# RV34x シリーズ ルータでの AnyConnect バーチ ャル プライベート ネットワーク(VPN)接続の 設定

## 目的

このドキュメントの目的は、RV34x シリーズ ルータで AnyConnect VPN 接続を設定する方法を 説明することです。

AnyConnectセキュアモビリティクライアントを使用する利点:

- 1. セキュアで持続的な接続
- 2. 継続的なセキュリティとポリシーの適用
- 3. 適応型セキュリティアプライアンス(ASA)またはエンタープライズソフトウェアデプロ イメントシステムから導入可能
- 4. カスタマイズ可能で翻訳可能
- 5.設定が容易
- インターネットプロトコルセキュリティ(IPSec)とセキュアソケットレイヤ(SSL)の両 方をサポート
- 7. インターネットキーエクスチェンジバージョン2.0(IKEv2.0)プロトコルをサポート

#### 概要

バーチャルプライベートネットワーク(VPN)接続では、インターネットなどのパブリックまたは 共有ネットワークを経由してプライベートネットワークとの間でデータのアクセス、送信、およ び受信を行うことができますが、プライベートネットワークとそのリソースを保護するために、 基盤となるネットワークインフラストラクチャへの安全な接続を確保します。

VPNクライアントは、リモートネットワークに接続するコンピュータにインストールされ、実行 されるソフトウェアです。このクライアントソフトウェアは、IPアドレスや認証情報など、 VPNサーバと同じ設定でセットアップする必要があります。この認証情報には、データの暗号化 に使用されるユーザ名と事前共有キーが含まれます。接続するネットワークの物理的な場所に応 じて、VPNクライアントはハードウェアデバイスにすることもできます。これは通常、VPN接続 を使用して、別の場所にある2つのネットワークを接続する場合に発生します。

Cisco AnyConnectセキュアモビリティクライアントは、さまざまなオペレーティングシステムや ハードウェア構成で動作するVPNに接続するためのソフトウェアアプリケーションです。このソ フトウェアアプリケーションを使用すると、ユーザが自分のネットワークに直接接続しているか のように、別のネットワークのリモートリソースに安全な方法でアクセスできるようになります 。Cisco AnyConnectセキュアモビリティクライアントは、コンピュータベースまたはスマートフ ォンプラットフォーム上のモバイルユーザを保護する革新的な新しい方法を提供し、エンドユー ザに対してよりシームレスで常に保護されたエクスペリエンスを提供し、IT管理者に対して包括 的なポリシーを適用します。

RV34xルータでは、ファームウェアバージョン1.0.3.15からAnyConnectライセンスは不要です。 クライアントライセンスに対してのみ料金が発生します。

RV340シリーズルータでのAnyConnectライセンスの詳細については、「<u>RV340シリーズルータ用</u> <u>のAnyConnectライセンス</u>」の記事を参照してください。



## 該当するデバイス |ファームウェアバージョン

- Cisco AnyConnect セキュア モビリティ クライアント | 4.4(最新バージョンをダウンロード)
- RV34xシリーズ | 1.0.03.15(最新バージョンをダウンロード)

## RV34xでのAnyConnect VPN接続の設定

## RV34xでのSSL VPNの設定

ステップ1:ルータのWebベースユーティリティにアクセスし、[VPN]>[SSL VPN] を選択します。



ステップ2: [On] オプションボタンをクリックして、Cisco SSL VPNサーバを有効にします。

E	cisco	RV345P	-RV345P	•
SSL VPN				
Gen	eral Configu	ration	Group	Policies
Cisco	SSL VPN Se	erver: 💿		r <b>r</b>

## 必須ゲートウェイ設定

次の構成設定は必須です。

ステップ3:ドロップダウンリストからゲートウェイインターフェイスを選択します。これは、 SSL VPNトンネルを通過するトラフィックに使用されるポートです。次のオプションがあります

- o
- WAN1
- WAN2
- USB1
- USB2

# Mandatory Gateway Settings

WAN1 Gateway Interface:

注:この例では、WAN1が選択されています。

ステップ 4:SSL VPNゲートウェイに使用するポート番号を[Gateway Port] フィールドに1 ~ 65535の範囲で入力します。

Gateway Interface:	WAN1 🗸	
Gateway Port:	8443	(Range: 1-65535)

**注:この**例では、ポート番号として8443が使用されています。

ステップ 5:ドロップダウンリストから証明書ファイルを選択します。この証明書は、SSL VPNトンネルを介してネットワークリソースにアクセスしようとするユーザを認証します。ドロ ップダウンリストには、デフォルトの証明書とインポートされる証明書が含まれています。



注:この例では、[Default]が選択されています。

手順 6 : [Client Address Pool] フィールドにクライアントアドレスプールのIPアドレスを入力しま す。このプールは、リモートVPNクライアントに割り当てられるIPアドレスの範囲です。

**注:IPア**ドレスの範囲がローカルネットワークのどのIPアドレスとも重複していないことを確認 してください。



**注:この**例では、192.168.0.0が使用されています。

手順7:ドロップダウンリストからクライアントネットマスクを選択します。



**注:この**例では、255.255.255.128が選択されています。

ステップ 8 : [Client Domain] フィールドにクライアントドメイン名を入力します。これは、SSL VPNクライアントにプッシュするドメイン名になります。



