Shrew Soft VPN Clientを使用したRV130および RV130W上のIPSec VPNサーバとの接続

目的

IPSec VPN(バーチャルプライベートネットワーク)を使用すると、インターネット上に暗 号化されたトンネルを確立して、リモートリソースを安全に取得できます。

RV130およびRV130WはIPSec VPNサーバとして動作し、Shrew Soft VPNクライアントを サポートします。

クライアントソフトウェアの最新リリースをダウンロードしてください。

Shrew Soft(<u>https://www.shrew.net/download/vpn</u>)

注: IPSec VPNサーバを使用してShrew Soft VPN Clientを正常にセットアップおよび設定で きるようにするには、まずIPSec VPNサーバを設定する必要があります。この方法の詳細に ついては、『<u>RV130およびRV130WでのIPSec VPNサーバの設定</u>』を参照してください。

このドキュメントの目的は、Shrew Soft VPN Clientを使用してRV130およびRV130W上の IPSec VPNサーバに接続する方法を示すことです。

該当するデバイス

- ・ RV130W Wireless-N VPNファイアウォール
- ・ RV130 VPNファイアウォール

システム要件

- ・ 32または64ビットシステム
- ・ Windows 2000、XP、VistaまたはWindows 7/8

トポロジ

次に、ShareSoftのクライアントとサイト間の設定に関係するデバイスを示すトップレベル トポロジを示します。



小規模企業のネットワーク環境におけるDNSサーバの役割を示すより詳細なフローチャートを次に示します。



[Software Version]

•1.0.1.3

Shrew Soft VPN Clientのセットアップ

IPSec VPNのセットアップとユーザ設定

ステップ1:Web設定ユーティリティにログインし、[VPN] > [IPSec VPN Server] > [Setup] を 選択します。[Setup] ページが開きます。

Setup		
Server Enable:		
NAT Traversal:	Disabled Edit	
Phase 1 Configuration		
Pre-Shared Key:	Testkey]
Exchange Mode:	Main 👻	
Encryption Algorithm:	DES 🗸	
Authentication Algorithm:	MD5 👻	
DH Group:	Group1 (768 bit) 👻	
IKE SA Life Time:	3600	Seconds (Range: 30 - 86400, Default: 3600)
Phase 2 Configuration		
Local IP:	Subnet 👻	
IP Address:	192.168.1.0	(Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)
IPSec SA Lifetime:	28800	Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	DES 👻	
Authentication Algorithm:	MD5 🗸	
PFS Key Group:	Enable	
DH Group:	Group 1(768 bit) 👻	
Save Cancel		

<u>ステップ2:</u>RV130のIPSec VPNサーバが正しく設定されていることを確認します。IPSec VPNサーバが設定されていない、または誤って設定されている場合は、『<u>RV130および</u> <u>RV130WでのIPSec VPNサーバの設定</u>』を参照し、[Save] をクリックします。

Cature		
Setup		
Conliguration setti	ings have been saved successiony	
Server Enable:		
NAT Traversal:	Disabled Edit	
Phase 1 Configuration		
Pre-Shared Key:	Testkey	
Exchange Mode:	Main 👻	
Encryption Algorithm:	DES -	
Authentication Algorithm:	MD5 -	
DH Group:	Group1 (768 bit) -	
IKE SA Life Time:	3600 Seconds (Range: 30 - 86400, Default: 3600)	
Phase 2 Configuration		
Local IP:	Subnet -	
IP Address:	192.168.1.0 (Hint: 1.2.3.4)	
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)	
IPSec SA Lifetime:	28800 Seconds (Range: 30 - 86400, Default: 28800)	
Encryption Algorithm:	DES -	
Authentication Algorithm:	MD5 -	
PFS Key Group:	Enable	
DH Group:	Group 1(768 bit) -	
Save Cancel		

注:上記の設定は、RV130/RV130W IPSec VPNサーバの設定例です。設定は、ドキュメン ト『<u>*RV130およびRV130WでのIPSec VPNサーバの設定*</u>』に基づいており、以降の手順で参 照します。

ステップ3:[VPN] > [IPSec VPN Server] > [User] に移動します。[User] ページが表示されます。

User		
User Account Table		
🔲 UserName	Password	
No data to display		
Add Row Edit Delete Im	port	
Save Cancel		

<u>ステップ4:[</u>Add Row] をクリックしてユーザアカウントを追加し、VPNクライアントの認証 (拡張認証)に使用して、表示されるフィールドに必要なユーザ名とパスワードを入力しま す。

