RV215Wの高度なVPNセットアップ

目的

バーチャルプライベートネットワーク(VPN)は、ネットワーク内またはネットワーク間で確立されるセキュアな接続です。VPNは、指定されたホストとネットワーク間のトラフィックを、許可されていないホストとネットワークのトラフィックから分離するのに役立ちます。この記事では、RV215WでAdvanced VPN Setupを設定する方法について説明します。

該当するデバイス

・ RV215W

[Software Version]

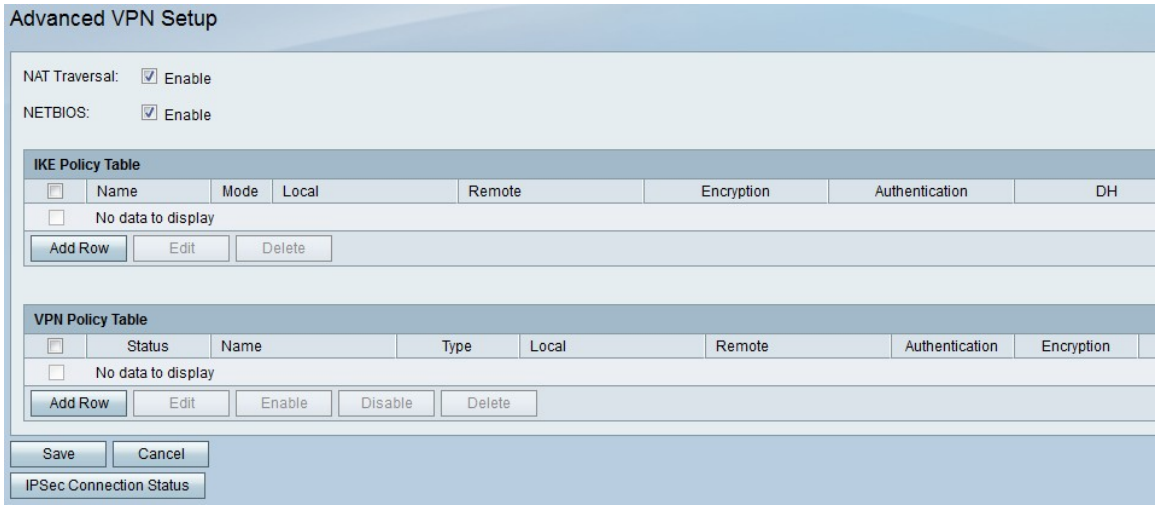
•1.1.0.5

高度なVPNセットアップ

初期設定

この手順では、Advanced VPN Setupの初期設定を行う方法について説明します。

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



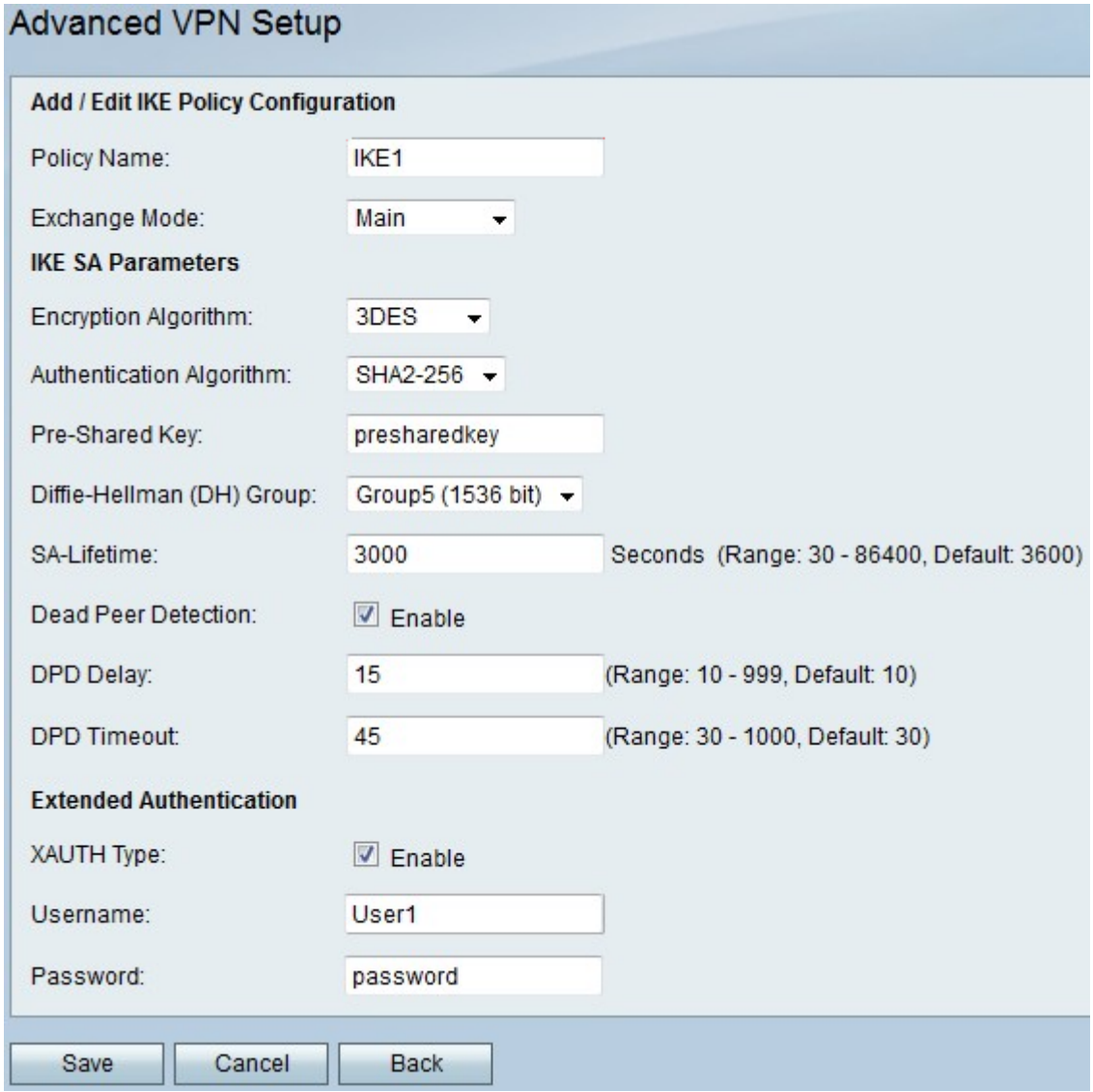
ステップ2:（オプション）VPN接続のネットワークアドレス変換(NAT)トラバーサルを有効にするには、[NAT Traversal]フィールドの[Enable] チェックボックスをオンにします。NATトラバーサルでは、NATを使用するゲートウェイ間でVPN接続を行うことができます。VPN接続がNAT対応ゲートウェイを通過する場合は、このオプションを選択します。

ステップ3:（オプション）VPN接続を介して送信されるNetwork Basic Input/Output System(NetBIOS)ブロードキャストを有効にする場合は、NETBIOSフィールドの**Enable**チェックボックスをオンにします。NetBIOSにより、ホストはLAN内で相互に通信できます。

IKEポリシー設定

Internet Key Exchange（IKE；インターネットキーエクスチェンジ）は、VPNで通信するためのセキュアな接続を確立するために使用されるプロトコルです。この確立されたセキュアな接続は、セキュリティアソシエーション(SA)と呼ばれます。 この手順では、セキュリティのために使用するVPN接続のIKEポリシーを設定する方法について説明します。VPNが正常に機能するには、両方のエンドポイントのIKEポリシーが同じである必要があります。

ステップ1:IKEポリシーテーブルで、[**Add Row**]をクリックして**新しい**IKEポリシーを作成します。IKEポリシーを編集するには、ポリシーのチェックボックスをオンにし、[**Edit**]をクリックします。[*Advanced VPN Setup*]ページが変更されます。

