VPN デバイス アクセス制御用の DN ベースの暗号化マップの設定

内容

概要

ここでは、VPN デバイスが Cisco IOS® ルータとの VPN トンネルを確立し、アクセス制御を提供する識別名（DN）ベースの暗号化マップの設定方法について説明します。ここでの例では、Rivest, Shamir, and Adelman（RSA）署名が IKE 認証方式として使用されています。標準の証明書検証に加え、DN ベースの暗号化マップは、ピアの ISAKMP ID を、X.500 識別名や完全修飾ドメイン名（FQDN）などの証明書内の特定のフィールドと比較します。

前提条件

要件

この機能は、Cisco IOSソフトウェアリリース12.2(4)Tで初めて導入されました。この設定には、このリリース以降が必要です。

Cisco IOSソフトウェアリリース12.3(5)もテストされています。ただし、Cisco Bug ID CSCed45783（登録ユーザ専用）により、DNベースの暗号マップに障害が発生しました。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco 7200 ルータ
- Cisco IOS ソフトウェア リリース 12.2(4)T1 c7200-ik8o3s-mz.122-4.T1

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「シスコ テクニカル ティップスの表記法」を参照してください。

背景説明

以前は、RSA署名方式を使用したIKE認証中、および証明書検証とオプションの証明書失効リスト(CRL)チェックの後、Cisco IOSはIKEクイックモードネゴシエーションを続行しました。暗号化ピアのIPアドレスの制限以外に、リモートVPNデバイスが暗号化インターフェイスと通信するのを防ぐ方法は提供されませんでした。

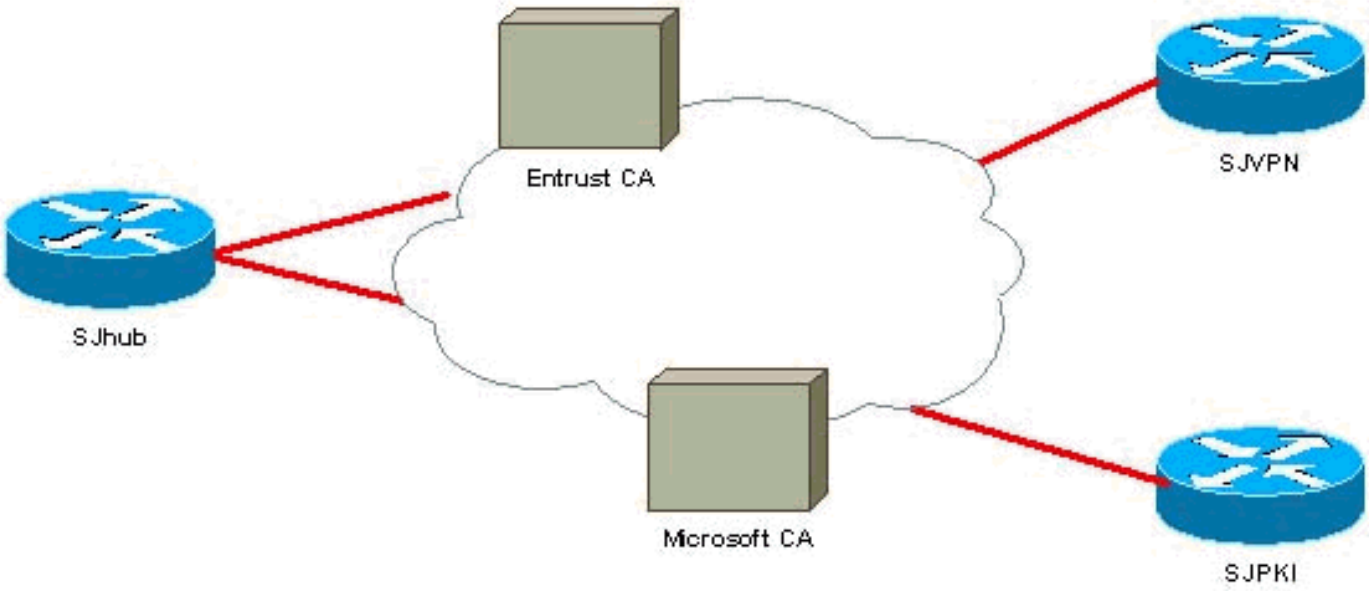
DNベースの暗号マップを使用すると、Cisco IOSはリモートVPNピアを、特定の証明書を持つ選択したインターフェイスだけにアクセスするように制限できます。特に、特定のDNまたはFQDNを持つ証明書。

設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

ネットワーク図

このドキュメントでは、次の図で示されるネットワーク設定を使用しています。



設定

このドキュメントでは、次に示す設定を使用しています。

この例では、機能を紹介する目的で、単純なネットワーク設定が使用されています。SJhub ルータには 2 つの ID 証明書があります。1 つは Entrust 認証局（CA）から取得したもので、もう 1 つは Microsoft CA から取得したものです。詳細については、「関連情報」を参照してください。