User		
You must save before you can edit or delete.		
User Account Table		
UserName	Password	
TestUser	•••••	
Add Row Edit Delete Import		
Save Cancel		

ステップ5:[Save] をクリックして設定を保存します。

VPN Client の設定

ステップ1:Share 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。



[VPN Site Configuration] ウィンドウが表示されます。

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host
Host Name or IP Address Port
Auto Configuration ike config pull 🔻
Local Host
Adapter Mode
Use a virtual adapter and assigned address 💌
MTU 👽 Obtain Automatically
1380 Address
Netmask
Save Cancel

ステップ2:[General] タブの[Remote Host] セクションで、接続するネットワークのパブリッ クホスト名またはIPアドレスを入力します。

VPN Site Configuration
General Client Name Resolution Authenticatic
Remote Host
Host Name or IP Address Port
Auto Configuration like configinul
Local Host
Adapter Mode
Use a virtual adapter and assigned address 🔻
MTU 👽 Obtain Automatically
1380 Address
Netmask
Save Cancel

注:ポート番号がデフォルト値の500に設定されていることを確認します。VPNが機能する には、トンネルはUDPポート500を使用します。このポートは、ISAKMPトラフィックがフ ァイアウォールで転送されるように設定する必要があります。

ステップ3:[Auto Configuration] ドロップダウンリストで、[disabled] を選択します。

VPN Site Configuration		
General Client Name Res	solution Authenticatic	
Remote Host		
Host Name or IP Address	Port	
12114128	500	
Auto Configuration	ike config pull 🚽	
CLocal Host	ike config pull	
Adapter Mode	ke config push dhcp over ipsec	
Use a virtual adapter and	l assigned address 🔻	
MTU	Obtain Automatically	
1380 Address		
Netmask		
C	Save Cancel	

使用可能なオプションは次のように定義されています。

・ Disabled:自動クライアント設定を無効にします。

・ IKE Config Pull:クライアントによるコンピュータからの設定要求を許可します。コン ピュータによるPullメソッドのサポートにより、要求はクライアントがサポートする設定 のリストを返します。

・ IKE Config Push:設定プロセスを通じて設定をクライアントに提供する機会をコンピ ュータに与えます。コンピュータによるPushメソッドのサポートにより、要求はクライア ントがサポートする設定のリストを返します。

・ DHCP Over IPSec : クライアントがDHCP over IPSecを使用してコンピュータに設定 を要求できるようにします。

ステップ4:[Local Host] セクションで、[Adapter Mode] ドロップダウンリストから[Use an existing adapter and current address] を選択します。

VPN Site Configuration		
General Client Name Resolution Authenticatic		
Remote Host		
Host Name or IP Address Port		
Auto Configuration disabled		
Adapter Mode		
Use a virtual adapter and assigned address 🔻		
Use a virtual adapter and assigned address Use a virtual adapter and random address		
Use an existing adapter and current address		
Netmask		
Save Cancel		

使用可能なオプションは次のように定義されています。

・仮想アダプタと割り当てられたアドレスを使用する:クライアントが、指定されたアド レスをIPsec通信の送信元とする仮想アダプタを使用できるようにします。

・ Use a virtual adapter and random address: クライアントが、ランダムアドレスを持つ 仮想アダプタをIPsec通信の送信元として使用できるようにします。

・既存のアダプタと現在のアドレスを使用する:現在のアドレスをIPsec通信の送信元と する既存の物理アダプタのみをクライアントが使用できるようにします。

ステップ5:[Client] タブをクリックします。[NAT Traversal] ドロップダウンリストで、『 <u>RV130およびRV130WでのIPSec VPNサーバの設定</u>』のNATトラバーサル用に RV130/RV130Wで設定したものと同じ設定を選択します。

VPN Site Configuration		
General Client Name Resolut	tion Authenticatic	
Firewall Options		
NAT Traversal	disable 🔹 🗸	
NAT Traversal Port	disable enable	
Keep-alive packet rate	force-draft	
IKE Fragmentation	force-cisco-udp	
	540 p	
Maximum packet size	540 Bytes	
Other Options		
Enable Dead Peer Detection		
Enable ISAKMP Failure Notifications		
Enable Client Login Banner		
Save Cancel		

使用可能なNetwork Address Translation Traversal(NATT)メニューオプションは、次のよう に定義されています。

・ Disable:NATプロトコル拡張は使用されません。

・ Enable:NATプロトコル拡張は、ネゴシエーション中にVPNゲートウェイがサポートを 示し、NATが検出された場合にのみ使用されます。

・ Force-Draft:VPNゲートウェイがネゴシエーション中にサポートを示すか、NATが検出 されるかにかかわらず、NATプロトコル拡張のドラフトバージョンが使用されます。

