

RV110WファイアウォールでのAdvanced Virtual Private Network(VPN)セットアップの設定

目的

バーチャル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またはインターネットを使用して、プライベートネットワークを確立し、安全に通信します。インターネットキー交換(IKE)は、2つのネットワーク間で安全な通信を確立するプロトコルです。これは、トラフィックフローの前にキーを交換するために使用されます。これにより、VPNトンネルの両端の信頼性が保証されます。

VPNの両端が同じVPNポリシーに従って、互いに正常に通信する必要があります。

このドキュメントの目的は、RV110WワイヤレスルータでIKEプロファイルを追加し、VPNポリシーを設定する方法を説明することです。

該当するデバイス

- RV110W

[Software Version]

- 1.2.0.9

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: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。

Advanced VPN Setup

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>					

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>			

Advanced VPN Setup

<input type="checkbox"/>	Name	Mode	Local	Remote
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Delete"/>				

<input type="checkbox"/>	Status	Name	Type	Local
No data to display				
<input type="button" value="Add Row"/> <input type="button" value="Edit"/> <input type="button" value="Enable"/> <input type="button" value="Disable"/> <input type="button" value="Delete"/>				

ステップ2:[Add Row]をクリックして、新しいIKEポリシーを作成します。[Advanced VPN Setup] ページが開きます。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: ▼

IKE SA Parameters

Encryption Algorithm: ▼

Authentication Algorithm: ▼

Pre-Shared Key:

Diffie-Hellman (DH) Group: ▼

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ3:[Policy Name]フィールドに、識別しやすいIKEポリシーの名前を入力します。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode: Main
Main
Aggressive

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ4:[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:IKEポリシーの動作をアグレッシブモードよりも安全に、かつ低速にできます。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:IKEポリシーの動作がメインモードよりも速いが安全ではない。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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm: (Dropdown menu showing: AES-128, DES, 3DES, AES-128, AES-192, AES-256)

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ5:[Encryption Algorithm]ドロップダウンリストからアルゴリズムを選択します。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) では、データ暗号化に56ビットキーサイズを使用します。DESは古いため、1つのエンドポイントがDESのみをサポートしている場合にのみ使用する必要があります。
- ・ 3DES — Triple Data Encryption Standard(3DES)は、DESを3回実行しますが、実行されるDESのラウンドに応じて、キーサイズを168ビットから112ビット、112ビットから56ビットに変更します。3DESはDESやAESよりも安全です。
- ・ 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よりも高速ですが、安全性は低いのですが、一部のタイプのハードウェアでは3DESの高速化が可能です。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、安全性は高く、AES-192はAES-256よりも高速ですが、安全性は低くなります。
- ・ 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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ6:[Authentication Algorithm]ドロップダウンリストから必要な認証を選択します。

- ・ 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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ7:[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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ8:[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。

- ・ グループ1 - 768ビット：最小強度キーと最も安全でない認証グループ。しかし、IKEキーの計

算にかかる時間が短縮されます。このオプションは、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。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。

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime: Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection: Enable

DPD Delay: (Range: 10 - 999, Default: 10)

DPD Timeout: (Range: 30 - 1000, Default: 30)

ステップ9:[SA-Lifetime]フィールドに、VPNのSAが更新されるまでの期間 (秒) を入力します。

ステップ10: (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]を有効にします。Dead Peer Detection(DPD)は、IKEピアを監視して、ピアが機能を停止したかどうかを確認します。Dead Peer Detection(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11: (オプション) ステップ9でDead Peer Detectionを有効にした場合は、Dead Peer 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) を入力します。

ステップ12: (オプション) ステップ9でDead Peer Detectionを有効にした場合は、Dead Peer Detection Timeoutフィールドに、非アクティブなピアがドロップされるまでに待機する秒数を入力します。

ステップ13:[Save]をクリックして、すべての設定を適用します。

VPNポリシーの設定

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

Advanced VPN Setup

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						

Add Row Edit Delete


<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

Advanced VPN Setup

 Configuration settings have been saved successfully

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		

Add Row Edit Delete

<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

ステップ2:VPNポリシーテーブルから[Add Row]をクリックします。[Advanced VPN Policy Setup]ウィンドウが表示されます。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: ▼

Remote Endpoint: ▼

(Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: ▼

VPNポリシー設定の追加/編集

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

ステップ1:[Policy Name]フィールドにポリシーの一意の名前を入力して識別します。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

