

RV320およびRV325 VPNルータシリーズでの Group ClientからGateway Virtual Private Network(VPN)への設定

目的

バーチャルプライベートネットワーク(VPN)は、セキュリティを提供するために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するために使用されるプライベートネットワークです。VPNの種類の一つは、クライアントからゲートウェイへのVPNです。クライアントとゲートウェイを使用すると、地理的に異なるエリアにある会社の異なるブランチをリモートで接続して、エリア間のデータをより安全に送受信できます。グループVPNでは、各ユーザのVPNの設定が不要になるため、VPNの設定が簡単になります。RV32x VPNルータシリーズは、最大2つのVPNグループをサポートできます。

このドキュメントの目的は、RV32xシリーズVPNルータ(ISR)でゲートウェイVPNへのグループクライアントを設定する方法を説明することです。

該当するデバイス

- ・ RV320デュアルWAN VPNルータ
- ・ RV325ギガビットデュアルWAN VPNルータ

[Software Version]

- ・ v1.1.0.09

グループクライアントからゲートウェイVPNへの設定

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

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No.

1

Tunnel Name:

Interface:

WAN1

Keying Mode:

IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type:

IP Only

IP Address:

0.0.0.0

Local Security Group Type:

Subnet

IP Address:

192.168.1.0

Subnet Mask:

255.255.255.0

Remote Client Setup

Remote Security Gateway Type:

IP Only

IP Address

:

ステップ2:[Group VPN]ラジオボタンをクリックして、グループクライアントとゲートウェイ間のVPNを追加します。

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

注：グループ番号：グループの番号を表します。自動生成フィールドです。

ステップ2:[Interface]ドロップダウンリストから、VPNグループがゲートウェイに接続する適切なインターフェイスを選択します。

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

ステップ3:[Enable] チェックボックスをオンにして、ゲートウェイ間VPNを有効にします。デフォルトでは有効になっています。

Client to Gateway

Add a New Group VPN

Tunnel Group VPN Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

注：Keying Mode (キーイングモード)：使用される認証モードを表示します。事前共有キーを使用したIKEは唯一のオプションです。つまり、事前共有キーを自動的に生成して交換し、トンネルの認証済み通信を確立するために、Internet Key Exchange (IKE；インターネット鍵交換)プロトコルが使用されます。

ステップ4：これまでの設定を保存し、残りをデフォルトのままにするには、下にスクロールして[Save]をクリックして設定を保存します。

ローカルグループの設定

ステップ1:[ローカルセキュリティグループタイプ(Local Security Group Type)]ドロップダウンリストから、VPNトンネルにアクセスできる適切なローカルLANユーザまたはユーザグループを選択します。デフォルトは[Subnet]です。

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

Remote Client Setup

Remote Client: DomainName(FQDN)

Domain Name:

使用可能なオプションは次のように定義されます。

- ・ IP：特定の1つのLANデバイスだけがトンネルにアクセスできます。このオプションを選択した場合は、[IP Address]フィールドにLANデバイスのIPアドレスを入力します。デフォルトのIPは192.168.1.0です。
- ・ サブネット：特定のサブネット上のすべてのLANデバイスがトンネルにアクセスできます。このオプションを選択した場合は、LANデバイスのIPアドレスとサブネットマスクをそれぞれ[IP Address]フィールドと[Subnet Mask]フィールドに入力します。デフォルトマスクは255.255.255.0です。
- ・ IP範囲：さまざまなLANデバイスがトンネルにアクセスできます。このオプションを選択した場合は、範囲の最初と最後のIPアドレスをそれぞれ[Start IP]フィールドと[End IP]フィールドに入力します。デフォルトの範囲は192.168.1.0 ~ 192.168.1.254です。

ステップ2：これまでの設定を保存し、残りをデフォルトのままにするには、下にスクロールして[Save]をクリックして設定を保存します。

リモートクライアントの設定

ステップ1:[Remote Security Group Type]ドロップダウンリストから、VPNトンネルにアクセスできる適切なリモートLANユーザまたはユーザのグループを選択します。

Client to Gateway

Add a New Group VPN

Tunnel
 Group VPN
 Easy VPN

Group No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Group Type: IP

IP Address: 192.168.3.0

Remote Client Setup

Remote Client:
DomainName(FQDN)

DomainName(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

Domain Name:

使用可能なオプションは次のように定義されます。

- ・ ドメイン名(FQDN)認証：トンネルへのアクセスは、登録済みドメインを介して可能です。このオプションを選択した場合は、[ドメイン名]フィールドに登録済みドメインの名前を入力します。
- ・ E-mail Addr(USER FQDN)認証：トンネルへのアクセスは、電子メールアドレスを介して可能です。このオプションを選択した場合は、[電子メールアドレス]フィールドに電子メールアドレスを入力します。
- ・ Microsoft XP/2000 VPN Client:Microsoft XPまたは2000 VPN Clientソフトウェアが組み込まれているクライアントソフトウェアを使用して、トンネルにアクセスできます。