・ Force-RFC:NATプロトコルのRFCバージョンは、VPNゲートウェイがネゴシエーショ ン中のサポートを示すか、NATが検出されるかにかかわらず使用されます。

・ Force-Cisco-UDP:NATを使用しないVPNクライアントのUDPカプセル化を強制します。

ステップ6:DNSを有効にする場合は、[Name Resolution] タブをクリックし、[Enable DNS] チェックボックスをオンにします。サイト設定に特定のDNS設定が必要ない場合は、 [Enable DNS] チェックボックスをオフにします。

VPN Site Configuration		
Client Name Resolution	Authentication Phase	
DNS Split DNS WI	NS	
Enable DNS	Obtain Automatically	
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
DNS Suffix	Obtain Automatically	
	Save Cancel	

ステップ7(オプション)リモートゲートウェイがConfiguration Exchangeをサポートする ように設定されている場合、ゲートウェイは自動的にDNS設定を提供できます。そうでな い場合は、[Obtain Automatically] チェックボックスがオフになっていることを確認し、有効 なDNSサーバアドレスを手動で入力します。

VPN Site Configuration		
Client Name Resolution Authentication Phase		
DNS WINS		
🛛 🖾 Enable DNS 🔹 💿 Obtain Automatically		
Server Address #1		
Server Address #2		
Server Address #3		
Server Address #4		
Obtain Automatically DNS Suffix		
	-	
Save Car	ncel	

ステップ8:(オプション)Windows Internet Name Server(WINS)を有効にするには、[Name Resolution] タブをクリックし、[Enable WINS] チェックボックスをオンにします。 Configuration Exchangeをサポートするようにリモートゲートウェイが構成されている場合 、ゲートウェイは自動的にWINS設定を提供できます。そうでない場合は、[Obtain Automatically] チェックボックスがオフになっていることを確認し、有効なWINSサーバア ドレスを手動で入力します。

VPN Site Configuration	— X
Client Name Resolution	Authentication Phase
DNS Split DNS WI	NS
Enable WINS	Obtain Automatically
Server Address #1	
Server Address #2	
(Save Cancel

注:WINS構成情報を提供することにより、クライアントはリモートプライベートネットワ ークにあるサーバを使用してWINS名を解決できます。これは、Uniform Naming Conventionのパス名を使用してリモートWindowsネットワークリソースにアクセスしよう とする場合に便利です。WINSサーバは通常、Windowsドメインコントローラまたは Sambaサーバに属します。

ステップ9:[Authentication] タブをクリックし、[Authentication Method] ドロップダウンリス トで[Mutual PSK + XAuth] を選択します。

VPN Site Configuration	×
Client Name Resolution	Authentication Phase
Authentication Method	Mutual PSK + XAuth 🛛 🔻
Local Identity Remot	Hybrid RSA + XAuth Hybrid GRP + XAuth Mutual RSA + XAuth
Identification Type	Mutual PSK + XAuth
IP Address	Mutual RSA
Address String	local host address
	Save Cancel

使用可能なオプションは次のように定義されています。

・ RSAとXAuthのハイブリッド:クライアント・クレデンシャルは不要です。クライアン トはゲートウェイを認証します。クレデンシャルは、PEMまたはPKCS12証明書ファイル またはキーファイルタイプの形式になります。

 Hybrid GRP + XAuth: クライアントクレデンシャルは必要ありません。クライアント はゲートウェイを認証します。クレデンシャルは、PEMまたはPKCS12証明書ファイルと 共有秘密ストリングの形式になります。

・相互RSA + XAuth:クライアントとゲートウェイの両方が認証にクレデンシャルを必要 とする。クレデンシャルは、PEMまたはPKCS12証明書ファイルまたはキータイプの形式 になります。

・相互PSK + XAuth:クライアントとゲートウェイの両方が認証にクレデンシャルを必要 とする。クレデンシャルは、共有秘密ストリングの形式になります。

・相互RSA:クライアントとゲートウェイの両方が認証にクレデンシャルを必要とする。 クレデンシャルは、PEMまたはPKCS12証明書ファイルまたはキータイプの形式になりま す。

・双方向PSK:クライアントとゲートウェイの両方が認証のためにクレデンシャルを必要 とします。クレデンシャルは、共有秘密ストリングの形式になります。

ステップ10:[Authentication] セクションで、[Credentials] サブタブをクリックし、[IPsec VPN Server Setup] ページで設定したのと同じ事前共有キーを[Pre Shared Key] フィールド に入力します。

