

RV320およびRV325 VPNルータシリーズでのシングルクライアントからゲートウェイへの仮想プライベートネットワーク(VPN)の設定

目的

このドキュメントの目的は、RV32xシリーズVPNルータのゲートウェイVirtual Private Network (VPN ; バーチャルプライベートネットワーク) への単一のクライアントの設定方法を示すことです。

概要

VPNは、パブリックネットワークを介してリモートユーザ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1つのタイプは、クライアントからゲートウェイへのVPNです。クライアントからゲートウェイへのVPNは、リモートユーザとネットワーク間の接続です。クライアントは、VPNクライアントソフトウェアを使用してユーザのデバイスで設定されます。ユーザは安全にネットワークにリモート接続できます。

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

単一クライアントからゲートウェイVPNへの設定

ステップ1: Web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:[Tunnel] オプションボタンをクリックして、クライアントの単一トンネルをゲートウェイVPNに追加します。

Client to Gateway

Add a New Tunnel

Tunnel

Group VPN

Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: ▼

Keying Mode: ▼

Enable:

Local Group Setup

Local Security Gateway Type: ▼

IP Address: 0.0.0.0

Local Security Group Type: ▼

IP Address:

Subnet Mask:

Remote Client Setup

Remote Security Gateway Type: ▼

▼ :

新しいトンネルの追加

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

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 :

注：トンネル番号：トンネルの番号を表します。この番号は自動的に生成されます。

ステップ1:[Tunnel Name]フィールドにトンネルの名前を入力します。

ステップ2:[Interface]ドロップダウンリストから、リモートクライアントがVPNにアクセスするインターフェイスを選択します。

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1
WAN1
WAN2
USB1
USB2

Keying Mode:

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

ステップ3:[キーイングモード(Keying Mode)]ドロップダウンリストから、適切なキー管理モードを選択し、セキュリティを確保します。デフォルトモードは、事前共有キーを使用したIKEです。

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key
Manual
IKE with Preshared key
IKE with Certificate

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

オプションは次のように定義されます。

- Manual – カスタムセキュリティモードを使用して、新しいセキュリティキーを自分で生成し、キーとのネゴシエーションを行いません。これは、トラブルシューティング時または小規模なスタティック環境で使用するのが最適です。
- 事前共有キーを使用したIKE：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。
- 証明書を使用したIKE：証明書を使用したインターネットキー交換(IKE)プロトコルは、事前共有キーを自動的に生成して交換し、トンネルに対してより安全な通信を確立するための、より安全な方法です。

ステップ4:[Enable] チェックボックスをオンにして、クライアントからゲートウェイへの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 Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No.

Tunnel Name:

Interface:

Keying Mode:

Enable:

Local Group Setup

Local Security Gateway Type:

Domain Name:

Local Security Group Type:

IP Address:

ステップ5：これまでの設定を保存する場合は、下にスクロールして[保存]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

手動または事前共有キーを使用したIKEによるローカルグループの設定

注：「新しいトンネルの追加」セクションのステップ3で、「Keying Mode」ドロップダウンリストから「Manual」または「IKE with Preshared key」を選択した場合は、次の手順に従います。

ステップ1:[Local Security Gateway]ドロップダウンリストから適切なルータ識別方法を選択し、VPNトンネルを確立します。

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: IP Only

IP Address:

Local Security Group Type:

IP Address:

Subnet Mask: 255.255.255.0

オプションは次のように定義されます。

- IP Only : トンネルへのアクセスは、スタティックWAN IPからのみ可能です。このオプションは、ルータだけにスタティックWAN IPがある場合に選択できます。スタティックWAN IPアドレスが自動的に生成されます。
- IP +ドメイン名(FQDN)認証 : トンネルへのアクセスは、スタティックIPアドレスと登録済みドメインを使用して可能です。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。スタティックWAN IPアドレスが自動的に生成されます。
- IP + E-mail Addr(USER FQDN)認証 : スタティックIPアドレスと電子メールアドレスを使用して、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、[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。スタティックWAN IPアドレスが自動的に生成されます。
- ダイナミックIP +ドメイン名(FQDN)認証 : ダイナミックIPアドレスと登録済みドメインを使用して、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、[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。
- ダイナミックIP + Eメールアドレス(USER FQDN)認証 : ダイナミックIPアドレスと電子メールアドレスを使用して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、[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。
- IPアドレス : WANインターフェイスのIPアドレスを表します。読み取り専用フィールドです。

ステップ2:[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の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 Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Preshared key

Enable:

Local Group Setup

Local Security Gateway Type: Dynamic IP + Domain Name(FQDN) Authentication

Domain Name: domain_1

Local Security Group Type: Subnet

IP Address:

