

RV016、RV042、RV042G、およびRV082 VPNルータでのゲートウェイ間VPNの詳細設定

目的

仮想プライベートネットワーク(VPN)は、パブリックネットワークを介してリモートユーザのデバイスを仮想的に接続してセキュリティを提供するために使用されるプライベートネットワークです。具体的には、ゲートウェイ間VPN接続では、2台のルータを安全に相互に接続し、一方の端のクライアントが論理的にもう一方の端の同じリモートネットワークの一部であるように見せることができます。これにより、データとリソースをインターネット経由でより簡単かつ安全に共有できます。ゲートウェイ間VPN接続を正常に確立するには、接続の両側で同じ設定を行う必要があります。

ゲートウェイ間VPNの高度な設定により、VPNトンネルのオプションの設定を柔軟に行うことができ、VPNユーザにとってより使いやすくなります。詳細オプションは、事前共有キーモードのIKEでのみ使用できます。詳細設定は、VPN接続の両側で同じである必要があります。

このドキュメントの目的は、RV016、RV042、RV042G、およびRV082 VPNルータでゲートウェイ間VPNトンネルの詳細設定を行う方法を説明することです。

注：ゲートウェイVPNへのゲートウェイの設定方法の詳細については、『[RV016、RV042、RV042G、およびRV082 VPNルータでのゲートウェイVPNへのゲートウェイの設定](#)』を参照してください。

適用可能なデバイス

- RV016
- RV042
- RV042G
- RV082

[Software Version]

- v4.2.2.08

ゲートウェイ間VPNの詳細設定

ステップ 1：ルータ設定ユーティリティにログインし、VPN > Gateway To Gatewayの順に選択します。Gateway To Gatewayページが開きます。

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Local Group Setup

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

Remote Group Setup

Remote Security Gateway Type :

:

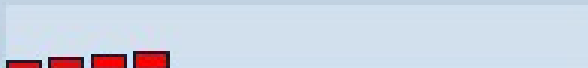
Remote Security Group Type :

IP Address :

Subnet Mask :

ステップ 2：IPSec Setupセクションまでスクロールして、Advanced +をクリックします。Advanced領域が表示されます。

IPSec Setup

Keying Mode :	IKE with Preshared key	▼
Phase 1 DH Group :	Group 1 - 768 bit	▼
Phase 1 Encryption :	DES	▼
Phase 1 Authentication :	MD5	▼
Phase 1 SA Life Time :	28800	seconds
Perfect Forward Secrecy :	<input checked="" type="checkbox"/>	
Phase 2 DH Group :	Group 1 - 768 bit	▼
Phase 2 Encryption :	DES	▼
Phase 2 Authentication :	MD5	▼
Phase 2 SA Life Time :	3600	seconds
Preshared Key :	abcd1234	
Minimum Preshared Key Complexity :	<input checked="" type="checkbox"/>	Enable
Preshared Key Strength Meter :		

Advanced +

Save

Cancel

ステップ 3 : ネットワーク速度が低い場合は、Aggressive Modeチェックボックスにチェックマークを付けます。これにより、SA接続 (フェーズ1) 中にトンネルのエンドポイントのIDがクリアテキストで交換されます。交換に要する時間は短くなりますが、安全性は低下します。

ステップ 4 : IPデータグラムのサイズを圧縮する場合は、Compress (Support IP Payload

Compression Protocol (IPComp))チェックボックスにチェックマークを付けます。IPCompは、IPデータグラムのサイズを圧縮するために使用されるIP圧縮プロトコルです。IP圧縮は、ネットワーク速度が遅く、ユーザが低速ネットワークを通じてデータを損失することなく迅速に送信したい場合に便利ですが、セキュリティは提供されません。

ステップ 5 : VPNトンネルの接続を常にアクティブのままにしておく場合は、Keep-Aliveチェックボックスにチェックマークを付けます。キープアライブを使用すると、接続が非アクティブになった場合に、接続を即座に再確立できます。

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm MD5 ▼

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval seconds

Tunnel Backup :

Remote Backup IP Address :

Local Interface : WAN1 ▼

VPN Tunnel Backup Idle Time : seconds (Range:30~999 sec)

Split DNS :

DNS1 :

DNS2 :

Domain Name 1 :

Domain Name 2 :

Domain Name 3 :

Domain Name 4 :

手順 6 : 認証ヘッダー(AH)を有効にする場合は、AH Hash Algorithmチェックボックスをオンにします。AHは、発信元データに対する認証、チェックサムによるデータ整合性、およびIPヘッダーへの保護を提供します。トンネルの両側で同じアルゴリズムを使用する必要があります。

