

RV016、RV042、RV042G、およびRV082 VPNルータでのVPNユーザの管理とQuick VPNの設定

目的

バーチャルプライベートネットワーク(VPN)は、異なるネットワーク上のエンドポイントを、インターネットなどのパブリックネットワーク経由で接続する方法です。VPNの便利な用途は、VPNクライアントソフトウェアを使用するリモートユーザが、インターネットにアクセスできる限り、プライベートネットワーク上の情報に安全にアクセスできる点です。RV0xxシリーズVPNルータは、QuickVPNを使用するユーザがルータでVPNトンネルを作成できるように設定できます。Cisco QuickVPNは、バーチャルプライベートネットワーク(VPN)へのリモートアクセス用に開発されたソフトウェアです。

VPN証明書は、VPNトンネルのセキュリティを強化する方法です。証明書はルータによって生成され、ルータとQuickVPNユーザの両方が安全であることを確認するために使用されます。ルータから、QuickVPNクライアントが使用できる証明書をエクスポートできます。

この記事では、VPNユーザを設定し、RV0xxシリーズVPNルータのVPN証明書を管理する方法について説明します。

注：VPNユーザを設定する前に、VPNトンネルを設定する必要があります。ゲートウェイ間VPNの設定方法の詳細については、『RV016、RV042、RV042GおよびRV082 VPNルータでのゲートウェイ間VPNの設定』を参照してください。クライアントからゲートウェイへのVPNの設定方法の詳細については、『RV016、RV042、RV042G、およびRV082 VPNルータでのVPNクライアント用のリモートアクセストンネル(クライアントからゲートウェイ)のセットアップ』を参照してください。VPNユーザを設定した後、ユーザのPCでQuickVPNを設定して、VPNトンネルにアクセスする必要があります。

適用可能なデバイス

- RV016
- RV042
- RV042G
- RV082

[Software Version]

- ・ v4.2.2.08 [RVシリーズVPNルータ]
- ・ 1.4.2.1 [Cisco QuickVPN]

VPNユーザの設定

ステップ 1 : Router Configuration Utilityにログインし、VPN > VPN Client Accessの順に選択します。VPN Client Accessページが開きます。

The screenshot shows the 'VPN Client Access' configuration page. It features several input fields and controls:

- Username :** A text input field.
- New Password :** A text input field.
- Confirm New Password :** A text input field.
- Allow Password Change :** Radio buttons for 'Yes' and 'No', with 'No' selected.
- Active :** A checkbox.
- Buttons:** 'Add to list', 'Delete', and 'Add New'.

The bottom section is titled 'Certificate Management' and includes:

- Generate New Certificate :** A 'Generate' button.
- Export Certificate for Administrator :** An 'Export for Admin' button.
- Export Certificate for Client :** An 'Export for Client' button.
- Import Certificate :** A 'Choose File' button (with 'No file chosen' text) and an 'Import' button.
- Existing Certificate :** A text field containing 'RV042G_0101_0000.pem'.
- Buttons:** 'Save' and 'Cancel'.

VPN Client Access

Username :	<input type="text" value="user_1"/>
New Password :	<input type="password" value="...."/>
Confirm New Password :	<input type="password" value="...."/>
Allow Password Change :	<input type="radio"/> Yes <input checked="" type="radio"/> No
Active :	<input checked="" type="checkbox"/>

ステップ 2 : UsernameフィールドにVPN Clientのユーザ名を入力します。

ステップ 3 : New Passwordフィールドにユーザのパスワードを入力します。

ステップ 4 : Confirm New Passwordフィールドに確認のためにパスワードを再入力します。
。

ステップ5: (オプション) ユーザがパスワードを変更できるようにするには、Yesオプションボタンをクリックします。

手順 6 : VPNユーザをアクティブにするには、Activeチェックボックスをオンにします。

手順 7 : Add to listをクリックして、テーブルにユーザを追加します。

VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change : Yes No

Active :

Add to list

user_1=>Active

Delete Add New

VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change : Yes No

Active :

user_1=>Active
user_2=>Active

ステップ8: (オプション) ユーザに関する情報を編集するには、テーブルで特定のユーザをクリックします。必要な情報を編集して、Updateをクリックします。ユーザ名は編集できません。

