# RV016、RV042、RV042G、およびRV082 VPNルータでのMac OS向けQuick VPNの代替ソ リューションの導入

#### 目的

Mac OSに適したQuick VPNバージョンはありません。ただし、Mac OS用のQuick VPNの代替を導入したいと考えるユーザが増えています。この記事では、Quick VPNの代替として IPセキュリティを使用します。

注:設定を開始する前に、MAC OSにIPセキュリティをダウンロードしてインストールする 必要があります。次のリンクからダウンロードできます。

http://www.lobotomo.com/products/IPSecuritas/

この記事では、Mac OS用のQuick VPNの代替をRv016、RV042、RV042G、およびRV082 VPNルータに導入する方法について説明します。

## 適用可能なデバイス

- RV016
- RV042
- · RV042G
- RV082

#### [Software Version]

• v4.2.2.08

## Mac OS用のQuick VPNの代替を導入する

注:デバイスのVPN Clientからゲートウェイへの設定を最初に行う必要があります。VPN Clientをゲートウェイに設定する方法の詳細については、『RV016、RV042、RV042G、お よびRV082 VPNルータでのVPN Client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)の設定』を参照してください。

ステップ1:Mac OSでIPセキュリティを実行します。IPSecuritasウィンドウが表示されます。

000	IPSecuritas
Profile: Default :	
IPSec inactive	
Stop Start	

ステップ 2 : [Start(スタート)] をクリックします。

1	IPSecuritas	File	Edit	Connections	Certificates	Window	Help
00	0			Edit Connec	tions	жЕ)	
				Import Export Export Wiza	仓 rd Template	жі же	
				Protect Unprotect			
				Edit Profiles		жP	
Profil IPSec	le: Default inactive Stop		Start	÷			

ステップ 3:メニューバーから、Connections > Edit Connectionsの順に選択します。 Connectionsウィンドウが表示されます。

00	Connections
Connections	General Phase 1 Phase 2 ID DNS Options
	Remote IPSec Device:       Local Side   Prefer IPv6 Address
	Endpoint Mode:
	Remote Side
	Endpoint Mode:
+**1□ - 코 더 ≞ ≞	

ステップ4:+アイコンをクリックして、新しい接続を追加します。

● ○ ○	Connections				
Connections	General Phase 1 Phase 2 ID DNS Options				
ExampleConnection	Remote IPSec Device:     192.168.1.1       Local Side     Prefer IPv6 Address				
	Endpoint Mode: IP Address (optional): Host ‡				
	Remote Side				
	Endpoint Mode: Network Address:				
	Network + 192.168.1.0				
+**0-90-	Network Mask (CIDR): 24				

ステップ 5:connectionsの下に新しい接続の名前を入力します。

0 0	Connections
Connections ExampleConnection	General       Phase 1       Phase 2       ID       DNS       Options         Remote IPSec Device:       192.168.1.1         Local Side       Prefer IPv6 Address         Endpoint Mode:       IP Address (optional):         Host       ‡         Remote Side
+ * <sup>†</sup> 🗗 – 된 더 🖴 🖴	Endpoint Mode:       Network Address:         Network ‡       192.168.1.0         Network Mask (CIDR):       24

ステップ1: [General]タブをクリックします

ステップ 2: Remote IPSec DeviceフィールドにリモートルータのIPアドレスを入力します。

注:この設定はリモートクライアント用であるため、ローカル側を設定する必要はありません。リモートモードを設定するだけです。

ステップ 3: Remote Side領域で、Endpoint ModeドロップダウンリストからNetworkを選択します。

ステップ 4: Network Mask (CIDR)フィールドにサブネットマスクを入力します。

ステップ 5: Network Addressフィールドにリモートネットワークアドレスを入力します。

フェーズ 1

フェーズ1は、トンネルの両端の間のシンプレックスの論理セキュリティアソシエーション (SA)で、セキュアな認証通信をサポートします。

0 0	Connections	
Connections ExampleConnection	General Phase 1 Phase 2 ID DNS Options	
	Lifetime: 2880 Seconds ‡	
	DH Group: 1024 (2) ‡	
	Encryption: DES \$	
	Authentication: SHA-1 ‡	
	Exchange Mode: Main +	
	Proposal Check: Obey ‡	
	Nonce Size: 16	
+**10 - 9 6 8 2		