Subnet Mask: 255.255.255.0

- 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：トンネルにアクセスできるLANデバイスの範囲。このオプションを選択した場合は、開始IPフィールドと終了IPアドレスをそれぞれ開始IPフィールドと終了IPアドレスに入力します。デフォルトの範囲は192.168.1.0 ~ 192.168.1.254です。

ステップ3：これまでの設定を保存する場合は、下にスクロールして[保存]をクリックして設定を保存します。

トンネルVPNの証明書を使用したIKEによるローカルグループの設定

注：「新しいトンネルの追加」セクションのステップ3のKeying ModeドロップダウンリストからCertificateを使用したIKEを選択した場合は、次の手順に従います。

Client to Gateway

Add a New Tunnel

Tunnel Group VPN Easy VPN

Tunnel No. 1

Tunnel Name:

Interface: ▼

Keying Mode: ▼

Enable:

Local Group Setup

Local Security Gateway Type: ▼

IP Address: 0.0.0.0

Local Certificate: ▼

Local Security Group Type: ▼

IP Address:

- ローカルセキュリティゲートウェイタイプ：証明書を使用してIPを介してトンネルにアクセスできます。
- IPアドレス：WANインターフェイスのIPアドレスを表します。読み取り専用フィールドです。

ステップ1:[Local Certificate]ドロップダウンリストから、ルータを識別する適切なローカル証明書を選択します。[セルフジェネレータ]をクリックして証明書を自動的に生成するか、[証明書のインポート]をクリックして新しい証明書をインポートします。

注：証明書を自動的に生成する方法の詳細については、「RV320ルータでの証明書の生成」を参照して、証明書のインポート方法については、「RV320ルータでの証明書の設定」を参照してください。

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

Interface: WAN1

Keying Mode: IKE with Certificate

Enable:

Local Group Setup

Local Security Gateway Type: IP + Certificate

IP Address: 0.0.0.0

Local Certificate: 01. Issuer: 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52

Local Security Group Type: IP

IP Address:

- IP
- IP
- Subnet
- IP Range

ステップ2:[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ローカルLANユーザまたはユーザグループの適切なタイプを選択します。デフォルトは[Subnet]です。

- 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、[IP Address]フィールドと[Subnet Mask]フィールドにそれぞれLANデバイスのIPアドレスとサブネットマスクを入力します。デフォルトマスクは255.255.255.0です。
- IP範囲：トンネルにアクセスできるLANデバイスの範囲。このオプションを選択した場合は、[Start IP]フィールドと[End IP]フィールドにそれぞれ開始IPアドレスと終了IPアドレスを入力します。デフォルトの範囲は192.168.1.0 ~ 192.168.1.254です。

ステップ3：これまでの設定を保存する場合は、下にスクロールして[保存]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

手動または事前共有キーを使用したIKEによるリモートクライアントのセットアップ

注：「新しいトンネルの追加」セクションのステップ3で、[キーイングモード]ドロップダウンリストから[Manual]または[IKE with Preshared Key]を選択した場合、次の手順に従います。

Client to Gateway

Add a New Tunnel

Tunnel
 Group VPN
 Easy VPN

Tunnel No. 1

Tunnel Name: tunnel_1

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: IP

IP Address: 192.168.2.1

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address :

- IP Only
- IP Only
- IP + Domain Name(FQDN) Authentication
- IP + Email Address(USER FQDN) Authentication
- Dynamic IP + Domain Name(FQDN) Authentication
- Dynamic IP + Email Address(USER FQDN) Authentication

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

ステップ1:[Remote Security Gateway]ドロップダウンリストから、VPNトンネルを確立するための適切なクライアント識別方法を選択します。デフォルトは[IP Only]です。

- IP Only : クライアントのスタティックWAN IPからのみ、トンネルへのアクセスが可能です。このオプションは、クライアントのスタティックWAN IPまたはドメイン名がわかっている場合にのみ選択できます。ドロップダウンリストから[IP Address]を選択し、隣接するフィールドにクライアントのスタティックIPを入力するか、ドロップダウンリストから[IP by DNS Resolved]を選択し、隣接するフィールドにIPアドレスのドメイン名を入力します。IPアドレスのローカルDNSサーバを介して、ルータはIPアドレスを自動的に取得できます。

注 : [Add a New Tunnel Through Tunnel or Group VPN]セクションのステップ3の [Keying Mode] ドロップダウンリストから [Manual]を選択した場合は、これが唯一のオプションです。

- IP +ドメイン名(FQDN)認証 : クライアントのスタティックIPアドレスと登録済みドメインを使用して、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、[Domain Name]フィールドに登録済みドメインの名前を入力します。ドロップダウンリストから[IP Address]を選択し、隣接するフィールドにクライアントのスタティックIPを入力するか、ドロップダウンリストから[IP by DNS Resolved]を選択し、隣接するフィールドにIPアドレスのドメイン名を入力します。IPアドレスのローカルDNSサーバを介して、ルータはIPアドレス