ステップ2:[Policy Type]ドロップダウンリストから適切なポリシータイプを選択します。

- ・ 自動ポリシー：パラメータは自動的に設定できます。この場合、ポリシーに加えて、IKE(Internet Key Exchange)プロトコルが2つのVPNエンドポイント間でネゴシエートする必要があります。
- ・ 手動ポリシー：この場合、VPNトンネルのキーの設定を含むすべての設定は、エンドポイントごとに手動で入力されます。

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

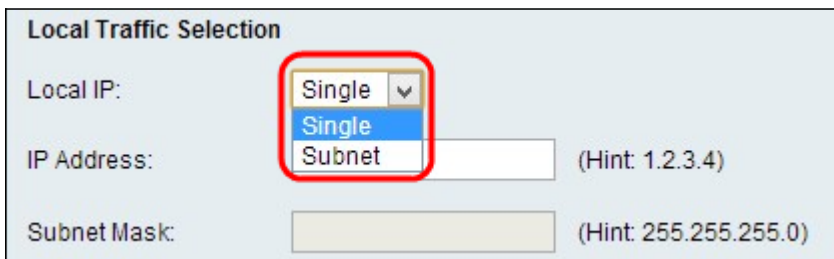
Remote Endpoint: (Hint: 1.2.3.4 or abc.com)

ステップ3:[リモートエンドポイント]ドロップダウンリストから、リモートエンドポイントのゲートウェイを識別するIP IDのタイプを選択します。

- ・ IPアドレス：リモートエンドポイントのゲートウェイのIPアドレス。このオプションを選択した場合は、フィールドにIPアドレスを入力します。
- ・ FQDN (完全修飾ドメイン名)：リモートエンドポイントのゲートウェイの完全修飾ドメイン名を入力します。このオプションを選択した場合は、フィールドに完全修飾ドメイン名を入力し

ます。

ローカルトラフィックの選択



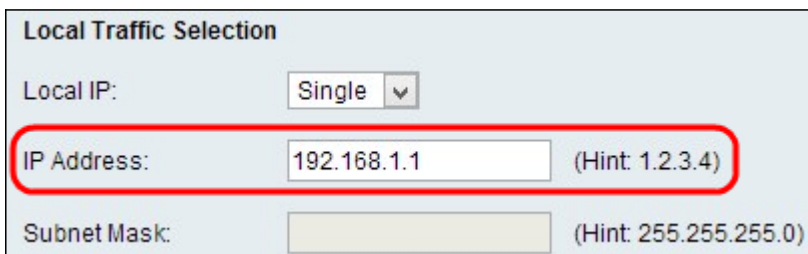
Local Traffic Selection

Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

ステップ1:[Local IP]ドロップダウンリストから、エンドポイントに指定する識別子のタイプを選択します。



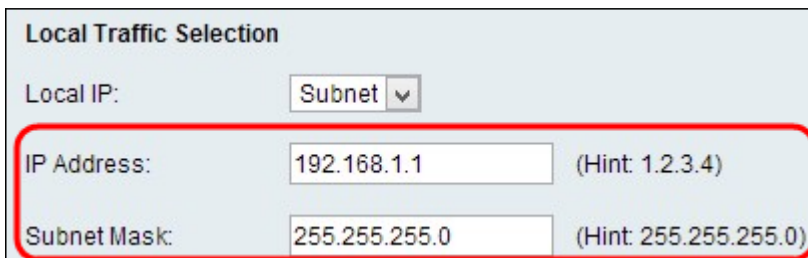
Local Traffic Selection

Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

・ Single : これにより、ポリシーが1つのホストに制限されます。このオプションを選択した場合は、[IP address]フィールドにIPアドレスを入力します。



Local Traffic Selection

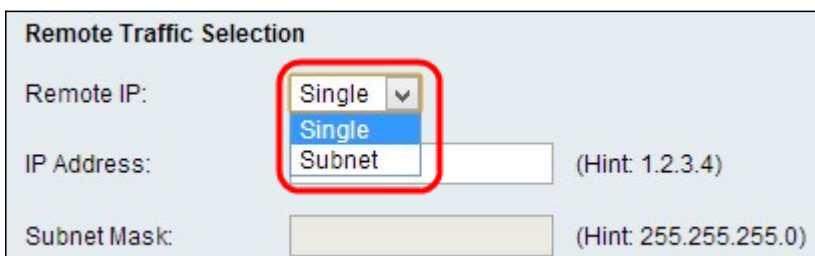
Local IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