ステップ1: Phase 1タブをクリックします。

ステップ 2:トンネルの設定時に入力したライフタイムをLifetimeフィールドに入力します 。時間が経過すると、新しいキーが自動的に再ネゴシエートされます。キーのライフタイム は1081 ~ 86400秒の範囲です。Phase 1のデフォルト値は28800秒です。

ステップ3:Lifetimeドロップダウンリストから、Lifetimeに適切な時間単位を選択します。 デフォルトは秒です。

ステップ 4 : DH Groupドロップダウンリストから、トンネルの設定に入力したものと同じ DHグループを選択します。Diffie-Hellman(DH)グループは、キー交換に使用されます。

ステップ 5:トンネルの設定用に入力した暗号化タイプをEncryptionドロップダウンリスト から選択します。暗号化方式は、Encapsulating Security Payload(ESP)パケットの暗号化/復 号化に使用されるキーの長さを決定します。

手順 6: Authenticationドロップダウンリストから、トンネル設定に入力した認証方式を選 択します。認証のタイプによって、ESPパケットを認証する方法が決まります。

手順7:Exchange Modeドロップダウンリストから適切なExchangeモードを選択します。

・ Main:完全修飾ドメイン名(FQDN)以外のすべてのタイプのゲートウェイのExchangeモードを表します。

・アグレッシブ:完全修飾ドメイン名(FQDN)ゲートウェイの交換モードを表します。

フェーズ 2

フェーズ2は、データパケットが2つのエンドポイントを通過する間のデータパケットのセキュリティを決定するセキュリティアソシエーションです。

$\Theta \circ \circ$	Connections	
Connections ExampleConnection	GeneralPhase 1PhasLifetime:2880PFS Group:1024 (2)	e 2 ID DNS Options Seconds ‡
+ ***	Encryption: DES 3DES AES 256 AES 192 AES 128 Blowfish Cast 128	Authentication: HMAC MD5 HMAC SHA-1 HMAC SHA-256 HMAC SHA-384 HMAC SHA-512 Null

ステップ1: Phase 2タブをクリックします。

ステップ2:トンネルの設定とフェーズ1で入力したライフタイムをLifetimeフィールドに入力します。

ステップ3:トンネルとフェーズ1の設定で入力したライフタイムの同じ時間単位を、 Lifetimeドロップダウンリストから選択します。

ステップ 4:トンネルの設定用に入力したPerfect Forwarding Secrecy(PFS)Groupドロップ ダウンリストから、同じDHグループを選択します。

ステップ 5:使用されていないすべての暗号化方式と認証方式のチェックマークをはずします。Phase 1タブで定義されているものだけにチェックマークを付けます。

00	Connections
Connections	Connections         General       Phase 1       Phase 2       D       DNS       Options         Local Identifier:       Address       \$         Remote Identifier:       Address       \$         Authentication Method:       Preshared Key       \$
+ *** 🗇 - 코 더 🖴 🖴	Preshared Key:

ステップ1: IDタブをクリックします。

ステップ 2:Local Identifierドロップダウンリストから、トンネルと同じローカルID方式を 選択します。必要に応じて、ローカルIDのタイプに応じて適切な値を入力します。

ステップ 3: Remote Identifierドロップダウンリストから、トンネルと同じリモートID方式 を選択します。 必要に応じて、リモートIDのタイプに応じて適切な値を入力します。

ステップ4: Authentication Methodドロップダウンリストから、トンネルと同じ認証方式を 選択します。必要に応じて、認証方式のタイプに応じて適切な認証値を入力します。

ステップ 5 : xアイコン(赤い円)をクリックして、接続ウィンドウを閉じます。設定が自動的に保存されます。IPSecuritasウィンドウが表示されます。

Connection

000	IPSec	curitas	
[Fuermale Connection]			
ExampleConnection			
Profile: Default	\$		
IPSec inactive			
Stop	Start		

ステップ1:IPSecuritasウィンドウで、Startをクリックします。その後、ユーザはVPNに アクセスするために接続されます。 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。