を自動的に取得できます。

- IP + E-mail Addr(USER FQDN)認証：クライアントのスタティックIPアドレスと電子メールアドレスを使用して、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、[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。ドロップダウンリストから[IPアドレス]を選択し、隣接フィールドにクライアントの静的IPを入力するか、ドロップダウンリストから[IP by DNS Resolved]を選択し、IPアドレスの名を入力します。IPアドレスのローカルDNSサーバを介して、ルータはIPアドレスを自動的に取得できます。
- ダイナミックIP + ドメイン名(FQDN)認証：クライアントのダイナミックIPアドレスと登録済みドメインを通じて、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、[Domain Name]フィールドに登録済みドメインの名前を入力します。
- ダイナミックIP + Eメールアドレス(USER FQDN)認証：クライアントのダイナミックIPアドレスと電子メールアドレスを介して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、[Email Address]フィールドに電子メールアドレスを入力します。

ステップ2：これまでの設定を保存する場合は、下にスクロールして[保存]をクリックして設定を保存します。

証明書を使用したIKEによるリモートグループセットアップ

注：「新しいトンネルの追加」セクションのステップ3でKeying Modeドロップダウンリストから証明書を使用したIKEを選択した場合は、次の手順に従ってください。

The screenshot shows a configuration interface with two main sections: "Local Group Setup" and "Remote Client Setup".

Local Group Setup:

- Local Security Gateway Type: IP + Certificate
- IP Address: 0.0.0.0
- Local Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52
- Buttons: Self-Generator, Import Certificate
- Local Security Group Type: Subnet
- IP Address: 192.168.3.1
- Subnet Mask: 255.255.255.0

Remote Client Setup (highlighted with a red box):

- Remote Security Gateway Type: IP + Certificate
- IP Address: 192.168.3.2
- Remote Certificate: 01. Issuer : 6c:20:56:c6:16:52 - Subject: 6c:20:56:c6:16:52
- Buttons: Import Remote Certificate, Authorize CSR

- Remote Security Gateway Type：クライアントの識別は、証明書を使用したIPを介してVPN接続を確立できます。

ステップ1：ドロップダウンリストから[IP Address]または[IP by DNS Resolved]を選択します。

- IPアドレス：クライアントのスタティックWAN IPからのみ、トンネルへのアクセスが可能です。このオプションは、クライアントのスタティックWAN IPがわかっている場合にのみ選択できます。[IP address]フィールドにクライアントの静的IPを入力します。
- IP By DNS Resolved – クライアントのIPアドレスがわからないが、そのIPアドレスのドメインがわかっている場合に便利です。IPアドレスのドメイン名を入力します。IPアドレスのローカルDNSサーバを介して、ルータはIPアドレスを自動的に取得できます。

ステップ2:[リモート証明書]ドロップダウンリストから適切なリモート証明書を選択します。新しい証明書をインポートするには[リモート証明書のインポート]をクリックし、デジタル署名要求で証明書を識別するには[CSRの承認]をクリックします。

注：新しい証明書をインポートする方法の詳細については、「RV320ルータでの信頼できるSSL証明書の表示/追加」を参照してください。また、承認されたCSRの詳細については、「RV320ルータでの証明書署名要求(CSR)」を参照してください。