VPN Site Configuration
Client Name Resolution Authentication Phase
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

ステップ11:[Phase 1] タブをクリックします。このドキュメントの「<u>IPSec VPNサー/Ĭユー</u> <u>ザ設定</u>」セクションの<u>ステップ2で設定したRV130/RV130Wと同じ設定になるように、次の</u> <u>パラメータを設定します。</u>

VPN Site Configuration	×
Name Resolution Authent	ication Phase 1 Pha:
Proposal Parameters	
Exchange Type	main 🔻
DH Exchange	group 1 🔹
Cipher Algorithm	des 🔻
Cipher Key Length	- Bits
Hash Algorithm	md5 🔹
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Co	ompatible Vendor ID

Shrew Softのパラメータは、次のようにフェーズ1のRV130/RV130W設定と一致する必要があります。

- ・「Exchange Type」は「Exchange Mode」と一致する必要があります。
- ・「DH Exchange」は「DH Group」と一致している必要があります。
- ・暗号アルゴリズムは暗号アルゴリズムと一致すること。
- ・ハッシュアルゴリズムは認証アルゴリズムと一致する必要があります。

ステップ12:(オプション)フェーズ1ネゴシエーション中にゲートウェイがシスコ互換のベ ンダーIDを提供する場合は、[Enable Check Point Compatible Vendor ID] チェックボックス をオンにします。ゲートウェイが表示されない場合、または不明な場合は、チェックボック スをオフのままにします。

VPN Site Configuration	×
Name Resolution Authent	ication Phase 1 Pha:
Proposal Parameters	·
Exchange Type	main 🔻
DH Exchange	group 1 🔹
Cipher Algorithm	des 🔹
Cipher Key Length	Bits
Hash Algorithm	md5 🔹
Key Life Time limit	3600 Secs
Key Life Data limit	0 Kbytes
Enable Check Point Co	Save Cancel

ステップ13:[Phase 2] タブをクリックします。このドキュメントの「*IPSec VPNサー/Ĭユー <u>ザ設定</u>」セクションの<u>ステップ2で設定したRV130/RV130Wと同じ設定になるように、次の</u> <u>パラメータを設定します。</u>*

VPN Site Configuration	×
Authentication Phase 1 Phas	e 2 Policy
Proposal Parameters	-des
Transform Key Length	- Bits
HMAC Algorithm md	5 🔹
PFS Exchange gro	up 1 🚽
Compress Algorithm disa	abled 👻
Key Life Time limit 🧲	28800 Secs
Key Life Data limit	0 Kbytes
	ave Cancel

Shrew Softのパラメータは、次のようにフェーズ2のRV130/RV130W設定と一致する必要があります。

- ・「変換アルゴリズム」は「暗号化アルゴリズム」と一致する必要があります。
- ・「HMACアルゴリズム」は「認証アルゴリズム」と一致する必要があります。

・ RV130/RV130WでPFSキーグループが有効になっている場合、「PFS Exchange」は「 DH Group」と一致する必要があります。そうでない場合は、**disabled**を選択します。

・「Key Life Time limit」は「IPSec SA Lifetime」と一致する必要があります。

ステップ14:[Policy] タブをクリックし、[Policy Generation Level] ドロップダウンリストで [require] を選択します。[Policy Generation Level] オプションでは、IPSecポリシーが生成さ れるレベルを変更します。ドロップダウンリストに表示されるさまざまなレベルは、さまざ まなベンダーの実装によって実装されるIPSec SAネゴシエーション動作に対応します。

VPN Site Configuration	
Authentication Phase 1 Phase 2 Policy	
Add Modify Delete Save Cancel	

使用可能なオプションは次のように定義されています。

・ Auto:クライアントは適切なIPSecポリシーレベルを自動的に決定します。

 Require:クライアントは、ポリシーごとに一意のセキュリティアソシエーション (SA)をネゴシエートしません。ポリシーは、ローカルパブリックアドレスをローカルポリ シーIDとして使用し、リモートネットワークリソースをリモートポリシーIDとして使用し て生成されます。フェーズ2の提案では、ネゴシエーション中にポリシーIDを使用します 。

・ Unique : クライアントはポリシーごとに一意のSAをネゴシエートします。

・共有:ポリシーは必要なレベルで生成されます。フェーズ2の提案では、ネゴシエーション時に、ローカルポリシーIDをローカルIDとして使用し、Any(0.0.0.0/0)をリモートIDとして使用します。