ステップ9: (オプション) テーブルからユーザを削除するには、テーブルから特定のユーザをクリックし、Deleteをクリックします。

ステップ10: (オプション) 新しいVPNユーザを追加するには、Add Newをクリックして、ステップ1 ~ 7に従います。

ステップ 11[Save] をクリックして、設定を保存します。

証明書の管理

注：PC上で証明書なしでVPN接続を確立できます。ただし、証明書はVPNのセキュリティを強化します。

ステップ 1 : Router Configuration Utilityにログインし、VPN > VPN Client Accessの順に選択します。VPN Client Accessページが開きます。Certificate Management領域までスクロールダウンします。

VPN Client Access

Username :

New Password :

Confirm New Password :

Allow Password Change : Yes No

Active :

Add to list

user_1=>Active
user_2=>Active
user23=>Active
user_3=>Active

Delete Add New

Certificate Management

Generate New Certificate :

Export Certificate for Administrator :

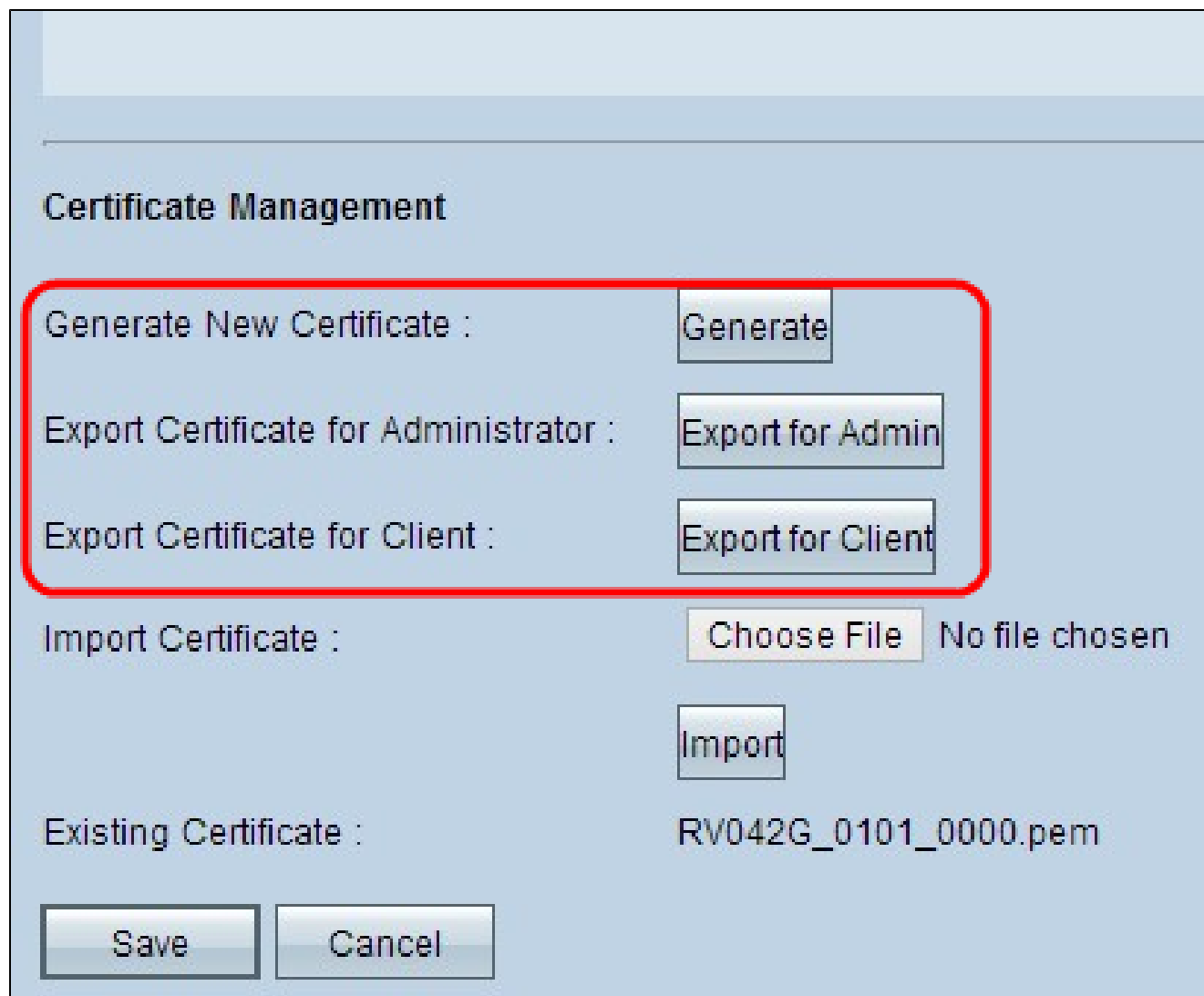
Export Certificate for Client :