ステップ3：これまでの設定を保存する場合は、下にスクロールして[保存]をクリックして設定を保存します。

IPSecの設定

手動キーによるIPSecセットアップ

注：新しいトンネルの追加セクションのステップ3でKeying ModeドロップダウンリストからManualを選択した場合は、次の手順に従ってください。

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5

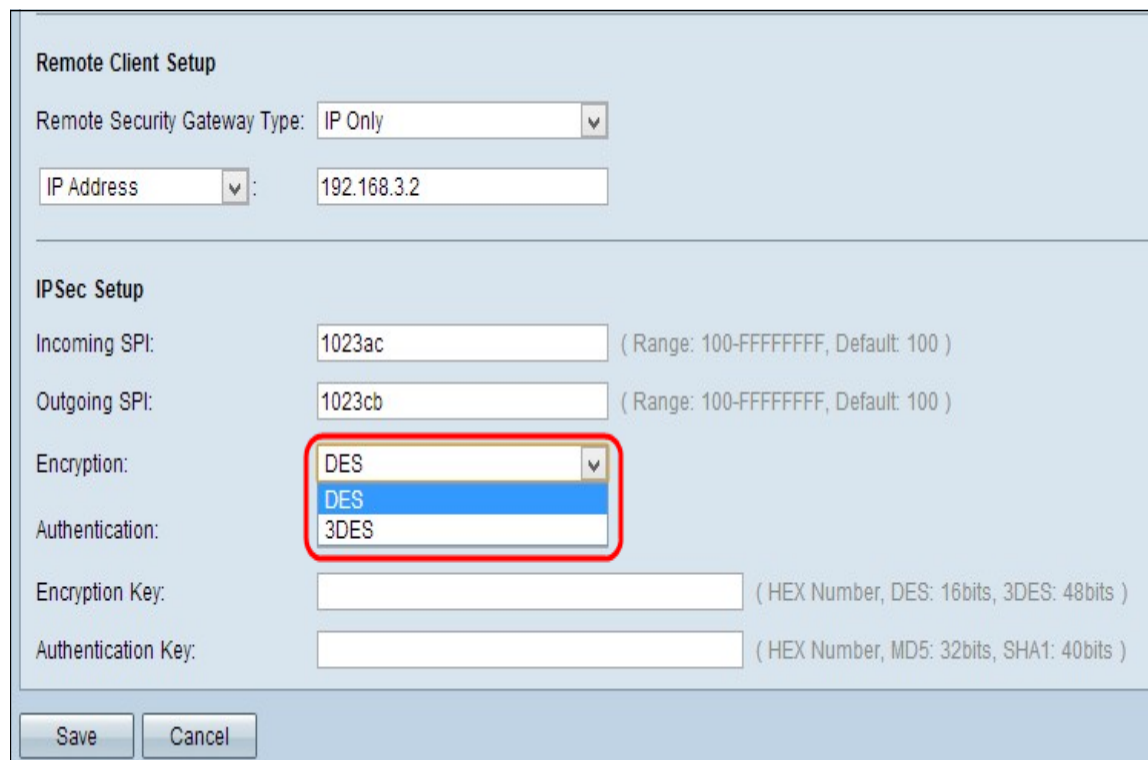
Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

ステップ1:[Incoming SPI]フィールドに、着信セキュリティパラメータインデックス(SPI)の一意の16進数値を入力します。SPIはEncapsulating Security Payload Protocol(ESP)ヘッダー内で伝送され、これにより着信パケットのセキュリティアソシエーション(SA)が決定されます。範囲は100 ~ ffffffffで、デフォルトは100です。

ステップ2:[発信SPI]フィールドに、発信セキュリティパラメータインデックス(SPI)の一意の16進数値を入力します。SPIはEncapsulating Security Payload Protocol(ESP)ヘッダーで伝送され、ともに発信パケットのセキュリティアソシエーション(SA)を決定します。範囲は100 ~ ffffffffで、デフォルトは100です。

注：接続されたデバイスの着信SPIとトンネルのもう一方の端の発信SPIは、互いに一致してトンネルを確立する必要があります。



Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES (highlighted)

Authentication: 3DES

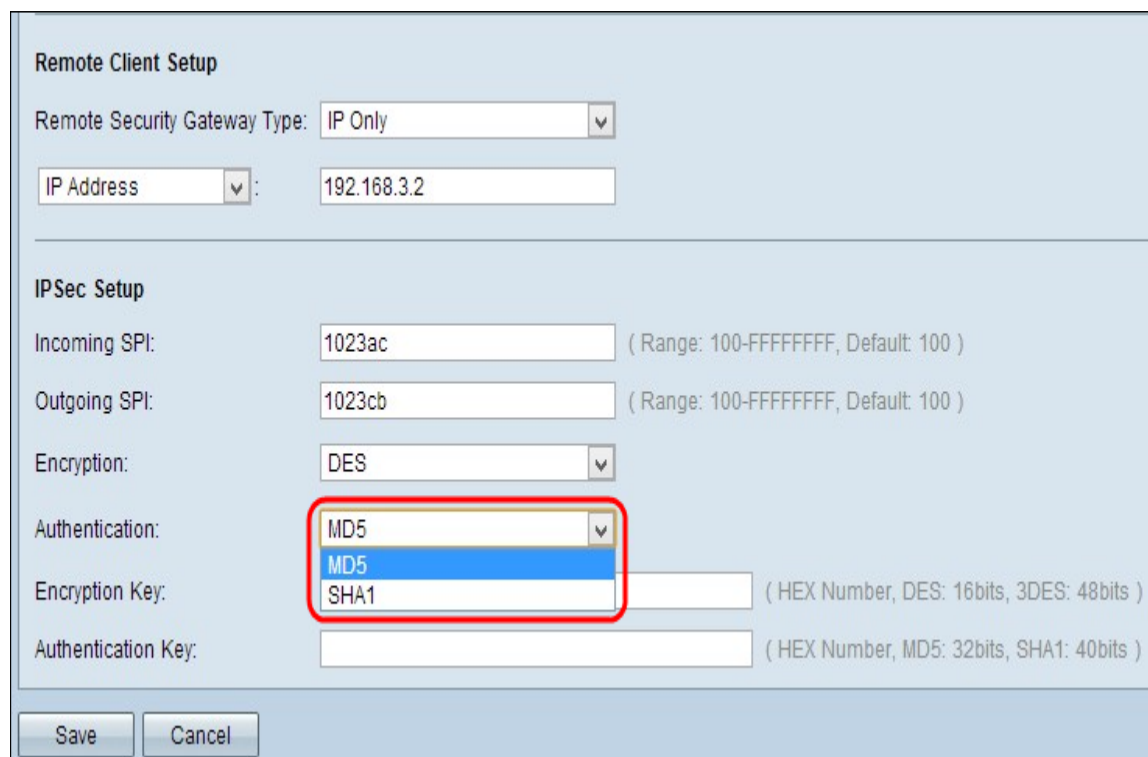
Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