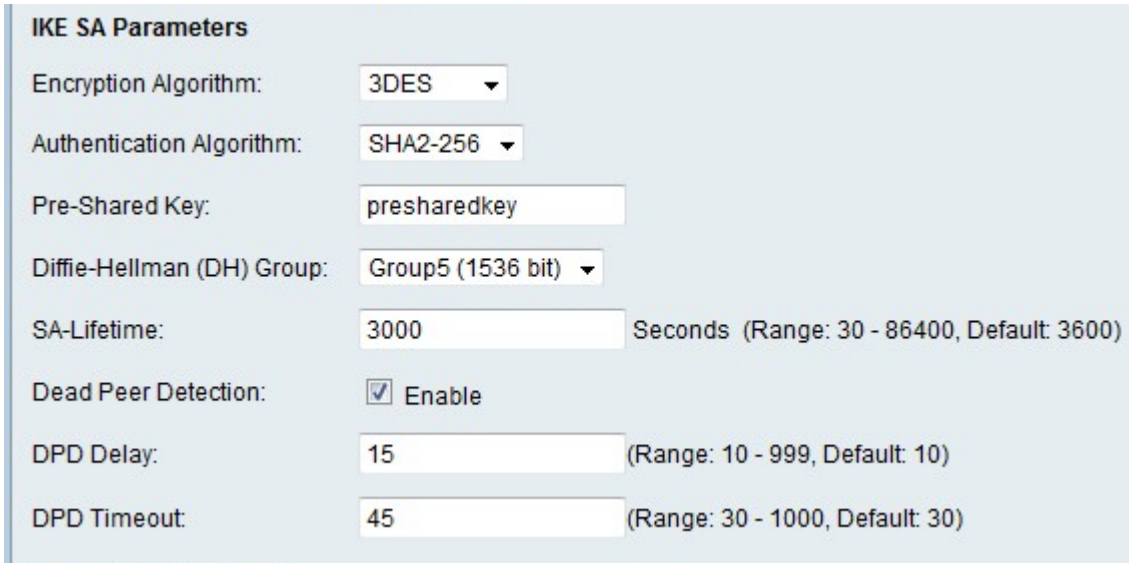


ステップ2:[Policy Name]フィールドに、IKEポリシーの名前を入力します。

ステップ3:[Exchange Mode]ドロップダウンリストから、オプションを選択します。

- Main：このオプションを使用すると、IKEポリシーをアグレッシブモードよりも安全に、かつ低速で動作させることができます。よりセキュアなVPN接続が必要な場合は、このオプションを選択します。

- Aggressive：このオプションを使用すると、IKEポリシーの動作がメインモードよりも高速で、セキュアではなくなります。より高速なVPN接続が必要な場合は、このオプションを選択します。



ステップ4:[Encryption Algorithm]ドロップダウンリストから、オプションを選択します。

・ 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5:[Authentication Algorithm]ドロップダウンリストから、オプションを選択します。

・ MD5:Message-Digest Algorithm 5(MD5)は、認証に128ビットのハッシュ値を使用します。MD5はSHA-1およびSHA2-256よりもセキュアではありませんが、高速です。

・ SHA-1：セキュアハッシュ関数1(SHA-1)は、認証に160ビットのハッシュ値を使用します。SHA-1はMD5よりも低速ですが安全性が高く、SHA-1はSHA2-256よりも高速ですが安全性が低くなります。

・ SHA2-256:256ビットのハッシュ値(SHA2-256)を持つセキュアハッシュアルゴリズム2は、認証に256ビットのハッシュ値を使用します。SHA2-256はMD5およびSHA-1よりも低速ですが、セキュアです。

ステップ6:[Pre-Shared Key]フィールドに、IKEポリシーで使用する事前共有キーを入力します。

ステップ7:[Diffie-Hellman (DH) Group]ドロップダウンリストから、IKEが使用するDHグル

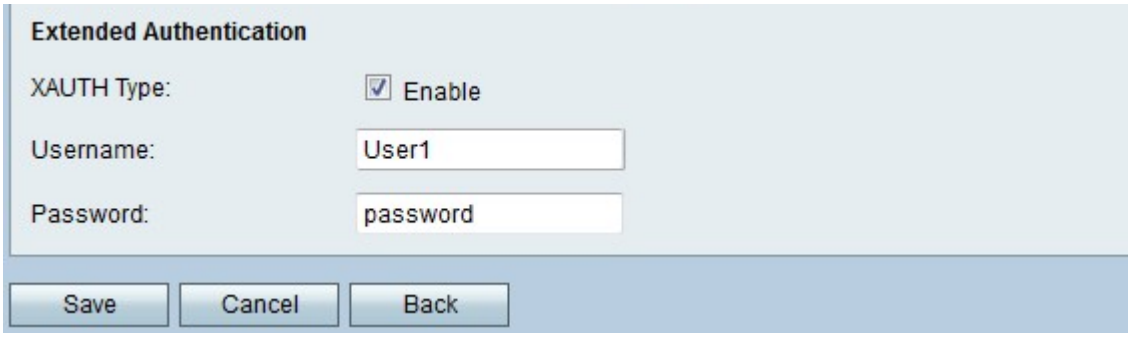
ープを選択します。DHグループ内のホストは、互いに認識せずにキーを交換できます。グループビット番号が大きいほど、グループのセキュリティは高くなります。

