# RV34Xシリーズルータに接続するためのShrew Soft VPN Clientの設定

## 目的

このドキュメントの目的は、Shrew Soft VPN Clientを使用してRV340シリーズルータに接続する 方法を示すことです。

最新バージョンのShrew Soft VPN Clientソフトウェアは、次の場所からダウンロードできます。

https://www.shrew.net/download/vpn

## 該当するデバイス |ソフトウェアバージョン

RV340 | 1.0.3.17 <u>(最新のダウンロード)</u>

RV340W | 1.0.3.17 (最新のダ<u>ウンロード</u>)

RV345 | 1.0.3.17 (最新のダ<u>ウンロード</u>)

RV345P | 1.0.3.17 (最新のダ<u>ウンロード</u>)

#### 概要/使用例

IPSec VPN(Virtual Private Network)を使用すると、インターネット経由で暗号化さ れたトンネルを確立することで、リモートリソースを安全に取得できます。 RV34XシリーズルータはIPSEC VPNサーバとして動作し、Shrew Soft VPN Clientをサポートします。このガイドでは、ルータとShrew Soft Clientを設定して 、VPNへの接続を保護する方法について説明します。

このドキュメントには、次の2つの部分があります。

RV340シリーズルータの設定

Shrew Soft VPN Clientの設定

## RV34Xシリーズルータを設定します。

まず、RV34xでクライアント**からサイトへのVPNを**設定します

#### 手順 1

[VPN] > [Client-to-Site]で、



#### 手順2

#### クライアント**からサイトへのVPNプロファ**イルの追加

_						
٢	Getting Started	Client to Site			Apply	Cancel
Ģ	Status and Statistics					
*	Administration	IPSec Client-to-Site Tunnels				•
٥	System Configuration					
0	WAN	tt @ □ Group/Turnel Name ≜	WAN Interface	Authentication Method =		
#	LAN					
<b>?</b>	Wireless					
8	Routing					
	Firewall					
	VPN 1					
	VPN Status					
	IPSec Profiles					
	Site-to-Site					
С	Client-to-Site 2					

#### 手順 3

[Cisco VPN Client]オプションを選択します。



#### 手順 4

[Enable] ボックスをオンにして、VPN Clientプロファイルをアクティブにします。グループ名を 設定*し、WANイ*ンターフェイス**を選択**し、事前共有キ**ーを入力します**。 **注**:後でクライアントを構成する際に使用するグループ名と事前共有キーに注意してください。

Enable:	
Group Name:	Clients
Interface:	WAN1 ~
IKE Authentication Method	t de la construcción de la const
<ul><li>IKE Authentication Method</li><li>Pre-shared Key:</li></ul>	d •••••
<ul> <li>IKE Authentication Method</li> <li>Pre-shared Key: Minimum Pre-shared Key Complexity:</li> </ul>	d ••••• □ Enable
<ul> <li>IKE Authentication Method</li> <li>Pre-shared Key:</li> <li>Minimum Pre-shared Key Complexity:</li> <li>Show Pre-shared Key:</li> </ul>	Enable     Enable

#### 手順5

ここでは、[ユー**ザーグループ表]は**空白のままにします。これはルータ上の*ユーザグ*ループ用です が、まだ設定していません。[Mode]が[**Client**]に**設定され**ていることを確認します。クライアント LANのプール範囲を入力します。172.16.10.1 ~ 172.16.10.10を使用します。

**注**:プール範囲は、ネットワーク上の他の場所では使用されない一意のサブネットを使用する必要があります。

User Group:	
User Group Table	
Mode:	Client O NEM
Pool Range for Client LAN	
Start IP:	172.16.10.1
End IP:	172.16.10.10

#### 手順6

ここでは、モード設定を構成します。使用する設定は次のとおりです。

**プライマリDNSサーバ**:内部DNSサーバがある場合、または外部DNSサーバを使用する場合は、ここに入力できます。それ以外の場合、デフォルトはRV340 LAN IPアドレスに設定されます。この例では、デフォルトを使用します。

**スプリットトンネル**:[Split Tunneling]をオンにします。これは、VPNトンネルを通過するト ラフィックを指定するために使用されます。この例では、スプリットトンネルを使用します 。

# **スプリットトンネルテーブル**:VPNクライアントがVPN経由でアクセスする必要があるネットワークを入力します。この例では、RV340 LANネットワークを使用しています。

Mode Configuration			
Primary DNS Server:	192.168.1.1		
Secondary DNS Server:			
Primary WINS Server:			
Secondary WINS Server:			
Default Domain:			
Backup Server 1:		(IP Address or Domain Name)	
Backup Server 2:		(IP Address or Domain Name)	
Backup Server 3:		(IP Address or Domain Name)	
Split Tunnel:			
Split Tunnel Table			
+ 🕜 💼			
IP Address ≑			Netmask 🜩
☑ 192.168.1.0			255.255.255.0

## ステップ7

#### [Save]をク**リック**すると、[IPSec Client-to-Site Groups]リストにプロファイ**ルが表示さ**れます。

Client to Site		
IPSec Client-to-Site Tunnels		
<ul> <li>+ I and a second second</li></ul>	WAN Interface 🗢	Authentication Method \$
Clients	WAN1	Pre-shared Key