WideDomain.com

注:この例では、クライアントのドメイン名としてWideDomain.comが使用されています。

ステップ 9 : [Login Banner] フィールドにログインバナーとして表示されるテキストを入力しま す。これは、クライアントがログインするたびに表示されるバナーです。

#### Mandatory Gateway Settings

Gateway Interface:	WAN1 ~
Gateway Port:	8443
Certificate File:	Default 🗸
Client Address Pool:	192.168.0.0
Client Netmask:	255.255.255.0 ~
Client Domain:	yourdomain.com
Login Banner:	Welcome to WideDomain!

**注:この**例では、Welcome to Widedomain!がログインバナーとして使用されています。

オプションのゲートウェイ設定

次の構成設定はオプションです。

ステップ 1 : アイドルタイムアウトの値を秒単位で入力します。値の範囲は60 ~ 86400です。こ れは、SSL VPNセッションがアイドル状態を維持できる時間です。

**Optional Gateway Settings** 

Idle Timeout:	3000	sec. (Range: 60-86400)
idie fiffiedut.	3000	sec. (Range: 60-86400)

注:この例では、3000が使用されています。

ステップ 2: [*Session Timeout*]フィールドに秒単位の値を入力します。これは、Transmission Control Protocol(TCP;伝送制御プロトコル)またはUser Datagram Protocol(UDP;ユーザデ ータグラムプロトコル)セッションが、指定したアイドル時間の後にタイムアウトするまでの時 間です。範囲は 60 ~ 1209600 です。

**Optional Gateway Settings** 

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)

注:この例では、60が使用されています。

ステップ 3 : [ClientDPD Timeout] フィールドに0 ~ 3600の範囲で秒単位の値を入力します。この 値は、VPNトンネルのステータスを確認するためのHELLO/ACKメッセージの定期的な送信を指 定します。

注:この機能は、VPNトンネルの両端で有効にする必要があります。

**Optional Gateway Settings** 

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)

## **注:この**例では、350が使用されています。

ステップ 4 : [GatewayDPD Timeout] フィールドに0 ~ 3600の範囲で秒単位の値を入力します。 この値は、VPNトンネルのステータスを確認するためのHELLO/ACKメッセージの定期的な送信

#### を指定します。

#### 注:この機能は、VPNトンネルの両端で有効にする必要があります。

#### **Optional Gateway Settings**

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)
Gateway DPD Timeout:	360	sec. (Range: 0-3600)

## 注:この例では、360が使用されています。

## ステップ 5 : [Keep Alive] フィールドに0 ~ 600の範囲の値を秒単位で入力します。この機能により、ルータは常にインターネットに接続されます。VPN接続がドロップされた場合は、再確立が 試行されます。

### **Optional Gateway Settings**

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)
Gateway DPD Timeout:	360	sec. (Range: 0-3600)
Keep Alive:	40	sec. (Range: 0-600)

#### 注:この例では、40が使用されています。

手順 6 : [Lease Duration] フィールドに、接続するトンネルの期間を秒単位で入力します。範囲は 600 ~ 1209600 です。

#### **Optional Gateway Settings**

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)
Gateway DPD Timeout:	360	sec. (Range: 0-3600)
Keep Alive:	40	sec. (Range: 0-600)
Lease Duration:	43500	sec. (Range: 600-1209600)

#### 注:この例では、43500が使用されています。

手順 7 : ネットワーク経由で送信できるパケットサイズをバイト単位で入力します。範囲は 576 ~ 1406 です。

## **Optional Gateway Settings**

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)
Gateway DPD Timeout:	360	sec. (Range: 0-3600)
Keep Alive:	40	sec. (Range: 0-600)
Lease Duration:	43500	sec. (Range: 600-1209600)
Max MTU:	1406	bytes (Range: 576-1406)

## **注:この**例では、1406が使用されています。

## ステップ 8 : [Rekey Interval] フィールドにリレー間隔の時間を入力します。キー再生成機能を使 用すると、セッションの確立後にSSLキーを再ネゴシエートできます。範囲は 0 ~ 43200 です。

## Optional Gateway Settings

Idle Timeout:	3000	sec. (Range: 60-86400)
Session Timeout:	60	sec. (Range: 0,60-1209600)
Client DPD Timeout:	350	sec. (Range: 0-3600)
Gateway DPD Timeout:	360	sec. (Range: 0-3600)
Keep Alive:	40	sec. (Range: 0-600)
Lease Duration:	43500	sec. (Range: 600-1209600)
Max MTU:	1406	bytes (Range: 576-1406)
Rekey Interval:	3600	sec. (Range: 0-43200)

## **注:この**例では、3600が使用されています。

## ステップ 9 : [Apply] をクリックします。



グループポリシーの設定

ステップ1: [Group Policies] タブをクリックします。

SSL VPN	
General Configuration	Group Policies

ステップ 2:SSL VPNグループテーブルの下にある[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。