ステップ8:[SA-Lifetime]フィールドに、SAが更新されるまでのVPNのSAの有効期間（秒）を入力します。

ステップ9:（オプション）[Dead Peer Detection]フィールドの[**Enable**]チェックボックスをオンにして、Dead Peer Detection(DPD)を有効にします。DPDはIKEピアを監視し、ピアが機能を停止したかどうかを確認します。DPDは、非アクティブなピアのネットワークリソースの浪費を防止します。

ステップ10:（オプション）ステップ9でDPDを有効にした場合は、[DPD Delay]フィールドにピアのアクティビティをチェックする頻度（秒単位）を入力します。

ステップ11:（オプション）ステップ9でDPDを有効にした場合は、非アクティブピアがドロップされるまでに待機する秒数を[DPD Timeout]フィールドに入力します。



ステップ12:（オプション）拡張認証(XAUTH)を有効にするには、[XAUTH Type]フィールドの[**Enable**]チェックボックスをオンにします。XAUTHを使用すると、複数のユーザが各ユーザのVPNポリシーではなく、単一のVPNポリシーを使用できます。

ステップ13:（オプション）ステップ12でXAUTHを有効にした場合は、ポリシーに使用するユーザ名を[Username]フィールドに入力します。

ステップ14:（オプション）ステップ12でXAUTHを有効にした場合は、ポリシーに使用するパスワードを[Password]フィールドに入力します。

ステップ15:[**Save**]をクリックします。元の[*Advanced VPN Setup*]ページが再表示されます。

VPNポリシーの設定

この手順では、使用するVPN接続のVPNポリシーを設定する方法について説明します。VPNが正常に機能するには、両方のエンドポイントのVPNポリシーが同じである必要があります。

ステップ1:VPNポリシーテーブルで、[**Add Row**]をクリックして新しいVPNポリシーを作成します。VPNポリシーを編集するには、ポリシーのチェックボックスをオンにし、[**Edit**]をクリックします。[*Advanced VPN Setup*]ページが変更されます。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

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)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

ステップ2:[Policy Name]フィールドに、VPNポリシーの名前を入力します。

ステップ3:[Policy Type]ドロップダウンリストからオプションを選択します。

・手動ポリシー：このオプションでは、データの暗号化と整合性のためのキーを設定できます。

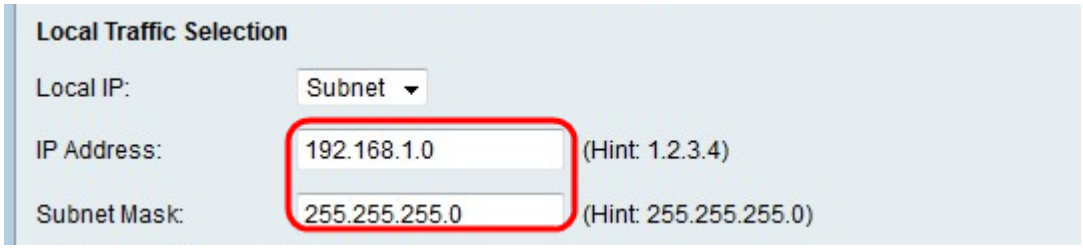
・ Auto Policy：このオプションでは、データ整合性と暗号化キー交換にIKEポリシーを使用します。

ステップ4:[Remote Endpoint]ドロップダウンリストから、オプションを選択します。

・ IPアドレス：このオプションは、リモートネットワークをパブリックIPアドレスで識別します。

・ FQDN：このオプションでは、完全修飾ドメイン名(FQDN)を使用してリモートネットワークを識別します。

ステップ5:[Remote Endpoint]ドロップダウンリストの下のテキスト入力フィールドに、リモートアドレスのパブリックIPアドレスまたはドメイン名を入力します。