#### 手順8

次に、VPN Clientユーザの認証に**使用する**ユーザグループを設定します。[システム**構成]**>[ユー **ザーグループ]で[+]をクリック**し、ユーザグループを追加します。



グループ名を入力します。

Overviev	V	
Group Name:	VPN	

#### 手順 10

[Services] セクション> [EzVPN/3rd Party] で、[Add] をクリックし、このユーザグループを以前に 設定したクライアントからサイトへのプロファイルにリンクします。

💿 altalta cisco	RV340W-router45	00E2	×				
User Groups			Add Feature List				
			Select a Profile Clients •				
Overview							
Overview			Add Cancel				
Group Name: VPN	4						
Local User Mem	bership List						
# 0 Join 0	User Name \$	Joined Gr	oups* 0				
1 0	cisco	admin					
2 🗆	guest	guest					
* Should have at lea	st one account in the " a	fmin" group					
Web Login/NETCON Site to Site VPN	IF/RESTCONF 💿 Disab	iled O Read Only	O Administrator				
Site to Site VPN	Profile Member In-use	Table					
+ 🔒							
□ # \$ Con	nection Name 🌣						
EzVPN/3rd Party							
EzVPN/3rd Party	Profile Member In-use	Table					
+ 🔒							
□ # \$ Gro	D # © Group Name ©						

EzVPN/3rd Partyのリストに[Client-to-Site Group Name]が表示されます



### ステップ 12

ユーザグループ**の設定を**適用すると、[ユーザグループ]リストに表示され、以前に作成したクライ アント間プロファイルで新しいユーザグループが使用されることが表示されます。

<ul> <li>(a)</li> <li>(b)</li> <li>(c)</li> <li>(c)</li></ul>	Getting Started	User	Groups			
*	Administration	User	Groups Table			
۰	System Configuration					
	System			Web Logic /NETCONE/DESTCONE .	606-UDM *	Ext/DN/2rd Duras
	Time	_	Group +	Web Login/NETCONF/RESTCONF +	525-VPN +	EzvPlo/Sid Party +
			VPN	Disabled	Disabled	Clients
	Log	0	admin	Admin	Disabled	Disabled
	Email	0	quest	Disabled	Disabled	Disabled
	User Accounts					
	User Groups					

#### 手順 13

次に、[System Configuration] > [User Accounts]で新しいユ**ーザを**設定**します**。[+]をクリ**ックして** 新しいユーザーを作成します。



#### 新しいユーザー**名と新**しいパスワードを**入力します**。グループが、構成した新**しいユー**ザーグル ープに設定されてい**ることを**確認してください。最後に、[Apply] をクリックします

User Accounts	User Accounts					
Add User Acc	ount					
User Name	vpnuser					
New Password		( Range: 0 - 127 )				
New Password Confirm						
Group	VPN •	]				

## ステップ 15

#### 新しいユー**ザーが**ローカルユーザーのリストに**表示されます**。

ocai Use	er Membersnip List		
+	User Name 🗢	Group * 🗢	
0 1	cisco	admin	
0 2	guest	guest	
3	vpnuser	VPN	

これで、RV340シリーズルータの設定は完了です。次に、Shrew Soft VPN Clientを設定します。

## ShrewSoft VPNクライアントの設定

次に、Shrew Soft VPN Clientを設定します。

#### 手順 1

ShrewSoft VPN Access Managerを開き、Addをクリックしてプロファイルを追加します。表示される[VPN Site Configuration]ウィンドウでGeneralタブを設定します。

ホスト名またはIPアドレス:WAN IPアドレス(またはRV340のホスト名)を使用する

自動設定:ike config pullを選択します

アダプタモード:[仮想アダプタと割り当てられたアドレスを使用する]を選択します

VPN Site Configuration	x				
General Client Name Resolution Authentication P					
Remote Host Host Name or IP Address 192.168.75.113 Auto Configuration ike config pull					
Adapter Mode Use a virtual adapter and assigned address					
MTU Obtain Automatically 1380 Address Netmask					
Save Cancel					

[クライアント]**タブを設**定します。ここでは、デフォルト設定だけを使用します。

VPN Site Configuration						
General Client Name Resolution	• •					
Firewall Options						
NAT Traversal	enable 🔻					
NAT Traversal Port	450					
Keep-alive packet rate	15 Secs					
IKE Fragmentation	•					
Maximum packet size	540 Bytes					
Other Options						
Enable Dead Peer Detectio	n					
Enable ISAKMP Failure Noti	fications					
🔽 Enable Client Login Banner						
Save Cancel						

#### 手順 3

[名前解決]**タブ> [DNS]**タブで、[DNSを有効**にする]**ボックスをオン**にし**、[自動的に取得する]ボッ クスをオンのままにします。

VPN Site Configuration	X
General Client Name Resolution Authenticatio	n P 🔸 🕨
DNS WINS	
Enable DNS 📝 Obtain Automatica	lly
Server Address #1	
Server Address #2	
Server Address #3	
Server Address #4	
✓ Obtain Automatica DNS Suffix	
Save	Cancel

