configureren van DNA-gebaseerde encryptie-kaarten voor VPN-toegangscontrole

Inhoud

Inleiding

Dit document beschrijft hoe u op DNA gebaseerde crypto-kaarten (Naam) kunt configureren om toegangscontrole te bieden zodat een VPN-apparaat VPN-tunnels kan opzetten met een Cisco IOS® router. In het voorbeeld van dit document is de handtekening van Rivest, Shamir en Adelman (RSA) de methode voor de IKE-verificatie. Naast de standaardcertificatie proberen op DN gebaseerde crypto-kaarten de ISAKMP-identiteit van de peer te koppelen aan bepaalde velden in zijn certificaten, zoals de X.500-voornaam of de volledig gekwalificeerde domeinnaam (FQDN).

Voorwaarden

Vereisten

Deze optie is voor het eerst geïntroduceerd in Cisco IOS-softwarerelease 12.2(4)T. U moet deze ontspanner of later voor deze configuratie uitschakelen.

De Cisco IOS-softwarerelease 12.3(5)werd ook getest. De op DN gebaseerde crypto-kaarten zijn echter niet mislukt door Cisco bug-ID CSCed45783 (alleen geregistreerde klanten).

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco 7200 routers
- Cisco IOS-softwarerelease 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg voor meer informatie over documentconventies de technische Tips van Cisco.

Achtergrondinformatie

Eerder, tijdens IKE-verificatie met behulp van de RSA-kenmerkingsmethode, en na certificatie-validatie en optionele certificaat-herroeping list (CRL) controle, zette Cisco IOS de IKE Quick Mode-onderhandeling voort. Het bevatte geen methode om te voorkomen dat de externe VPN-apparaten met versleutelde interfaces kunnen communiceren, met uitzondering van beperkingen op het IP-adres van de versleuteling.

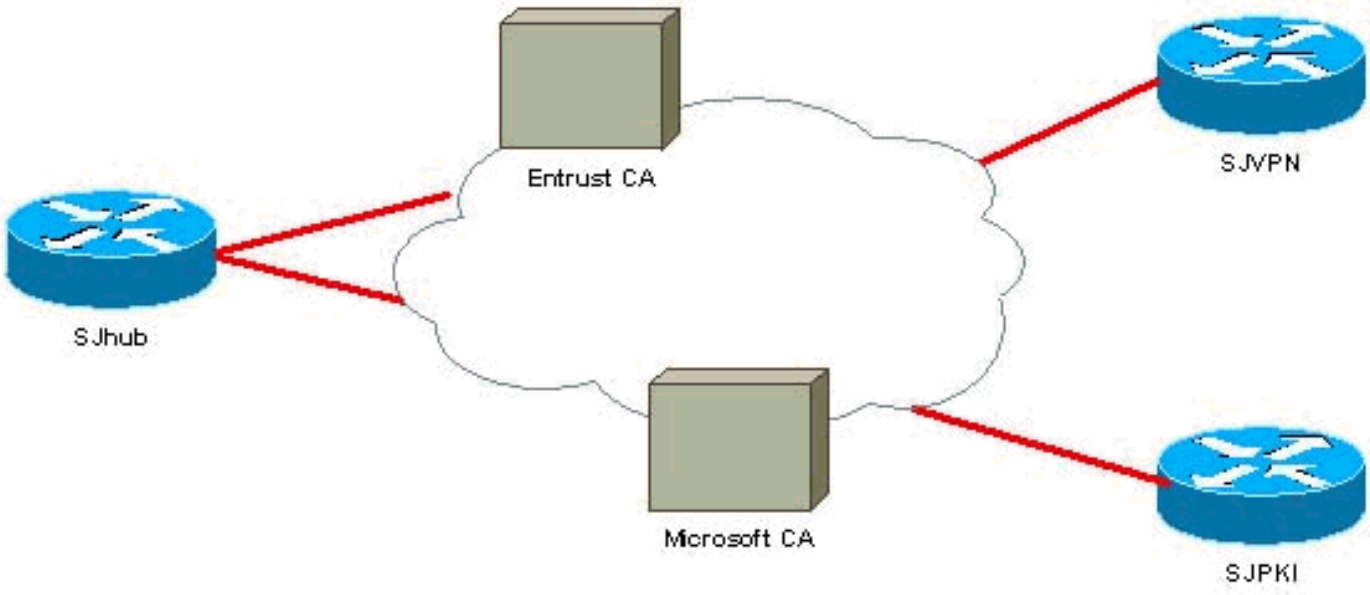
Nu met DNA-gebaseerde crypto map kan Cisco IOS externe VPN-peers beperken tot alleen geselecteerde interfaces met specifieke certificaten. Met name schuldbewijzen met bepaalde DNA's of FQDN's.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Netwerkdiagram

Dit document gebruikt de netwerkinstellingen die in dit diagram worden weergegeven.



Configuraties

Dit document gebruikt de configuraties die hier worden weergegeven.

In dit voorbeeld wordt een eenvoudige netwerkinstelling gebruikt om deze functie te demonstreren. De router van SJHub heeft twee identiteitscertificaten, één van de autoriteit van het Entrust certificaat (CA) en de andere van Microsoft CA. Zie de verwante informatie