

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

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

[はじめに](#)

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 で最初に導入されました。この設定用のこのリリースまたはそれ以降になります。

Cisco IOS ソフトウェア リリース12.3(5)はまたテストされました。ただし、DN は Cisco バグ ID [CSCed45783](#) ([登録ユーザのみ](#)) がクリプト マップによって壊れた原因で基づかせていました。

[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くものです。

- 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

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。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。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

[表記法](#)

ドキュメント表記の詳細は、『[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、の後の RSA シグニチャ方式を使用して IKE 認証の間に、およびチェックする認証検証およびオプションの証明書無効リスト（CRL）Cisco IOS は IKE Quick Mode ネゴシエーションを続けました。それは提供しませんでした暗号化ピアの IP アドレスの制限以外遠隔 VPN デバイスがある暗号化されたインターフェイスと、通信することを防ぐために方式を。

この場合 DN ベースの暗号マップと、Cisco IOS は特定の証明書が付いている選択したインターフェイスしかアクセスしないためにリモート VPN ピアを制限できます。特に、ある特定の DN の証明書が FQDN。

[設定](#)

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

[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構成を使用しています。

[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。