ステップ2：これまでの設定を保存し、残りをデフォルトのままにするには、下にスクロールして[Save]をクリックして設定を保存します。

IPSecの設定

ステップ1:[フェーズ1 DHグループ]ドロップダウンリストから適切なDiffie-Hellman (DH)グループを選択します。フェーズ1は、セキュアな認証通信をサポートするために、トンネルの両端の間にシプレックスの論理セキュリティアソシエーション(SA)を確立するために使用されます。Diffie-Hellmanは、フェーズ1接続で通信を認証するために秘密キーを共有するために使用される暗号キー交換プロトコルです。

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption :

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

使用可能なオプションは次のように定義されます。

- ・ Group1 (768ビット) : 最速でキーを計算しますが、最も安全ではありません。
- ・ Group2 (1024ビット) : キーの計算は遅くなりますが、Group1よりも安全です。
- ・ Group5 (1536ビット) : 最も遅いキーを計算しますが、最も安全です。

ステップ2:[Phase 1 Encryption]ドロップダウンリストから、キーを暗号化する適切な暗号化方法を選択します。AES-128は、高いセキュリティと高速なパフォーマンスを実現するために推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

使用可能なオプションは次のように定義されます。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) は56ビットの古い暗号化方式で、非常にセキュアな暗号化方式ではありませんが、後方互換性のために必要になる場合があります。
- ・ 3DES — Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、キーサイズを大きくするために使用される168ビットの簡単な暗号化方式です。これにより、DESよりもセキュリティが高くなりますが、AESよりもセキュリティが低くなります。
- ・ AES-128:128ビットキー(AES-128)を使用するAdvanced Encryption Standard(AES-128)では、AES暗号化に128ビットキーを使用します。AESはDESよりも高速で安全です。一般に、AESは3DESよりも高速で安全です。AES-128はAES-192およびAES-256よりも高速ですが、安全性は低くなります。
- ・ AES-192: AES-192では、AES暗号化に192ビットキーを使用します。AES-192は、AES-128よりも低速ですが、セキュアで、AES-256よりも高速ですが、セキュアではありません。
- ・ AES-256: AES-256は、AES暗号化に256ビットのキーを使用します。AES-256はAES-128およびAES-192よりも低速ですが、安全性は高くなります。

ステップ3:[Phase 1 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

使用可能なオプションは次のように定義されます。

- ・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算による悪意のある攻撃からデータを保護する128ビットハッシュ関数です。
- ・ SHA1 — Secure Hash Algorithm version 1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全です。

ステップ4:[Phase 1 SA Life Time]フィールドに、VPNトンネルがフェーズ1でアクティブなままである時間 (秒) を入力します。デフォルトの時間は28,800秒です。

Remote Client Setup

Remote Client:

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

ステップ5: (オプション) キーの保護を強化するには、[Perfect Forward Secrecy]チェックボックスをオンにします。このオプションを使用すると、キーが侵害された場合に新しいキーを生成できます。これは、セキュリティを強化するために推奨されるアクションです。

注：ステップ5で[Perfect Forward Secrecy]をオフにした場合、フェーズ2 DHグループを設定する必要はありません。

ステップ6:[Phase 2 DH Group]ドロップダウンリストから適切なDHグループを選択します。

IPSec Setup

Phase 1 DH Group: Group 2 - 1024 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: MD5

Phase 1 SA Lifetime: 2700 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit
Group 1 - 768 bit
Group 2 - 1024 bit
Group 5 - 1536 bit

Phase 2 Encryption:

Phase 2 Authentication: MD5

Phase 2 SA Lifetime: 3600 sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Advanced +

使用可能なオプションは次のように定義されます。

- ・ Group1 (768ビット) : 最速でキーを計算しますが、最も安全ではありません。
- ・ Group2 (1024ビット) : キーの計算は遅くなりますが、Group1よりも安全です。
- ・ Group5 (1536ビット) : 最も遅いキーを計算しますが、最も安全です。

ステップ2:[Phase 1 Encryption]ドロップダウンリストから、キーを暗号化する適切な暗号化方法を選択します。AES-128は、高いセキュリティと高速なパフォーマンスを実現するために推奨されます。VPNトンネルは、両端で同じ暗号化方式を使用する必要があります。