ステップ3:[Encryption]ドロップダウンリストから適切な暗号化方法を選択します。推奨される暗号化は3DESです。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。

- DES:Data Encryption Standard (DES ; データ暗号規格) は、56ビットの古い、より下位互換性のある暗号化方式で、それほど安全ではありません。
- 3DES - Triple Data Encryption Standard(3DES)は168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することで、キーサイズを大きくします。



Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: MD5 (highlighted)

Encryption Key: (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

ステップ4:[Authentication]ドロップダウンリストから適切な認証方法を選択します。推奨される認証はSHA1です。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。

- 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32桁の16進数ハッシュ関数を表します。
- SHA1 : セキュアハッシュアルゴリズムバージョン1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Incoming SPI: 1023ac (Range: 100-FFFFFFFF, Default: 100)

Outgoing SPI: 1023cb (Range: 100-FFFFFFFF, Default: 100)

Encryption: DES

Authentication: SHA1

Encryption Key: adbc234987bc (HEX Number, DES: 16bits, 3DES: 48bits)

Authentication Key: 233445bcfacfb (HEX Number, MD5: 32bits, SHA1: 40bits)

Save Cancel

ステップ5:[Encryption Key]フィールドに、データを暗号化および復号化するキーを入力します。ステップ3で暗号化方式としてDESを選択した場合は、16桁の16進数値を入力します。ステップ3で暗号化方式として3DESを選択した場合は、40桁の16進数値を入力します。

ステップ6:[Authentication Key]フィールドに事前共有キーを入力してトラフィックを認証します。ステップ4で認証方式として[MD5]を選択した場合は、32桁の16進数値を入力します。ステップ4で認証方式として[SHA]を選択した場合は、40桁の16進数値を入力します。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。

ステップ7 : これまでの設定を保存する場合は、下にスクロールして[保存]をクリックして設定を保存します。

事前共有キーを使用したIKEまたは証明書を使用したIKEによるIPSecのセットアップ

注 : Add a New Tunnelセクションのステップ3でKeying Modeドロップダウンリストから事前共有キーを使用したIKEまたは証明書を使用したIKEを選択した場合は、次の手順に従います。

Remote Client Setup

Remote Security Gateway Type: IP Only

IP Address: 192.168.3.2

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: Group 1 - 768 bit

Phase 1 Authentication: MD5

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

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: ■■■■

Advanced +

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

- グループ1 - 768ビット：最も低い強度キーと最も安全でない認証グループを表します。しかし、IKEキーの計算に必要な時間が短縮されます。ネットワークの速度が低い場合に推奨されます。
- グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。しかし、IKEキーを計算するには時間が必要です。
- グループ5 - 1536ビット：最高強度キーと最もセキュアな認証グループを表します。IKEキーを計算する時間が長くなる。ネットワークの速度が高い場合に推奨されます。

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: **DES** (dropdown menu open showing: DES, 3DES, AES-128, AES-192, AES-256)

Phase 1 Authentication: (dropdown menu)

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

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit

Phase 2 Encryption: DES

Phase 2 Authentication: MD5

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

Minimum Preshared Key Complexity: Enable

Preshared Key: (text input field)

Preshared Key Strength Meter: (progress bar)

Advanced +

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フェーズ1暗号化を選択します。AES-256は最も安全な暗号化方式であるため、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。

- DES:Data Encryption Standard (DES ; データ暗号規格) は56ビットで、古い暗号化方式ではあまり安全な暗号化方式ではありません。
- 3DES - Triple Data Encryption Standard(3DES)は168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することで、キーサイズを大きくします。
- AES-128 : 高度暗号化規格(AES)は、平文を繰り返し10サイクルの暗号テキストに変換する128ビット暗号化方式です。
- AES-192 : 高度暗号化規格(AES)は、平文を繰り返しの12サイクルで暗号テキストに変換する192ビット暗号化方式です。
- AES-256 : 高度暗号化規格(AES)は、平文を繰り返し14サイクルの暗号テキストに変換する256ビット暗号化方式です。

