

RV320およびRV325 VPNルータでの証明書の生成

目的

今日の最も一般的な暗号方式の1つは、公開鍵暗号です。公開キー暗号化では、公開キーと秘密キーが使用されます。システムは、まず公開キーを使用して情報を暗号化します。その後、秘密キーを使用することによってのみ、情報を復号化できます。公開鍵暗号化の一般的な用途は、Secure Socket Layer(SSL)またはTransport Layer Security(TLS)接続を使用してアプリケーショントラフィックを暗号化することです。証明書は、公開キーとそのサーバおよびその責任者である組織に関するその他の情報を配布するために使用される方法です。証明書は、認証局(CA)によってデジタル署名できます。CAは、証明書に含まれる情報が正確であることを確認した、信頼できるサードパーティです。

この記事では、RV32x VPNルータシリーズで証明書を生成する方法について説明します。

該当するデバイス

- ・ RV320デュアルWAN VPNルータ
- ・ RV325ギガビットデュアルWAN VPNルータ

[Software Version]

- ・ v1.1.0.09

証明書の生成

ステップ1: Web構成ユーティリティにログインし、[Certificate Management] > [Certificate Generator]を選択します。[証明書ジェネレータ]ページが開きます。

Certificate Generator

Certificate Generator

Type: Certificate Signing Request ▼

Country Name (C): United States ▼

State or Province Name (ST):

Locality Name (L):

Organization Name (O):

Organizational Unit Name (OU):

Common Name (CN):

Email Address (E):

Key Encryption Length: 512 ▼

Save Cancel

Certificate Generator

Certificate Generator

Type: Self-Signed Certificate ▼

Country Name (C): United States ▼

State or Province Name (ST): CA

Locality Name (L): Sanjose

Organization Name (O): companyname

Organizational Unit Name (OU): companybranch

Common Name (CN): name.domain.com

Email Address (E): admin@example.com

ステップ2:[Type]ドロップダウンリストから適切な証明書タイプを選択します。

- ・ 自己署名証明書：これは、独自の作成者によって署名されたSecure Socket Layer(SSL)証明書です。この証明書は、攻撃者によって秘密キーが侵害された場合に取り消すことができないため、信頼できません。
- ・ 認定署名要求(CSR)：これは、デジタルID証明書を申請するために認証局に送信される公開キーインフラストラクチャ(PKI)です。秘密キーは秘密にされるため、自己署名よりも安全です。