ステップ6:[Local IP]ドロップダウンリストから、オプションを選択します。

・ Single：このオプションでは、ローカルVPN接続ポイントとして1つのホストを使用します。

・サブネット：このオプションでは、ローカルネットワークのサブネットをローカルVPN接続ポイントとして使用します。

ステップ7:[IP Address]フィールドに、ローカルサブネットまたはローカルホストのホストまたはサブネットIPアドレスを入力します。

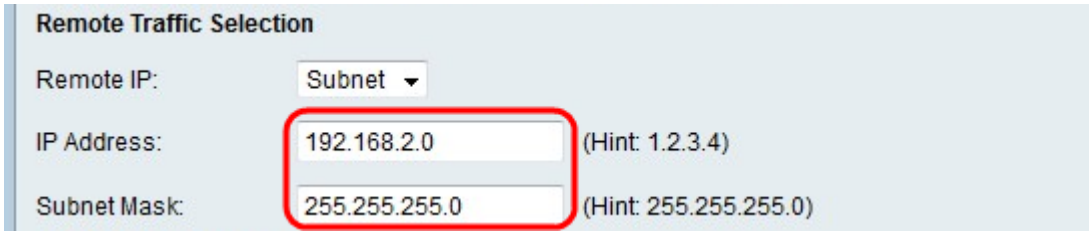
ステップ8:（オプション）ステップ6で[Subnet]を選択した場合は、[Subnet Mask]フィールドにローカルサブネットのサブネットマスクを入力します。

ステップ9:[Remote IP]ドロップダウンリストから、オプションを選択します。

・ Single：このオプションでは、リモートVPN接続ポイントとして1つのホストを使用し

ます。

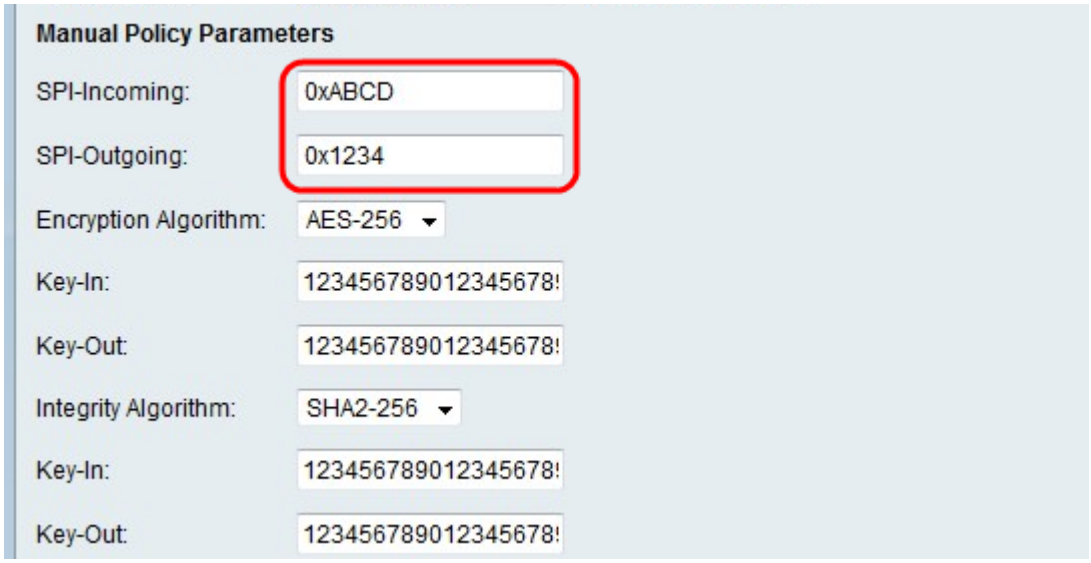
・サブネット：このオプションでは、リモートネットワークのサブネットをリモートVPN接続ポイントとして使用します。



ステップ10:[IP Address]フィールドに、リモートサブネットまたはリモートホストのホストまたはサブネットIPアドレスを入力します。

ステップ11:（オプション）ステップ9で[Subnet]を選択した場合は、[Subnet Mask]フィールドにリモートサブネットのサブネットマスクを入力します。

注：ステップ3で[Manual Policy]を選択した場合は、ステップ12 ~ 19を実行します。それ以外の場合は、ステップ20をスキップします。



ステップ12:[SPI-Incoming]フィールドで、VPN接続の着信トラフィックのセキュリティパラメータインデックス(SPI)タグに3 ~ 8の16進数を入力します。SPIタグは、あるセッションのトラフィックを他のセッションのトラフィックと区別するために使用されます。