SSL VPN	
General Configuration	Group Policies
SSL VPN Group Table	
<ul> <li>Image: Policy Name ⇒</li> </ul>	
SSLVPNDefaultPolicy	

**注:**SSL **VPNグ**ループテーブルには、デバイス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3: [Policy Name] フィールドに任意のポリシー名を入力します。

**Basic Settings** 

Policy Name:	Group1Policy
Primary DNS:	192.168.1.1

**注:この**例では、Group 1 Policyが使用されています。

ステップ 4 : 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:	Group1Policy
Primary DNS:	192.168.1.1

注:この例では、192.168.1.1が使用されています。

ステップ5:(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に障害が発生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:	Group1Policy
Primary DNS:	192.168.1.1
Secondary DNS:	192.168.1.2

## **注:この**例では、192.168.1.2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:	Group1Policy
Primary DNS:	192.168.1.1
Secondary DNS:	192.168.1.2
Primary WINS:	192.168.1.1

## **注:この**例では、192.168.1.1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、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:	Group1Policy
Primary DNS:	192.168.1.1
Secondary DNS:	192.168.1.2
Primary WINS:	192.168.1.1
Secondary WINS:	192.168.1.2

**Basic Settings** 

#### 注:この例では、192.168.1.2が使用されています。

ステップ8:(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

	0
Policy Name:	Group 1 Policy
Primary DNS:	192.168.1.1
Secondary DNS:	192.168.1.2
Primary WINS:	192.168.1.1
Secondary WINS:	192.168.1.2
Description:	Group policy with split tunnel

#### **注:この例**では、スプリットトンネルを使用したグループポリシーが使用されています。

ステップ9:(オプション)オプションボタンをクリックして[IE Proxy Policy]を選択し、Microsoft Internet Explorer(MSIE)プロキシ設定でVPNトンネルを確立できるようにします。次のオプション があります。

- [なし(None)]: ブラウザでプロキシ設定を使用しません。
- •[自動]: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 : ブラウザがリモートユーザに設定されているプロキシ設定をバイパスできるようにします。
- [無効(Disabled)]:MSIEプロキシ設定を無効にします。

IE Proxy Settings

IE Proxy Policy: O None O Auto O Bypass-local (O 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10(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せずに直接インターネットに 送信できるようにします。フルトンネリングでは、すべてのトラフィックがエンドデバイスに送 信され、エンドデバイスが宛先リソースにルーティングされるため、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。

# Split Tunneling Settings

## Enable Split Tunneling

ステップ11:(オプション)オプションボタンをクリックして、スプリットトンネリングを適用す る際にトラフィックを含めるか除外するかを選択します。



注:この例では、[Include Traffic]が選択されています。

ステップ 12[Split Network Table]で、[Add] ボタンをクリックして、分割ネットワークの例外を追加します。

#### Split Network Table

ステップ 13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 Tunneling Settings						
Splin	<ul> <li>Enable Split Tunneling</li> <li>Split Selection</li> <li>Include Traffic</li> <li>Exclude Traffic</li> </ul>				Exclude Traffic	
S	Split Network Table					
	+	IP ≑				
		192.168.1.0				

注:この例では、192.168.1.0が使用されています。

ステップ 14:スプリットDNSテーブルで、[Add] 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



ステップ15:表示されたフィールドにドメイン名を入力し、Applyをクリックします。

#### Split DNS Table



## AnyConnect VPN接続の確認

ステップ1: [AnyConnect Secure Mobility Client] アイコンをクリックします。



ステップ2: [AnyConnect Secure Mobility Client]ウィンドウで、ゲートウェイIPアドレスとゲートウェイポート番号をコロン(:)で区切って入力し、[Connect] をクリックします。

•••	AnyConnect Secure Mobility Client		cisco
	VPN: Ready to connect.		
	10.10.10.1:8443	~	Connect

**注:この**例では、10.10.10.1:8443が使用されています。ソフトウェアは、リモートネットワーク に接続していることを示します。

•••	AnyConnect Secure Mobility Client		cisco	1.
	VPN: Contacting 10.10.10.1:8443. 10.10.10.1:8443	~	Connect	

ステップ3:それぞれのフィールドにサーバのユーザ名とパスワードを入力し、**OK**をクリックします。

Please enter	r your username and password.			
Username:	Group1 user			
 Password:				
	Cancel OK			

**注:この**例では、ユーザ名としてGroup1ユーザが使用されています。

ステップ 4:接続が確立されるとすぐに、ログインバナーが表示されます。[Accept] をクリック します。

Cisco	o AnyConnect - Ba	anner
Welcome to W	ideDomain!	
	Disconnect	Accept

AnyConnectウィンドウに、ネットワークへのVPN接続が成功したことが示されます。

	AnyConnect Secure Mobility Client	cisco		
	VPN: Connected to 10.10. 10.10.10.1:8443	10.1:8443	~	Disconnect
00:03:49	)			IPv4

ステップ5:(オプション)ネットワークから切断するには、[Disconnect] をクリックします。 これで、RV34xシリーズルータを使用したAnyConnect VPN接続が正常に設定されました。 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。