[Name Resolution]タブ> [WINS]タブで、[Enable WINS]ボックスにチェックマークを入れ、[ Obtain Automatically]ボックスをオンのままにします。

VPN Site Configuration				
General Client Name Resolution Authentication	P			
DNS WINS	_			
Enable WINS Obtain Automatically				
Server Address #1				
Server Address #2				
Save Car	icel			

#### 手順 5

[Authentication]タブ> [Local Identity]タブを設定します。

IDタイプ:キー識別子の選択

**キーID文字列**:RV34xで設定されたグループ名を入力します

VPN Site Configuration	X		
General Client Name Resolution Authentication	P • •		
Authentication Method Mutual PSK + XAuth	•		
Local Identity Remote Identity Credentials			
Identification Type			
Key Identifier 👻			
Key ID String	_		
Clients			
Save	ancel		

[Authentication]タブ> [Remote Identity]タブで、[Default]の設定を終了します。

IDタイプ:iSCSIポータルの

アドレス文字列:<blank>

**検出されたリモートホストアドレスボックスを使**用します。チェックボックスをオンにしま す。

VPN Site Configuration				
General Client Name Resolution Authentication P · · ·				
Authentication Method Mutual PSK + XAuth				
Local Identity Remote Identity Credentials				
Identification Type				
IP Address				
Address String				
Use a discovered remote host address				
Save Cancel				

#### ステップ7

[Authentication]タブ> [Credentials]タブで、次の項目を設定します。

Authentication Method: [相互PSK + XAuth]を選択します

Pre-Shared Key:RV340クライアント・プロファイルに設定されている事前共有キーを入力

VPN Site Configuration				
General Client Name Resolution Authentication P				
Authentication Method Mutual PSK + XAuth				
Local Identity Remote Identity Credentials				
Server Certificate Autority File				
Client Certificate File				
Client Private Key File				
Pre Shared Key				
Save Cancel				

[Phase 1]タブでは、デフォルト設定はそのままにします。

Exchange Type:アグレッシブ

DH交換: group 2

暗号アルゴリズム:自動

hash algorithm:自動

VPN Site Configuration				
Client Name Resolution A	uthentication Phase	e1 F 🔸		
Proposal Parameters				
Exchange Type	aggressive	-		
DH Exchange	group 2	-		
Cipher Algorithm	auto	-		
Cipher Key Length		lits		
Hash Algorithm	auto	-		
Key Life Time limit	86400 S	lecs		
Key Life Data limit	0 K	bytes		
Enable Check Point Compatible Vendor ID				
[	Save	Cancel		

[Phase 2]タブのデフォルトも使用します。

**変換アルゴリズム**:自動

HMAC Algorithm:自動

PFS交換: Disabled

#### **圧縮アルゴリズム**: Disabled

Name Resolution Authentic	ation Phase 1 Phase 2
Proposal Parameters	
Transform Algorithm	auto 🔹
Transform Key Length	Test Bits
HMAC Algorithm	auto 🔻
PFS Exchange	disabled 🔹
Compress Algorithm	disabled 🗸
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
	Save Cancel

#### 手順 10

[ポリシー]タブでは、次の設定を使用します。

ポリシー生成レベル:自動

永続的なセキュリティアソシエーションの管理:チェックボックスをオンにします。

トポロジを自動的に取得するか、[Tunnel All]:チェックボックスをオンにします。

RV340でSplit-Tunnelingを設定したため、ここで設定する必要はありません。



終了したら、[保存]をクリックします。

#### 手順 11

接続をテストする準備ができました。*VPN* Access Manager*で、接続プロフ*ァイルを強調表示し、[**Connect**]ボタンをクリ**ック**します。

O VPN Access Manager				
File Edit	View He	lp		
8	•	🤣 🖨		
Connect	Add N	Aodify Delete		
Connectio	n Name 🏒	Host Name	Authenticat	
ten 192.168	.75.113	192.168.75.113	mutual-psk	

ステップ 12

表示される[**VPN Connect**]ウィンドウで、RV340で作成した**ユーザアカウント**のクレデンシャル を使用して**ユーザ名**と**パスワードを入力します(ステップ13 & 14)。** 

VPN Connect	t - 192.168.75.113
Connect Netwo	rk
config log do d	(an aita 1100 100 7E 110)
coning loaded	tor site 132.166.75.115
I	
Credentials	
Username	vpnuser
Password	•••••
	Connect Exit

終了したら、[接続]をクリ**ックします**。

#### 手順 13

トンネルが接続されていることを確認します。トンネルが有効になっているはずです。

VPN Connect	t - 192.168.75.113		X
Connect Netwo	ırk		
local id config remote id conf pre-shared ke bringing up tur network device tunnel enabled	ured igured y configured inel e configured		•
Credentials			
Username	vpnuser		
Password			
	Disconnect	Cancel	

# 結論

これで、VPNを介してネットワークに接続するようにセットアップされました。