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: MD5

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

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit


Phase 2 Encryption: DES

Phase 2 Authentication: MD5

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Advanced +

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法を選択します。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。

- 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32桁の16進数ハッシュ関数を表します。
- SHA1 : セキュアハッシュアルゴリズムバージョン1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: SHA1

Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 1 - 768 bit


Phase 2 Encryption: DES

Phase 2 Authentication: MD5

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter: 

Advanced +

ステップ4：フェーズ1で、VPNトンネルが[Phase 1 SA Lifetime]フィールドでアクティブのままである時間を秒単位で入力します。デフォルトの時間は28800秒です。

ステップ5:[Perfect Forward Secrecy]チェックボックスをオンにして、キーの保護を強化します。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。暗号化されたデータは、侵害されたキーによってのみ侵害されます。そのため、キーが侵害されても他のキーを保護するため、より安全で認証された通信を提供します。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。

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

Minimum Preshared Key Complexity: Enable

Preshared Key:

Preshared Key Strength Meter:

ステップ6:[Phase 2 DH Group]ドロップダウンリストから適切なフェーズ2 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(DH)は、フェーズ1接続で秘密キーを共有して通信を認証するために使用される暗号キー交換プロトコルです。

- グループ1 - 768ビット：最も低い強度キーと最も安全でない認証グループを表します。しかし、IKEキーの計算に必要な時間が短縮されます。ネットワークの速度が低い場合に推奨されます。
- グループ2 - 1024ビット：強度の高いキーとよりセキュアな認証グループを表します。しかし、IKEキーを計算するには時間が必要です。
- グループ5 - 1536ビット：最高強度キーと最もセキュアな認証グループを表します。IKEキーを計算する時間が長くなる。ネットワークの速度が高い場合に推奨されます。

IPSec Setup

Phase 1 DH Group: Group 1 - 768 bit

Phase 1 Encryption: AES-128

Phase 1 Authentication: SHA1

Phase 1 SA Lifetime: 2870 sec (Range: 120-86400, Default: 28800)

Perfect Forward Secrecy:

Phase 2 DH Group: Group 2 - 1024 bit

Phase 2 Encryption: **DES**

Phase 2 Authentication: DES

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

Minimum Preshared Key Complexity: AES-256

Preshared Key:

Preshared Key Strength Meter: ■ ■ ■ ■

Advanced +

ステップ7:[フェーズ2暗号化]ドロップダウンリストから、適切なフェーズ2暗号化を選択してキーを暗号化します。AES-256は最も安全な暗号化方式であるため、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。

- DES:Data Encryption Standard (DES ; データ暗号規格) は56ビットで、古い暗号化方式ではあまり安全な暗号化方式ではありません。
- 3DES - Triple Data Encryption Standard(3DES)は168ビットの簡単な暗号化方式で、DESよりもセキュリティが高いデータを3回暗号化することで、キーサイズを大きくします。
- AES-128 : 高度暗号化規格(AES)は、プレーンテキストを10サイクルの繰り返しで暗号テキストに変換する128ビット暗号化方式です。
- AES-192 : 高度暗号化規格(AES)は、プレーンテキストを12サイクルの繰り返しで暗号テキストに変換する192ビット暗号化方式です。
- AES-256 - Advanced Encryption Standard(AES)は、プレーンテキストを14サイクルの繰り返しで暗号テキストに変換する256ビットの暗号化方式です。

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8:[Phase 2 Authentication]ドロップダウンリストから適切な認証方法を選択します。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。

- 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32桁の16進数ハッシュ関数を表します。
- SHA1 : セキュアハッシュアルゴリズムバージョン1(SHA1)は、MD5よりも安全な160ビットのハッシュ関数です。
- Null : 認証方式は使用されません。

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9：フェーズ2で、VPNトンネルが[Phase 2 SA Lifetime]フィールドでアクティブのままである時間を秒単位で入力します。デフォルトの時間は3600秒です。

ステップ10：事前共有キーの強度メーターを有効にする場合は、[Minimum Preshared Key Complexity]チェックボックスをオンにします。

ステップ11:[Preshared Key]フィールドに、IKEピア間で以前に共有したキーを入力します。事前共有キーとして最大30文字の英数字を使用できます。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が安全な状態を維持するために、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。

- Preshared Key Strength Meter：色付きのバーを通した事前共有キーの強度を示します。赤は弱い強さを示し、黄色は許容される強さを示し、緑は強い強さを示します。IPSec Setupセクションのステップ10でMinimum Preshared Key Complexityチェックボックスにチェックマークを付けると、Preshared Key Strength Meterだけが表示されます。