ステップ3:[Country Name (国名)]ドロップダウンから、組織が登録されている国名を選択します。

ステップ4:[State]または[Province Name]フィールドに、組織が存在する都道府県、地域、

または地域の名前または省略形を入力します。

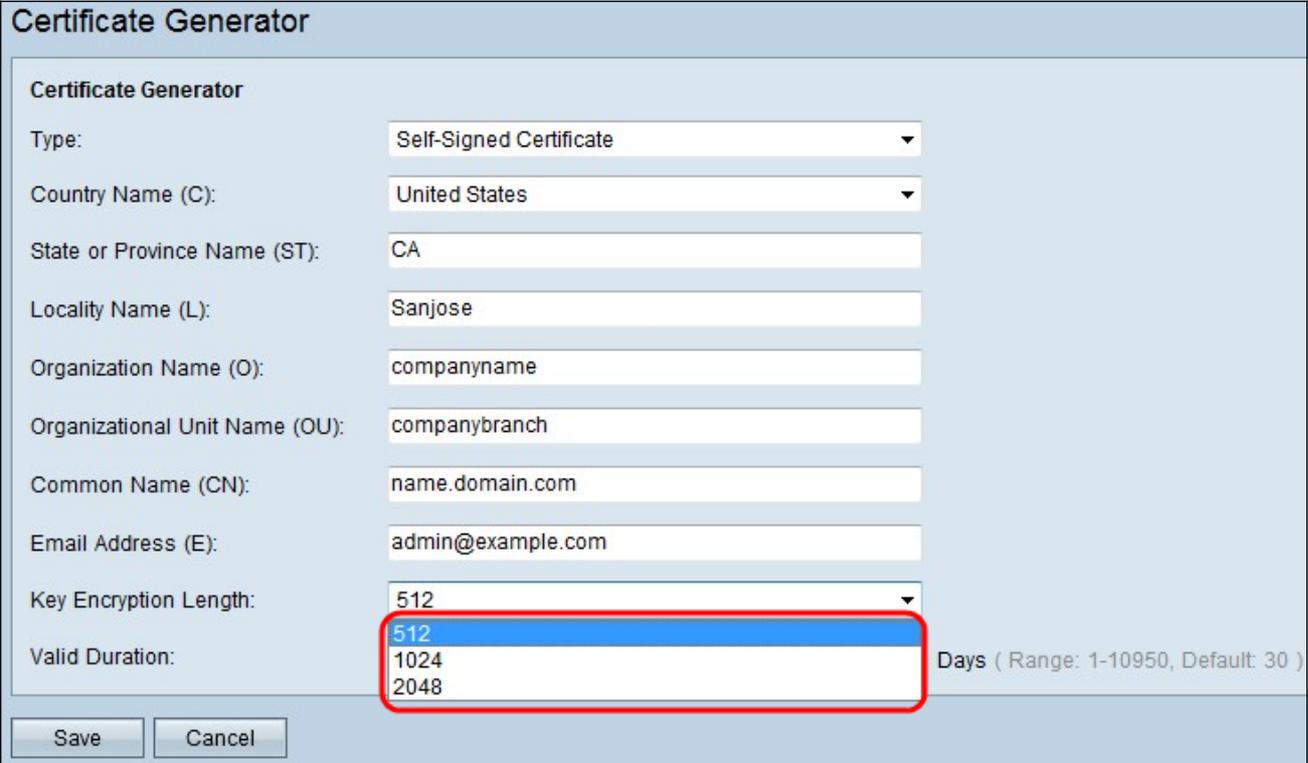
ステップ5:[Locality Name]フィールドに、組織が登録または配置されている市区町村の名前を入力します (図2を参照)。

ステップ6 : ビジネスが法的に登録されている名前を入力します。スモールビジネス/個人事業主として登録している場合は、[組織名(Organization Name)]フィールドに証明書要求者の名前を入力します。

ステップ7:[Organization Unit Name (組織単位名)]フィールドに名前を入力して、組織内の部門間で区別を行います。

ステップ8:[Common Name (共通名)]フィールドに名前を入力します。この名前は、証明書を使用するWebサイトの完全修飾ドメイン名である必要があります。

ステップ9 : 証明書を生成するユーザの電子メールアドレスを入力します。



Certificate Generator

Certificate Generator

Type: Self-Signed Certificate

Country Name (C): United States

State or Province Name (ST): CA

Locality Name (L): Sanjose

Organization Name (O): companyname

Organizational Unit Name (OU): companybranch

Common Name (CN): name.domain.com

Email Address (E): admin@example.com

Key Encryption Length: 512

Valid Duration: 512, 1024, 2048 Days (Range: 1-10950, Default: 30)

Save Cancel

ステップ10:[Key Encryption Length]ドロップダウンから[Key length]を選択します。キーサイズが大きいほど、証明書のセキュリティが高くなります。キーサイズが大きいほど、処理時間が長くなります。

Certificate Generator

Type:	Self-Signed Certificate
Country Name (C):	United States
State or Province Name (ST):	CA
Locality Name (L):	Sanjose
Organization Name (O):	companyname
Organizational Unit Name (OU):	companybranch
Common Name (CN):	name.domain.com
Email Address (E):	admin@example.com
Key Encryption Length:	1024
Valid Duration:	500

Save Cancel

注：証明書タイプを証明書署名要求として選択した場合は、ステップ11をスキップして続行します。

ステップ11：証明書が有効な日数を入力します。

ステップ12:[Save]をクリックして証明書を生成します。生成された証明書が[マイ証明書]ページに表示されます。[My Certificate]ページを表示するには、[Certificate Management] > [My Certificate]を選択します。