Import Certificate : No file chosen

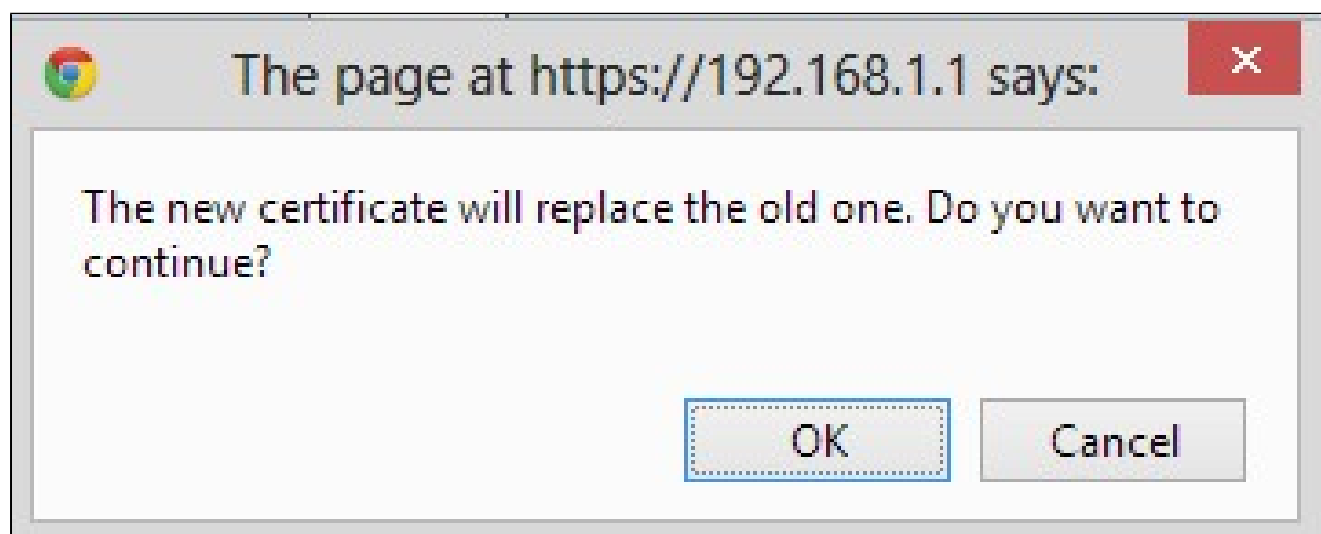
Existing Certificate : RV042G_0101_0000.pem

Existing Certificateフィールドに現在の証明書が表示されます。証明書をPCにエクスポートする場合は、「[証明書のエクスポート](#)」セクションに移動します。PCからルータに証明書をインポートする場合は、「[証明書のインポート](#)」セクションに進みます。

証明書のエクスポート



ステップ1: (オプション) ルータの新しい証明書を作成するには、Generateをクリックします。これにより、以前の証明書が新しい証明書に置き換えられます。警告メッセージウィンドウが表示されます。



ステップ 2 : OKをクリックして新しい証明書で続行し、古い証明書を新しい証明書で置き換えます。

ステップ3: (オプション) 証明書をダウンロードし、バックアップとしてPCに保存するには、Export for Adminをクリックします。管理証明書には秘密キーが含まれており、工場出荷時のリセット時にバックアップとして使用されます。