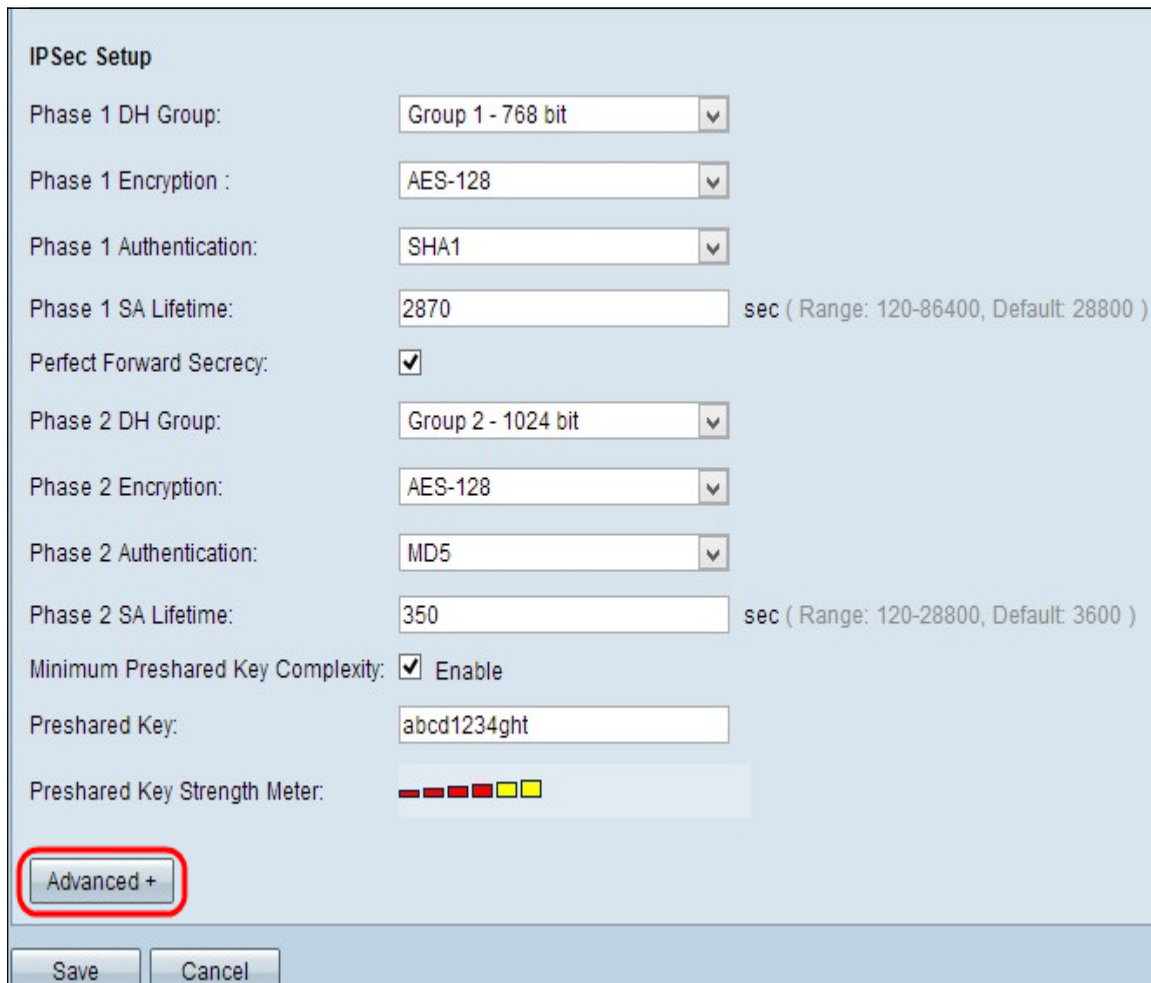
注：ステップ3のKeying Modeドロップダウンリストから事前共有キーを使用したIKEを選択して、Add a New Tunnelセクションを選択した場合は、ステップ10、ステップ11を設定し、事前共有キー強度メーターを表示するオプションしかありません。

ステップ12：これまでの設定を保存する場合は、下にスクロールして[保存]をクリックして設定を保存します。

事前共有キーを使用したIKEまたは証明書を使用したIKEによる高度なセットアップ

拡張設定は、事前共有キーを持つIKEと認証キーを持つIKEでのみ可能です。[手動]キーの設

定には、詳細設定がありません。



The image shows a configuration window titled "IPSec Setup". It contains several settings for Phase 1 and Phase 2. Phase 1 settings include DH Group (Group 1 - 768 bit), Encryption (AES-128), Authentication (SHA1), and SA Lifetime (2870 sec). Phase 2 settings include DH Group (Group 2 - 1024 bit), Encryption (AES-128), Authentication (MD5), and SA Lifetime (350 sec). There are also checkboxes for Perfect Forward Secrecy and Minimum Preshared Key Complexity (Enabled). A Preshared Key field contains "abcd1234ght" and a strength meter below it. At the bottom left, an "Advanced +" button is highlighted with a red circle. At the bottom, there are "Save" and "Cancel" buttons.

