

# RV34xシリーズルータでのグループポリシーの設定

## 目的

グループポリシーは、インターネットプロトコルセキュリティ(IPSec)接続のユーザ指向の属性または値の組み合わせのセットで、内部（ローカル）またはリモート認証ダイヤルインユーザサービス(RADIUS)またはLightweight Directory Access Protocol(LDAP)サーバに外部で保存されます。トンネルグループは、トンネルの確立後にバーチャルプライベートネットワーク(VPN)ユーザ接続の用語を設定するグループポリシーを使用します。

グループポリシーを使用すると、ユーザごとに属性を個別に指定する必要はなく、ユーザまたはユーザグループに属性のセット全体を適用できます。特定のユーザのグループポリシー属性を変更することもできます。

このドキュメントの目的は、RV34x VPNルータシリーズでグループポリシーを設定する方法を示すことです。

## 該当するデバイス

- RV34xシリーズ

## [Software Version]

- 1.0.01.16

## グループポリシーの設定

ステップ1：ルータのWebベースユーティリティにログインし、[VPN] > [SSL VPN]を選択します。



ステップ2:[SSL VPN]領域で、[Group Policies]タブをクリックします。

## SSL VPN

General Configuration

Group Policies

ステップ3:[SSL VPN Group Table]の下の[Add]ボタンをクリックして、グループポリシーを追加します。

Policy Name
SSLVPNDefaultPolicy

Add Edit Delete

注：SSL VPNグループテーブルには、デバイス上のグループポリシーのリストが表示されます。リストの最初のグループポリシー(SSLVPNDefaultPolicy)を編集することもできます。これは、デバイスによって提供されるデフォルトポリシーです。

ステップ4:[Policy Name]フィールドに希望するポリシー名を入力します。

SSL VPN

General Configuration Group Policies

### SSLVPN Group Policy - Add/Edit

#### Basic Settings

Policy Name: Group 1 Policy

Primary DNS: 192.168.1.1

Secondary DNS:

Primary WINS:

Secondary WINS:

注：この例では、グループ1ポリシーが使用されています。

ステップ5：表示されたフィールドにプライマリDNSのIPアドレスを入力します。デフォルトでは、このIPアドレスはすでに指定されています。

SSLVPN Group Policy - Add/Edit

#### Basic Settings

Policy Name: Group 1 Policy

Primary DNS: 192.168.1.1

Secondary DNS:

Primary WINS:

Secondary WINS:

注：この例では、192.168.1.1が使用されています。

ステップ6: ( オプション ) 表示されたフィールドにセカンダリDNSのIPアドレスを入力します。これは、プライマリDNSが失敗した場合のバックアップとして機能します。

**SSLVPN Group Policy - Add/Edit**

**Basic Settings**

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

注：この例では、192.168.1.2が使用されています。

ステップ7: ( オプション ) 表示されたフィールドにプライマリWINSのIPアドレスを入力します。

**SSLVPN Group Policy - Add/Edit**

**Basic Settings**

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

注：この例では、192.168.1.1が使用されています。

ステップ8: ( オプション ) 表示されたフィールドにセカンダリWINSのIPアドレスを入力します。

**SSLVPN Group Policy - Add/Edit**

**Basic Settings**

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

注：この例では、192.168.1.2が使用されています。

ステップ9: ( オプション ) [Description]フィールドにポリシーの説明を入力します。

**SSLVPN Group Policy - Add/Edit**

**Basic Settings**

Policy Name:

Primary DNS:

Secondary DNS:

Primary WINS:

Secondary WINS:

Description:

注：この例では、スプリットトンネルを使用するグループポリシーが使用されます。

ステップ10: ( オプション ) オプションボタンをクリックして、IEプロキシポリシーを選択し、Microsoft Internet Explorer(MSIE)プロキシ設定を有効にしてVPNトンネルを確立します。次のオプションがあります。

- [なし(None)] : ブラウザがプロキシ設定を使用しないようにします。
- [自動(Auto)] : ブラウザがプロキシ設定を自動的に検出できるようにします。
- Bypass-local : リモートユーザに設定されているプロキシ設定をブラウザがバイパスできるようにします。
- Disabled:MSIEプロキシ設定を無効にします。

**IE Proxy Settings**

IE Proxy Policy  None  Auto  Bypass-local  Disabled

注：この例では、[Disabled]が選択されています。これがデフォルト設定です。

ステップ11: ( オプション ) [Split Tunneling Settings]領域で、[Enable Split Tunneling]チェックボックスをオンにして、インターネット宛てのトラフィックを暗号化されずにインターネットに直接送信できるようにします。完全トンネリングは、すべてのトラフィックをエンドデバイスに送信し、エンドデバイスは宛先リソースにルーティングされ、Webアクセスのパスから企業ネットワークが排除されます。