- ・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算によって悪意のある攻撃からデータを保護する128桁の16進数ハッシュ関数です。
- ・ SHA1:Secure Hash Algorithm(SHA)バージョン1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm MD5 ▼
MD5
SHA1

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval seconds

Tunnel Backup :

Remote Backup IP Address :

Local Interface : ▼

VPN Tunnel Backup Idle Time : seconds (Range:30~999 sec)

Split DNS :

DNS1 :

DNS2 :

Domain Name 1 :

Domain Name 2 :

Domain Name 3 :

Domain Name 4 :

手順 7 : VPNトンネル経由でルーティング不可能なトラフィックを許可するには、NetBIOS Broadcastチェックボックスをオンにします。デフォルトはオフです。NetBIOSは、一部のソフトウェアアプリケーションやNetwork NeighborhoodなどのWindows機能を介して、ネットワーク内のプリンタやコンピュータなどのネットワークリソースを検出するために使用されます。

ステップ 8 : パブリックIPアドレスを介してプライベートLANからインターネットにアクセスする場合は、NAT Traversalチェックボックスにチェックマークを付けます。VPNルータがNATゲートウェイの背後にある場合は、このチェックボックスをオンにしてNATトラバーサルを有効にします。トンネルの両端で同じ設定が必要です。

ステップ 9 : Dead Peer Detection Intervalをチェックして、HelloまたはACKを介したVPNトンネルの存続可能性を定期的にチェックします。このチェックボックスをオンにした場合は、helloメッセージ間の間隔 (秒単位) を入力します。

注 : Dead Peer Detection Intervalをチェックしない場合は、ステップ11に進みます。

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds
- Tunnel Backup :
 - Remote Backup IP Address :
 - Local Interface :
 - VPN Tunnel Backup Idle Time : seconds (Range:30~999 sec)
- Split DNS :
 - DNS1 :
 - DNS2 :
 - Domain Name 1 :
 - Domain Name 2 :
 - Domain Name 3 :
 - Domain Name 4 :

ステップ 10 : トンネルバックアップをイネーブルにするには、Tunnel Backupチェックボックスにチェックマークを付けます。この機能は、Dead Peer Detection Intervalがチェックされている場合にのみ使用できます。この機能により、デバイスは代替ローカルWANインターフェイスまたはリモートIPアドレスを介してVPNトンネルを再確立できます。

- ・ Remote Backup IP Address : リモートゲートウェイの代替IPアドレスを入力するか、このフィールドにすでに設定されているWAN IPアドレスを入力します。
- ・ ローカルインターフェイス : 接続の再確立に使用されるWANインターフェイス。ドロップダウンリストから目的のインターフェイスを選択します。
- ・ VPNトンネルバックアップのアイドル時間 : バックアップトンネルが使用される前にプライマリトンネルが接続する必要がある時間 (秒) を入力します。

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds
- Tunnel Backup :
 - Remote Backup IP Address :
 - Local Interface :
 - VPN Tunnel Backup Idle Time : seconds (Range:30~999 sec)
- Split DNS :
 - DNS1 :
 - DNS2 :
 - Domain Name 1 :
 - Domain Name 2 :
 - Domain Name 3 :
 - Domain Name 4 :

ステップ 11 スプリットDNSを有効にするには、Split DNSチェックボックスにチェックマークを付けます。スプリットDNSでは、指定されたドメイン名に対する要求を、通常使用されるDNSサーバとは異なるDNSサーバで処理できます。ルータは、クライアントからDNS要求を受信すると、そのDNS要求をチェックしてドメイン名と照合し、その特定のDNSサーバに要求を送信します。

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm ▼

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval seconds

Tunnel Backup :

Remote Backup IP Address :

Local Interface : ▼

VPN Tunnel Backup Idle Time : seconds (Range:30~999 sec)

Split DNS :

DNS1 :

DNS2 :

Domain Name 1 :

Domain Name 2 :

Domain Name 3 :

Domain Name 4 :

ステップ 12DNS1フィールドにDNSサーバのIPアドレスを入力します。別のDNSサーバがある場合は、DNS2フィールドにDNSサーバのIPアドレスを入力します。

ステップ 13Domain Name 1 ~ Domain Name 4のフィールドにドメイン名を入力します。これらのドメイン名に対する要求は、手順12で指定したDNSサーバによって処理されます。

ステップ 14 : Saveをクリックして変更を保存します。

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。