ステップ 4 : Export for Clientをクリックして、クライアント証明書をダウンロードし、PCに保存します。ユーザがVPNトンネルにアクセスする際に使用されます。ルータは.pemファイルをコンピュータに保存します。

注:Windowsの証明書ストアに.pemファイルを保存するには、.pfxまたは.p12ファイルに変換する必要があります。

証明書のインポート



The screenshot shows a 'Certificate Management' window with several options. The 'Import Certificate' section is highlighted with a red border. It includes a 'Choose File' button, the text 'LICENSE', and an 'Import' button. Below this, the 'Existing Certificate' field displays 'RV042G_0101_0000.pem'.

Generate New Certificate :	Generate
Export Certificate for Administrator :	Export for Admin
Export Certificate for Client :	Export for Client
Import Certificate :	Choose File LICENSE
	Import
Existing Certificate :	RV042G_0101_0000.pem

ステップ 1 : Choose Fileをクリックし、インポートする証明書を選択します。ファイルタイプは.pemである必要があります。

ステップ 2 : Importをクリックして、証明書をインポートします。

ステップ 3 : [Save] をクリックして、設定を保存します。

Cisco QuickVPNのセットアップ

注 : このソフトウェアは、Windowsオペレーティングシステムでのみサポートされています。このソフトウェアは、シスコの公式Webサイト(www.cisco.com)からダウンロードできません。

ステップ 1 : Cisco QuickVPNソフトウェアを開きます。

Small Business
QuickVPN Client

Profile Name :

User Name :

Password :

Server Address :

Port For QuickVPN :

Use Remote DNS Server :

© 2010 Cisco Systems, Inc. All rights reserved. Ver 1.4.2.1



Small Business

QuickVPN Client

Profile Name :

TestTunnel

User Name :

Password :

Server Address :

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ステップ 2 : Profile Nameフィールドに、RV有線ルータで作成されたVPNトンネルの名前を入力します。



Small Business

QuickVPN Client

Profile Name :

TestTunnel

User Name :

username1

Password :

Server Address :

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ステップ 3 : User Nameフィールドに、ルータに割り当てられたユーザ名を入力します。



Small Business

QuickVPN Client

Profile Name : TestTunnel

User Name : username1

Password :

Server Address :

Port For QuickVPN : Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ステップ 4 : Passwordフィールドに、ルータに割り当てられたパスワードを入力します。



Small Business

QuickVPN Client

Profile Name :

TestTunnel

User Name :

username1

Password :

XXXXXXXX

Server Address :

192.168.10.0

Port For QuickVPN :

Auto

Use Remote DNS Server :

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

ステップ 5 : Server Addressフィールドに、VPNに使用するルータのIPアドレスを入力します。



Small Business

QuickVPN Client

Profile Name :

TestTunnel

User Name :

username1

Password :

Server Address :

192.168.10.0

Port For QuickVPN :

Auto

Use Remote DNS Server :

443
60443
Auto

Connect

Save

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

手順 6 : Use Remote DNS Server ドロップダウンリストで、適切なポート番号を選択します。Auto はデフォルト値で、VPN 設定に基づいてポート番号が自動的に選択されます。



Small Business

QuickVPN Client

Profile Name :	TestTunnel
User Name :	username1
Password :	XXXXXXXX
Server Address :	192.168.10.0
Port For QuickVPN :	Auto
Use Remote DNS Server :	<input checked="" type="checkbox"/>

Connect

Save

Delete

Help

© 2010 Cisco Systems, Inc. All rights reserved.

Ver 1.4.2.1

手順 7 : ドメイン名を解決できるDNSサーバがある場合は、Use Remote DNS Serverチェックボックスにチェックマークを入れます。そうでない場合は、チェックマークを外して、VPNネットワーク設定を使用します。



ステップ 8 : Connectをクリックして、VPNにアクセスします。

ステップ9: (オプション) 設定を保存するには、Saveをクリックします。

ステップ10: (オプション) 保存済みの構成を削除するには、[削除]をクリックします。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。