPN remotos se comuniquem com quaisquer interfaces criptografadas, além das restrições no endereço IP do peer de criptografia.

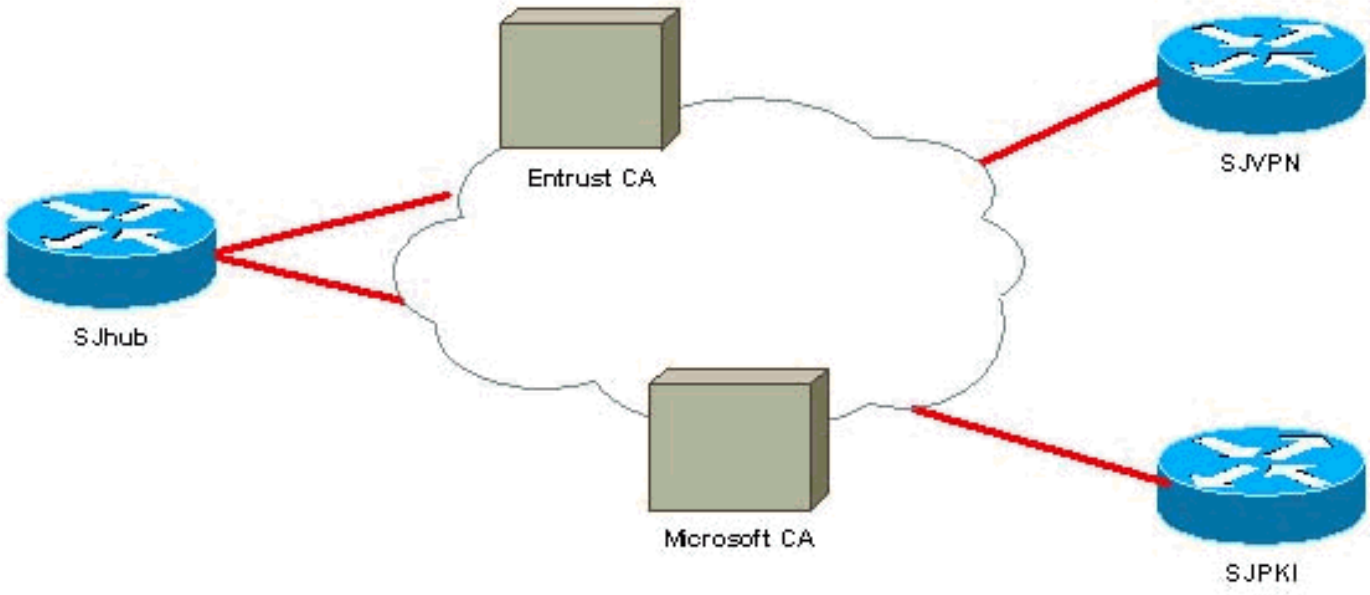
Agora com o mapa de criptografia baseado em DN, o Cisco IOS pode restringir os peers de VPN remotos para acessar apenas interfaces selecionadas com certificados específicos. Em particular, certificados com determinados DNs ou FQDNs.

Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Diagrama de Rede

Este documento utiliza a configuração de rede mostrada neste diagrama.



Configurações

Este documento utiliza as configurações mostradas aqui.

Neste exemplo, uma configuração de rede simples é usada para demonstrar o recurso. O roteador SJhub possui dois certificados de identidade, um da Autoridade de Certificação (CA) Entrust e outro da CA Microsoft. Consulte as informações relacionadas