・ サブネット : IPの境界を定義するマスクです。これにより、指定されたサブネットのホストだけがVPNに接続できます。VPNに接続するには、論理AND演算によりコンピュータを選択する。IPが必要な同じ範囲に収まっている場合は、コンピュータが選択されます。このオプションを選択した場合は、[IP address and Subnet]フィールドにIPアドレスとサブネットを入力します。

リモートトラフィックの選択



Remote Traffic Selection

Remote IP: (Hint: 1.2.3.4)

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

ステップ1:[Local IP]ドロップダウンリストから、エンドポイントに指定する識別子のタイプを選択します。

Remote Traffic Selection	
Remote IP:	Single ▼
IP Address:	192.168.1.5 (Hint: 1.2.3.4)
Subnet Mask:	(Hint: 255.255.255.0)

・ Single : これにより、ポリシーが1つのホストに制限されます。このオプションを選択した場合は、[IP address]フィールドにIPアドレスを入力します。

Remote Traffic Selection	
Remote IP:	Subnet ▼
IP Address:	192.168.1.5 (Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0 (Hint: 255.255.255.0)

・ サブネット : IPの境界を定義するマスクです。これにより、指定されたサブネットのホストだけがVPNに接続できます。VPNに接続するには、論理AND演算によりコンピュータを選択する。IPが必要な同じ範囲に収まっている場合は、コンピュータが選択されます。このオプションを選択した場合は、[IP address and Subnet]フィールドにIPアドレスとサブネットを入力します。

手動ポリシーパラメータ

手動ポリシーパラメータを設定するには、[Add/Edit VPN Policy Configuration]セクションのステップ2の[Policy Type]ドロップダウンリストから[Manual Policy]を選択します。

Manual Policy Parameters	
SPI-Incoming:	014C
SPI-Outgoing:	014C
Encryption Algorithm:	AES-128 ▼
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1 ▼
Key-In:	
Key-Out:	

ステップ1:[SPI-Incoming]フィールドに3 ~ 8の16進数値を入力します。ステートフルパケットインスペクション(SPI)は、ディープパケットインスペクションと呼ばれるテクノロジーです。SPIは、コンピュータネットワークを安全に保つために役立つセキュリティ機能を実装しています。SPI-Incoming値は、前のデバイスのSPI-Outgoingに対応します。リモートVPNエンドポイントのSPI-Outgoingフィールドの値が同じである場合は、任意の値を使用できます。

ステップ2:[SPI-Outgoing]フィールドに3 ~ 8の16進数値を入力します。

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:
3DES
DES
AES-128
AES-192
AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

ステップ3:[Encryption Algorithm]ドロップダウンリストから適切な暗号化アルゴリズムを選択します。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) では、データ暗号化に56ビットキーサイズを使用します。DESは古いため、1つのエンドポイントがDESのみをサポートしている場合にのみ使用する必要があります。
- ・ 3DES — Triple Data Encryption Standard(3DES)は、DESを3回実行しますが、実行されたDESのラウンドに基づいて、キーサイズを168ビットから112ビット、112ビットから56ビットに変更します。3DESはDESやAESよりも安全です。
- ・ 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よりも高速ですが、安全性は低いのですが、一部のタイプのハードウェアでは3DESの高速化が可能です。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、安全性は高く、AES-192はAES-256よりも高速ですが、安全性は低くなります。
- ・ 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。

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

ステップ4:[Key-In]フィールドにインバウンドポリシーの暗号化キーを入力します。キーの長さは、ステップ3で選択したアルゴリズムによって異なります。

ステップ5:[Key-Out]フィールドにアウトバウンドポリシーの暗号化キーを入力します。

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

ステップ6:[Integrity Algorithm]ドロップダウンリストから適切な整合性アルゴリズムを選択します。このアルゴリズムは、データの整合性を検証します。

- ・ MD5 : このアルゴリズムは、キーの長さを16文字に指定します。Message-Digest Algorithm 5(MD5)はコリジョンに強くないため、このプロパティに依存するSSL証明書やデジタル署名などのアプリケーションに適しています。MD5はバイトストリームを128ビット値に圧縮しますが、SHAは160ビット値に圧縮します。MD5は計算する方が若干安価ですが、MD5はハッシュアルゴリズムの古いバージョンであり、衝突攻撃に対して脆弱です。
- ・ SHA1 — Secure Hash Algorithm version 1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。
- ・ SHA2-256 : このアルゴリズムは、キーの長さを32文字に指定します。