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

- DES
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

使用可能なオプションは次のように定義されます。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) は56ビットの古い暗号化方式で、非常にセキュアな暗号化方式ではありませんが、後方互換性のために必要になる場合があります。
- ・ 3DES — Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、キーサイズを大きくするために使用される168ビットの簡単な暗号化方式です。これにより、DESよりもセキュリティが高くなりますが、AESよりもセキュリティが低くなります。
- ・ AES-128:128ビットキー(AES-128)を使用するAdvanced Encryption Standard(AES-128)では、AES暗号化に128ビットキーを使用します。AESはDESよりも高速で安全です。一般に、AESは3DESよりも高速で安全です。AES-128はAES-192およびAES-256よりも高速ですが、安全性は低くなります。
- ・ AES-192: AES-192では、AES暗号化に192ビットキーを使用します。AES-192は、AES-128よりも低速ですが、セキュアで、AES-256よりも高速ですが、セキュアではありません。
- ・ AES-256: AES-256は、AES暗号化に256ビットのキーを使用します。AES-256はAES-128およびAES-192よりも低速ですが、安全性は高くなります。

ステップ8:[Phase 2 Authentication]ドロップダウンリストから適切な認証方式を選択します。VPNトンネルは、両端で同じ認証方式を使用する必要があります。

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

使用可能なオプションは次のように定義されます。

- ・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算による悪意のある攻撃からデータを保護する128ビットハッシュ関数を表します。
- ・ SHA1 — Secure Hash Algorithm version 1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。

ステップ9:[Phase 2 SA Lifetime]フィールドに、VPNトンネルがフェーズ2でアクティブなままである時間 (秒) を入力します。デフォルトの時間は3600秒です。

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:


Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

ステップ10: (オプション) 事前共有キーの強度メーターを有効にする場合は、[最小事前共有キーの複雑度]チェックボックスをオンにします。

注 : [Minimum Preshared Key Complexity]チェックボックスをオンにすると、[Preshared Key Strength Meter]に、色付きのバーを使用して事前共有キーの強度が表示されます。赤は弱い強度、黄色は許容される強度、緑は強い強度を示します。

ステップ11:[Preshared Key]フィールドに目的のキーを入力します。事前共有キーとして最大30個の16進数を使用できます。VPNトンネルは、両端で同じ事前共有キーを使用する必要があります。

注 : VPNが保護されるように、IKEピア間で事前共有キーを頻繁に変更することを強く推奨します。

ステップ12 : これまでの設定を保存し、残りをデフォルトのままにするには、下にスクロールして[Save]をクリックして設定を保存します。

高度な設定

ステップ1:[Advanced]をクリックして、詳細設定を構成します。

IPSec Setup

Phase 1 DH Group:

Phase 1 Encryption:

Phase 1 Authentication:

Phase 1 SA Lifetime: sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group:

Phase 2 Encryption:

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced +

[Advanced]領域に新しいフィールドが表示されます。

Phase 2 Authentication:

Phase 2 SA Lifetime: sec (Range: 120-28800, Default: 3600)

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm
- NetBIOS Broadcast
- NAT Traversal

ステップ2: (オプション) ネットワーク速度が低い場合、[アグレッシブモード]チェックボックスをオンにします。アグレッシブモードは、SA接続時にトンネルのエンドポイントのIDをクリアテキストで交換します。これにより、交換に必要な時間は短縮されますが、セキ

セキュリティは低下します。

ステップ3: (オプション) 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))]チェックボックスをオンにします。IPCompはIP圧縮プロトコルで、ネットワーク速度が低い場合や、ユーザがデータを損失なく迅速に送信したい場合に、IPデータグラムのサイズを圧縮するために使用されます。

ステップ4: (オプション) VPNトンネルの接続を常にアクティブのままにする場合は、[Keep-Alive]チェックボックスをオンにします。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。

ステップ5: (オプション) データの送信元への認証、チェックサムによるデータの整合性、およびIPヘッダーに拡張された保護を行う場合は、[AH Hash Algorithm]チェックボックスをオンにします。次に、ドロップダウンリストから適切な認証方式を選択します。トンネルの両側で同じアルゴリズムが必要です。

使用可能なオプションは次のように定義されます。

- ・ MD5:Message Digest Algorithm-5(MD5)は、チェックサム計算による悪意のある攻撃からデータを保護する128ビットハッシュ関数を表します。
- ・ SHA1 — Secure Hash Algorithm version 1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。

ステップ6:VPNトンネルを介してルーティング不能なトラフィックを許可する場合は、[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、ソフトウェアアプリケーションやネットワークネイバーフッドなどのWindows機能を介して、ネットワーク内のプリンタ、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7: (オプション) プライベートLANからパブリックIPアドレス経由でインターネットにアクセスする場合は、[NAT Traversal]チェックボックスをオンにします。NATトラバーサルは、内部システムのプライベートIPアドレスをパブリックIPアドレスとして認識させ、悪意のある攻撃や検出からプライベートIPアドレスを保護するために使用されます。

ステップ8:[Save]をクリックして、設定を保存します。