Configuring DN-Based Crypto Maps for VPN Device Access Control

Índice

Introdução

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).

Pré-requisitos

Requisitos

Esta característica foi introduzida primeiramente no Cisco IOS Software Release 12.2(4)T. Você deve esta liberação ou mais tarde para esta configuração.

O Cisco IOS Software Release 12.3(5) foi testado igualmente. Contudo, o DN baseou falhado crypto map devido à identificação de bug Cisco CSCed45783 (clientes registrados somente).

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

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

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

Informações de Apoio

Previamente, durante a autenticação de IKE usando o método de assinatura de RSA, e após a validação de certificação e o Certificate Revocation List (CRL) opcional que verificam, o Cisco IOS continuou a negociação do Quick Mode IKE. Não forneceu um método para impedir que os dispositivos remotos VPN se comuniquem com nenhuma interfaces criptografada, a não ser limitações no endereço IP de Um ou Mais Servidores Cisco ICM NT do peer de criptografia.

Agora com mapa de criptografia com base em DN, o Cisco IOS pode restringir pares remotos VPN para alcançar somente interfaces selecionada com os Certificados específicos. Em particular, Certificados com determinados DN 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 instalação da rede simples é usada para demonstrar a característica. O roteador SJhub possui dois certificados de identidade, um da Autoridade de Certificação (CA) Entrust e outro da CA Microsoft. Veja a informação relacionada