Phase 1 DH Group:	Group 1 - 768 bit
Phase 1 Encryption :	AES-128
Phase 1 Authentication:	SHA1
Phase 1 SA Lifetime:	2870 sec (Range: 120-86400, Default: 28800)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/>
Phase 2 DH Group:	Group 2 - 1024 bit
Phase 2 Encryption:	AES-128
Phase 2 Authentication:	MD5
Phase 2 SA Lifetime:	350 sec (Range: 120-28800, Default: 3600)
Minimum Preshared Key Complexity:	<input checked="" type="checkbox"/> Enable
Preshared Key:	abcd1234ght
Preshared Key Strength Meter:	

Advanced +

Save Cancel

ステップ1:[Advanced]をクリックして、事前共有キーを使用したIKEの詳細設定を取得します。

The screenshot shows the 'Advanced' configuration window. A red box highlights the following options:

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol (IPComp))
- Keep-Alive
- AH Hash Algorithm: SHA1
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval: 15 sec (Range: 10-999, Default: 10)

Other visible options include:

- Extended Authentication
- IPSec Host
 - User Name:
 - Password:
- Edge Device: Default - Local Database
- Mode Configuration

Buttons at the bottom: Save, Cancel

ステップ2: ネットワーク速度が低い場合は、[アグレッシブモード]チェックボックスをオンにします。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するため、交換に必要な時間は短いですが、セキュリティは低くなります。

ステップ3: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。ネットワーク速度が低く、ユーザが低速ネットワークを介して損失なく迅速にデータを送信したい場合に使用します。

ステップ4: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。接続が非アクティブになった場合は、すぐに接続を再確立できます。

ステップ5: 認証ヘッダー(AH)を認証する場合、[AHハッシュアルゴリズム]チェックボックスをオンにします。AHはデータの送信元に認証を提供し、チェックサムを通じてデータの整合性を確保し、IPヘッダーに保護を拡張します。トンネルの両側で同じアルゴリズムが必要です。

- 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桁の16進数ハッシュ関数を表します。
- SHA1:セキュアハッシュアルゴリズムバージョン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: ルーティング不可能なトラフィックがVPNトンネルを通過できるようにするには、[NetBIOS Broadcast] をオンにします。デフォルトはオフです。NetBIOSは、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、一部の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機能を介して検出するために使用されます。

ステップ7:[NAT Traversal] チェックボックスをオンにすると、プライベートLANからパブリックIPアドレスを使用してインターネットにアクセスできます。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アドレスとして表示し、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:[Dead Peer Detection Interval]をチェックし、HelloまたはACKを定期的に通過するVPNトンネルの状態をチェックします。このチェックボックスをオンにした場合は、必要なhelloメッセージの期間または間隔を入力します。

Advanced

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm SHA1

NetBIOS Broadcast

NAT Traversal

Dead Peer Detection Interval 15 sec (Range: 10-999, Default: 10)

Extended Authentication

IPSec Host

User Name: user_1

Password:

Edge Device Default - Local Database Add/Edit

Mode Configuration

Save Cancel

ステップ9:[Extended Authentication]をオンにして、VPN接続のセキュリティと認証を強化します。該当するオプションボタンをクリックして、VPN接続の認証を拡張します。

- IPSecホスト：IPSecホストによる拡張認証。このオプションを選択した場合は、[User Name]フィールドにIPSecホストのユーザ名、[Password]フィールドにパスワードを入力します。
- エッジデバイス：エッジデバイスによる拡張認証。このオプションを選択した場合は、エッジデバイスを含むデータベースをドロップダウンリストから選択します。データベースを追加または編集する場合は、「追加/編集」をクリックします。

注：ローカルデータベースを追加または編集する方法の詳細については、『RV320ルータのユーザおよびドメイン管理の設定』を参照してください。

ステップ 10：[Mode Configuration]をオンにして、着信トンネルリクエストのIPアドレスを指定します。

注：ステップ9～11は、トンネルVPNのIKE事前共有キーイングモードで使用できます。

ステップ11:[Save]をクリックして、設定を保存します。

結論

これで、RV32xシリーズVPNルータ上のゲートウェイVPNに単一のクライアントを設定する手順が学習されました

[この記事に関連するビデオを表示...](#)

[シスコのその他のテクニカルトピックを表示するには、ここをクリックしてください](#)