Konfigurieren von DN-basierten Kryptozuordnungen für die VPN-Gerätezugriffskontrolle

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Sie DN-basierte Crypto Maps konfigurieren, um die Zugriffskontrolle zu ermöglichen, sodass ein VPN-Gerät VPN-Tunnel mit einem Cisco IOS®-Router einrichten kann. In dem Beispiel dieses Dokuments ist die Signatur Rivest, Shamir und Adelman (RSA) die Methode für die IKE-Authentifizierung. Neben der standardmäßigen Zertifikatsvalidierung versuchen DN-basierte Kryptozuordnungen, die ISAKMP-Identität des Peers mit bestimmten Feldern in den Zertifikaten des Peers abzustimmen, z. B. dem DN X.500 oder dem vollqualifizierten Domänennamen (FQDN).

Voraussetzungen

Anforderungen

Diese Funktion wurde erstmals in der Cisco IOS Software-Version 12.2(4)T eingeführt. Sie müssen diese Version oder höher für diese Konfiguration verwenden.

Die Cisco IOS Software Version 12.3(5) wurde ebenfalls getestet. Die DN-basierten Crypto Maps sind jedoch aufgrund der Cisco Bug ID CSCed45783 fehlgeschlagen (nur registrierte Kunden).

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco Router der Serie 7200
- Cisco IOS Softwareversion 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions.

Hintergrundinformationen

Bisher setzte Cisco IOS während der IKE-Authentifizierung mithilfe der RSA-Signaturmethode und nach der Überprüfung der Zertifizierungsprüfung und der optionalen CRL-Überprüfung (Certificate Revocation List) die IKE Quick Mode-Aushandlung fort. Sie bot keine Methode, um zu verhindern, dass die Remote-VPN-Geräte mit verschlüsselten Schnittstellen kommunizieren, mit Ausnahme der Einschränkungen für die IP-Adresse des verschlüsselnden Peers.

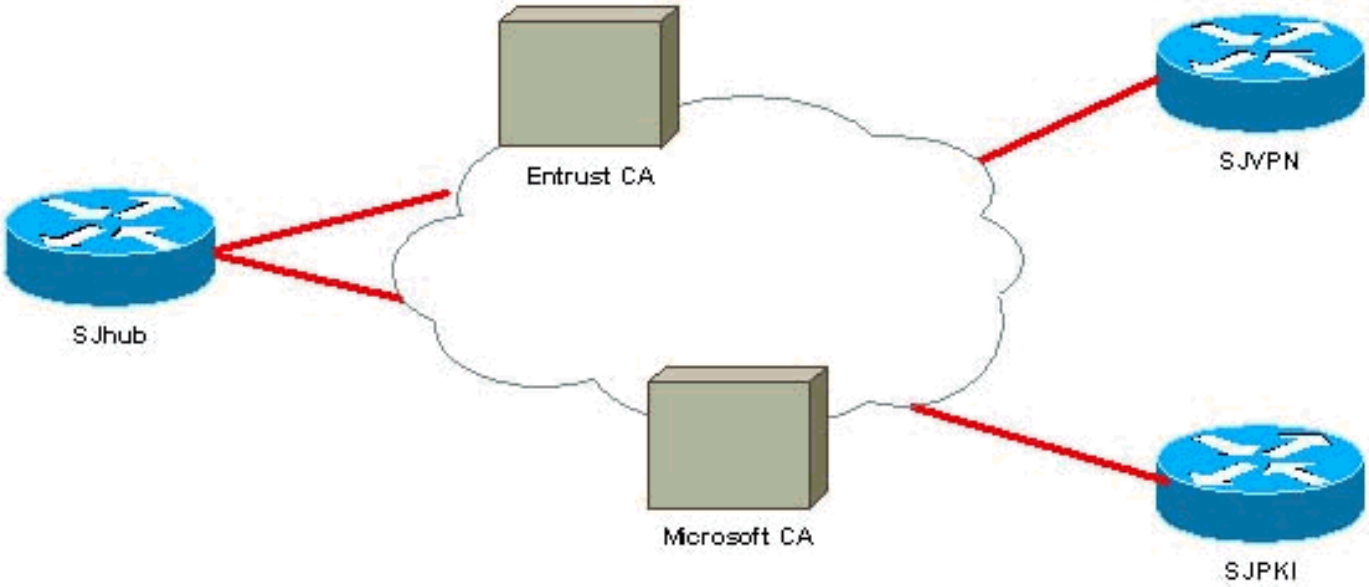
Mit der DN-basierten Crypto Map kann Cisco IOS die Remote-VPN-Peers auf den Zugriff auf ausgewählte Schnittstellen mit bestimmten Zertifikaten beschränken. Insbesondere Zertifikate mit bestimmten DNs oder FQDNs.

Konfiguration

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



Konfigurationen

In diesem Dokument werden die hier gezeigten Konfigurationen verwendet.

In diesem Beispiel wird eine einfache Netzwerkeinrichtung verwendet, um die Funktion zu veranschaulichen. Der SJ-Hub-Router verfügt über zwei Identitätszertifikate: eines von der Entrust Certificate Authority (CA) und das andere von der Microsoft CA. Weitere Informationen