ステップ13:[SPI-Outgoing]フィールドに、VPN接続の発信トラフィック用のSPIタグに3 ~ 8の16進数文字を入力します。

ステップ14:[Encryption Algorithm]ドロップダウンリストから、オプションを選択します。

・ 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。

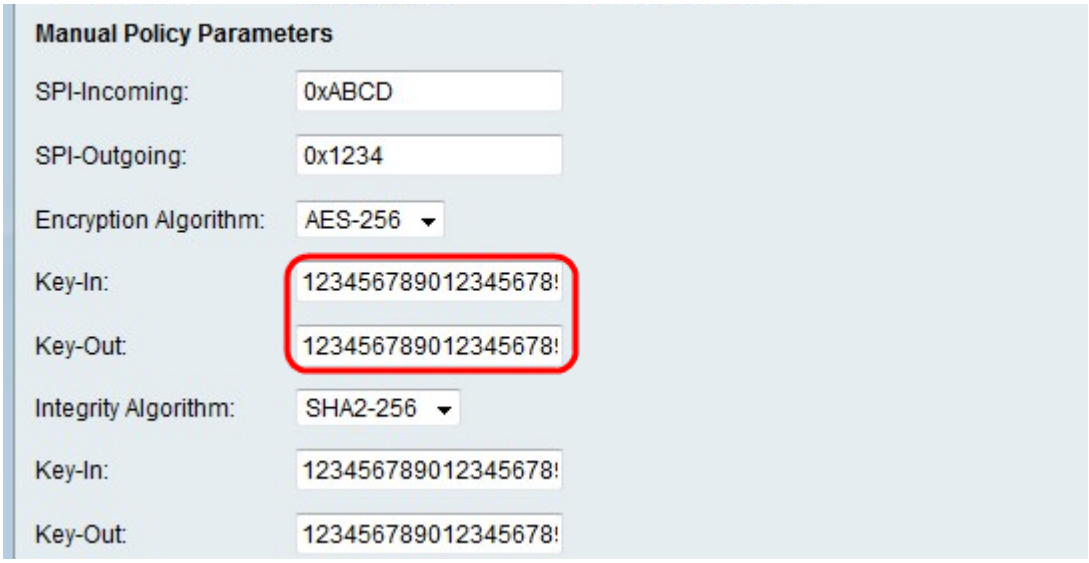
・ 3DES — Triple Data Encryption Standard(3DES)は、データを3回暗号化するため、キーサイズを大きくするために使用される168ビットの簡単な暗号化方式です。これにより、DESよりもセキュリティが高くなりますが、AESよりもセキュリティが低くなります。

・ 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15:[Key-In]フィールドに、インバウンドポリシーのキーを入力します。キーの長さは、ステップ14で選択したアルゴリズムによって異なります。

・ DESは8文字キーを使用します。

・ 3DESは24文字キーを使用します。

・ AES-128は12文字キーを使用します。

・ AES-192は24文字キーを使用します。

・ AES-256は32文字キーを使用します。

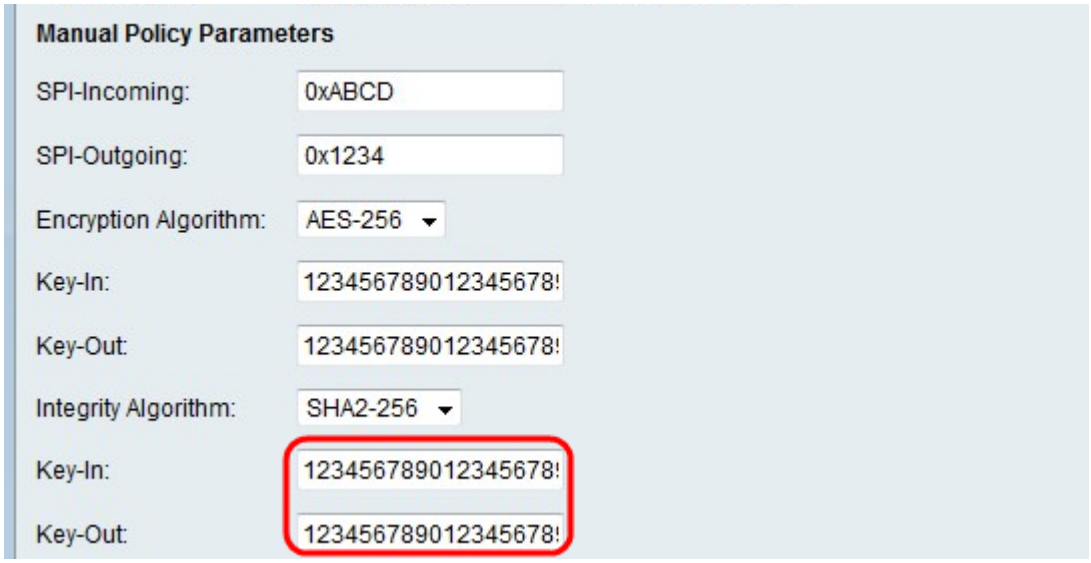
ステップ16:[Key-Out]フィールドに、発信ポリシーのキーを入力します。キーの長さは、ステップ14で選択したアルゴリズムによって異なります。キーの長さは、ステップ15と同じです。