ステップ15:[Obtain Topology Automatically or Tunnel All] チェックボックスをオフにします 。このオプションは、接続に対するセキュリティポリシーの設定方法を変更します。無効の 場合は、手動設定を実行する必要があります。有効にすると、自動設定が実行されます。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level
Maintain Persistent Security Associations
Dbtain Topology Automatically or Tunnel All
Remote Network Resource
Add Modify Delete
Save Cancel

ステップ16:[Add] をクリックして、接続先のリモートネットワークリソースを追加します。 リモートネットワークリソースには、リモートデスクトップアクセス、部門リソース、ネッ トワークドライブ、および安全な電子メールが含まれます。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy
IPSEC Policy Configuration
Policy Generation Level require 👻
Maintain Persistent Security Associations
Obtain Topology Automatically or Tunnel All
Remote Network Resource
Add Modify Delete
Save Cancel

[Topology Entry] ウィンドウが表示されます。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Policy Generation Level require Image: Configuration Type Include X Address . . Netmask . . Ok Cancel
Add Modify Delete
Save Cancel

ステップ17:[Address] フィールドに、RV130/RV130WのサブネットIDを入力します。この アドレスは、このドキュメントの「*IPSec VPNサーバのセットアップとユーザの設定*」セク ションの<u>ステップ2</u>にある「<u>IPアドレス</u>」フィールドと一致している必要があります。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Policy Generation Level require Vertice Type Include Vertice Address 192.168.1.0 Vertice Netmask . .
Add Modify Delete
Save Cancel

ステップ18:[Netmask] フィールドに、RV130/RV130Wのローカルネットワークのサブネッ トマスクを入力します。このネットマスクは、このドキュメントの「*IPSec VPNサーバユー ザ設定*」セクションの<u>ステップ2</u>の「<u>サブネットマスク</u>」フィールドと一致している必要が あります。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Policy Generation Level require Image: Configuration Topology Entry Image: Configuration Image: Configuration Type Include Image: Configuration Address 192.168.1.0 Image: Configuration Netmask (255.255.255.0) Image: Configuration
Add Modify Delete
Save Cancel

ステップ19:[OK] をクリックして、リモートネットワークリソースの追加を終了します。

VPN Site Configuration
Authentication Phase 1 Phase 2 Policy IPSEC Policy Configuration Policy Generation Level require Topology Entry Type Include Address 192.168.1.0 Netmask 255.255.255.0
Add Modify Delete
Save Cancel

ステップ20:[Save] をクリックして、VPNサイトに接続するための設定を保存します。

VPN Site Configuration					
Authentication Phase 1 Phase 2 Policy					
IPSEC Policy Configuration					
Policy Generation Level require 🔻					
Maintain Persistent Security Associations					
Obtain Topology Automatically or Tunnel All					
Remote Network Resource					
↔ 192.168.1.0 / 255.255.255.0					
Add Modify Delete					
Save Cancel					

ステップ21:[VPN Access Manager] ウィンドウに戻り、設定したVPNサイトを選択し、 [Connect] ボタンをクリックします。

(B) VPN Acc	ess Mar	nager			x
File Edit	View	Help			
Connect	C) Add	😕 Modify	elete		
B DEPKRE	н				
					н

[VPN Connect] ウィンドウが表示されます。

🐼 VPN Connect - 🚛 💷 💷 🔤 🔤 💌
Connect Network
config loaded for site
Credentials
Username
Password
Connect Exit

ステップ22:[Credentials] セクションで、このドキュメントの「<u>IPSec VPNサーバユーザ設</u> <u>定</u>」セクションの<u>ステップ4</u>で設定したアカウントのユーザ名とパスワードを入力します。

VPN Connect - Digital Title
Connect Network
config loaded for site ' 🖽 🛛 🖬 🖬 🖬 🖬 🕬
Credentials
Username TestUser
Password
Connect Exit

ステップ23:[Connect to VPN into the RV130/RV130W] をクリックします。

VPN Connect - 101114 71 H	J
Connect Network	
config loaded for site " 🖽 🖬 🖬 🖬 🖬	
Credentials	
Username TestUser	
Password •••••	
Connect Exit	

IPSec VPNトンネルが確立され、VPNクライアントはRV130/RV130W LANの背後にあるリ ソースにアクセスできます。

🐼 VPN Connect - 101011411111 🗖 🗖 💌 🗙
Connect Network
esp proposal configured client configured local id configured remote id configured pre-shared key configured bringing up tunnel
Credentials
Username TestUser
Password
Connect Cancel



この記事に関連するビデオを見る...

シスコのその他の技術に関する講演を表示するには、ここをクリックしてください。

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。