Manual Policy Parameters	
SPI-Incoming:	014C
SPI-Outgoing:	014C
Encryption Algorithm:	DES ▼
Key-In:	1452
Key-Out:	1452
Integrity Algorithm:	SHA2-256 ▼
Key-In:	1234
Key-Out:	1234

ステップ7：インバウンドポリシーの整合性キー（整合性モードのESP用）を入力します。キーの長さは、ステップ6で選択したアルゴリズムによって異なります。

ステップ8:[Key-Out]フィールドにアウトバウンドポリシーの整合性キーを入力します。VPN接続はアウトバウンドからインバウンドに設定されているため、一方の端からのアウトバウンドキーは他方の端のインバウンドキーと一致する必要があります。

注：正常な接続を行うには、SPI-IncomingおよびOutgoing、Encryption Algorithm、Integrity Algorithm、およびKeysがVPNトンネルの反対側で同じである必要があります。

自動ポリシーパラメータ

Auto Policy Parameters	
SA-Lifetime:	2800 Seconds (Range: 30 - 86400, Default: 28800)
Encryption Algorithm:	AES-128 ▼
Integrity Algorithm:	SHA-1 ▼
PFS Key Group:	<input type="checkbox"/> Enable
	DH-Group 1(768 bit) ▼
Select IKE Policy:	policy1 ▼
	<input type="button" value="View"/>

ステップ1:[SA Lifetime (SAライフタイム)]フィールドにセキュリティアソシエーション(SA)の期間を秒単位で入力します。SAライフタイムは、いずれかのキーがライフタイムに達した時点で、関連するすべてのSAが自動的に再ネゴシエートされます。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-128

Integrity Algorithm:

PFS Key Group: AES-128

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

ステップ2:[Encryption Algorithm]ドロップダウンリストから適切な暗号化アルゴリズムを選択します。

- ・ DES:Data Encryption Standard (DES ; データ暗号規格) では、データ暗号化に56ビットキーサイズを使用します。DESは古いため、1つのエンドポイントがDESのみをサポートしている場合にのみ使用する必要があります。
- ・ 3DES — Triple Data Encryption Standard(3DES)は、DESを3回実行しますが、実行されたDESのラウンドに基づいて、キーサイズを168ビットから112ビット、112ビットから56ビットに変更します。3DESはDESやAESよりも安全です。
- ・ 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よりも高速ですが、安全性は低いのですが、一部のタイプのハードウェアでは3DESの高速化が可能です。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、安全性は高く、AES-192はAES-256よりも高速ですが、安全性は低くなります。
- ・ 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。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: SHA-1

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

ステップ3:[Integrity Algorithm]ドロップダウンリストから適切な整合性アルゴリズムを選択します。このアルゴリズムは、データの整合性を検証します。

- ・ MD5 : このアルゴリズムは、キーの長さを16文字に指定します。Message-Digest Algorithm 5(MD5)はコリジョンに強くないため、このプロパティに依存するSSL証明書やデジタル署名などのアプリケーションに適しています。MD5はバイトストリームを128ビット値に圧縮しますが、

SHAは160ビット値に圧縮します。MD5は計算する方が若干安価ですが、MD5はハッシュアルゴリズムの古いバージョンであり、衝突攻撃に対して脆弱です。

- ・ SHA1 — Secure Hash Algorithm version 1(SHA1)は160ビットのハッシュ関数で、MD5よりも安全ですが、計算に時間がかかります。
- ・ SHA2-256 : このアルゴリズムは、キーの長さを32文字に指定します。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

ステップ4: (オプション) [PFS Key Group]フィールドの[Enable]チェックボックスをオンにして、*Perfect Forward Secrecy* (完全転送秘密) を有効にします。これはセキュリティを向上させるためです。

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: Enable

Select IKE Policy: policy1

DH-Group 1(768 bit)

DH-Group 1(768 bit)

DH-Group 2(1024 bit)

DH-Group 5(1536 bit)

View

ステップ5 : ステップ4で[Enable]をオンにした場合は、[PFS Key Group]フィールドのドロップダウンリストから適切なDiffie-Hellmanキー交換を選択します。

- ・ 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。

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

ステップ6:[Select IKE Policy]ドロップダウンリストから適切なIKEポリシーを選択します。
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。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7:[Save]をクリックして、すべての設定を適用します。

注：接続が成功するには、SA -Lifetime、Encryption Algorithm、Integrity Algorithm、PFSキーグループ、およびIKEポリシーが、VPNトンネルの反対側で同じである必要があります。

RV110Wに関する記事を表示する場合は、[ここをクリックしてください](#)。