ステップ17:[Integrity Algorithm]ドロップダウンリストから、オプションを選択します。

・ MD5:Message-Digest Algorithm 5(MD5)は、データ整合性のために128ビットのハッシュ値を使用します。MD5はSHA-1およびSHA2-256よりもセキュアではありませんが、高速です。

・ SHA-1：セキュアハッシュ関数1(SHA-1)は、データ整合性のために160ビットのハッシュ値を使用します。SHA-1はMD5よりも低速ですが安全性が高く、SHA-1はSHA2-256よりも高速ですが安全性が低くなります。

・ SHA2-256:256ビットのハッシュ値(SHA2-256)を持つセキュアハッシュアルゴリズム2は、データの整合性のために256ビットのハッシュ値を使用します。SHA2-256はMD5およびSHA-1よりも低速ですが、セキュアです。



ステップ18:[Key-In]フィールドに、インバウンドポリシーのキーを入力します。キーの長さは、ステップ17で選択したアルゴリズムによって異なります。

- MD5は16文字キーを使用します。
- SHA-1は20文字キーを使用します。
- SHA2-256は32文字キーを使用します。

ステップ19:[Key-Out]フィールドに、発信ポリシーのキーを入力します。キーの長さは、ステップ17で選択したアルゴリズムによって異なります。キーの長さは、ステップ18と同じです。

注：ステップ3で[Auto Policy]を選択した場合は、ステップ20 ~ 25を実行します。それ以外の場合は、ステップ 26 に進みます。

ステップ20:[SA-Lifetime]フィールドに、SAが更新前に継続する時間（秒）を入力します。

ステップ21:[Encryption Algorithm]ドロップダウンリストから、オプションを選択します。

- 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22:[Integrity Algorithm]ドロップダウンリストから、オプションを選択します。

・ MD5:Message-Digest Algorithm 5(MD5)は、データ整合性のために128ビットのハッシュ値を使用します。MD5はSHA-1およびSHA2-256よりもセキュアではありませんが、高速です。

・ SHA-1：セキュアハッシュ関数1(SHA-1)は、データ整合性のために160ビットのハッシュ値を使用します。SHA-1はMD5よりも低速ですが安全性が高く、SHA-1はSHA2-256よりも高速ですが安全性が低くなります。

・ SHA2-256:256ビットのハッシュ値(SHA2-256)を持つセキュアハッシュアルゴリズム2は、データの整合性のために256ビットのハッシュ値を使用します。SHA2-256はMD5およびSHA-1よりも低速ですが、セキュアです。

ステップ23:PFSキーグループの**Enable**チェックボックスをオンにして、Perfect Forward Secrecy(PFS)を有効にします。PFSはVPNセキュリティを高めますが、接続速度を遅くします。

ステップ24:（オプション）ステップ23でPFSを有効にすることを選択した場合は、次のドロップダウンリストに参加するDiffie-Hellman(DH)グループを選択します。グループ番号が大きいほど、グループのセキュリティは高くなります。

ステップ25:[Select IKE Policy]ドロップダウンリストから、VPNポリシーに使用するIKEポリシーを選択します。

注：[**View**]をクリック**すると**、[*Advanced VPN Setup*]ページの[IKE configuration]セクションに移動します。

ステップ26:[**Save**]をクリ**ックします**。元の[*Advanced VPN Setup*]ページが再表示されます。

ステップ27:[**Save**]をクリ**ックします**。