**IE Proxy Settings**

IE Proxy Policy  None  Auto  Bypass-local  Disabled

**Split Tunneling Settings**

Enable Split Tunneling

ステップ12: ( オプション ) スプリットトンネリングの適用時にトラフィックを含めるか除外するかを選択するには、オプションボタンをクリックします。

### Split Tunneling Settings

Enable Split Tunneling

Split Selection



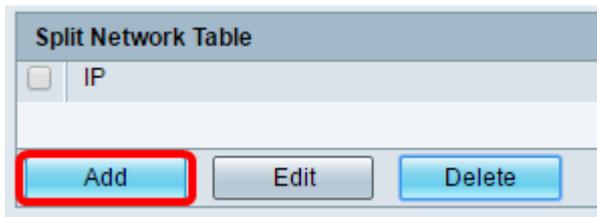
Include Traffic



Exclude Traffic

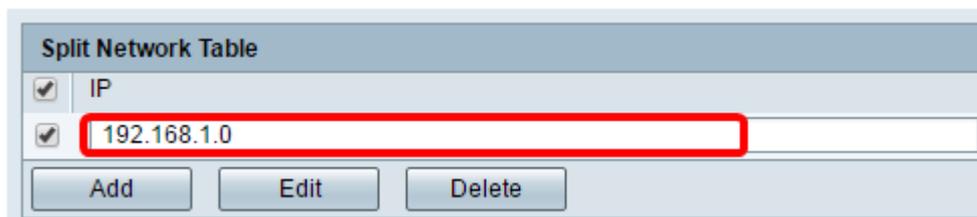
注：この例では、[Include Traffic]が選択されています。

ステップ13:[Split Network Table]で、[Add]ボタンをクリックして、Split Network例外を追加します。



Split Network Table	
<input type="checkbox"/>	IP
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

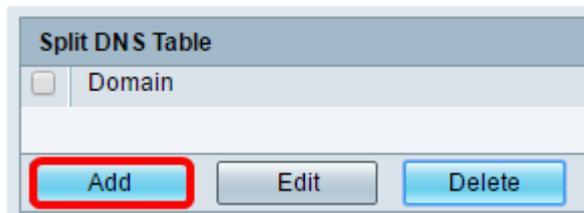
ステップ14：表示されたフィールドにネットワークのIPアドレスを入力します。



Split Network Table	
<input checked="" type="checkbox"/>	IP
<input checked="" type="checkbox"/>	192.168.1.0
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

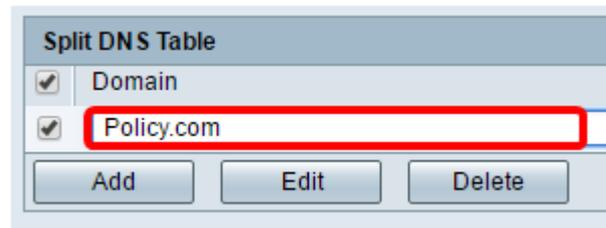
注：この例では、192.168.1.0が使用されています。

ステップ15:[スプリットDNSテーブル]で、[追加]ボタンをクリックして、スプリットDNS例外を追加します。



Split DNS Table	
<input type="checkbox"/>	Domain
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

ステップ16：表示されたフィールドにドメイン名を入力します。



Split DNS Table	
<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com
<input type="button" value="Add"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>	

注：この例では、Policy.comが使用されています。

ステップ17:[Apply]をクリックします。

Split DNS Table	
<input checked="" type="checkbox"/>	Domain
<input checked="" type="checkbox"/>	Policy.com

Add Edit Delete

Apply Cancel

設定が正常に保存されると、新しく追加されたグループポリシーを示すSSL VPNグループテーブルにリダイレクトされます。

SSL VPN Group Table	
Policy Name	Description
<input type="checkbox"/> Group 1 Policy	Group Policy with Split Tunneling
<input type="checkbox"/> SSLVPNDefaultPolicy	

Add Edit Delete

Apply Cancel

これで、RV34xシリーズルータでグループポリシーが正しく設定されました。

RV340のEasy Setup Guideを表示するには、[ここをクリックしてください](#)。

RV340のアドミニストレーションガイドを表示する場合は、[ここをクリックします](#)。グループポリシー情報は、93ページにあります。