

# 在RV110W防火墙上配置高级虚拟专用网络 (VPN)设置

## 目标

虚拟专用网络(VPN)使用公共网络或Internet建立专用网络以安全地通信。Internet密钥交换(IKE)是在两个网络之间建立安全通信的协议。它用于在流量传输之前交换密钥，确保VPN隧道两端的真实性。

VPN两端应遵循相同的VPN策略，以便成功相互通信。

本文档的目标是说明如何在RV110W无线路由器上添加IKE配置文件和配置VPN策略。

## 适用设备

·RV110W

## 软件版本

·1.2.0.9

## IKE策略设置

互联网密钥交换(IKE)是用于在VPN中建立通信安全连接的协议。此已建立的安全连接称为安全关联(SA)。此过程说明如何为VPN连接配置IKE策略以用于安全。要使VPN正常运行，两个端点的IKE策略应相同。

步骤1.登录到Web配置实用程序，然后选择VPN > Advanced VPN Setup。“高级VPN设置”页打开：

Advanced VPN Setup

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

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

Save Cancel

IPSec Connection Status

Advanced VPN Setup

IKE Policy Table				
<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"/>				

VPN Policy Table				
<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"/>				

步骤2.单击Add Row 以创建新的IKE策略。“高级VPN设置”页打开：

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)

步骤3.在Policy Name字段中，输入IKE策略的名称以便轻松识别。

### 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)

步骤4.从Exchange Mode下拉列表中选择选项：

·Main — 允许IKE策略比主动模式更安全地运行，但速度更慢。如果需要更安全的VPN连接，请选择此选项。

·主动 — 允许IKE策略比主模式运行更快，但安全性较低。如果需要更快的VPN连接，请选择此选项。

**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)

步骤5.从Encryption Algorithm下拉列表中选择算法：

- DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持DES 时，才应使用此方法。
- 3DES — 三重数据加密标准(3DES)执行DES三次，但根据执行的DES轮次，密钥大小从168位变为112位，从112位变为56位。3DES比DES和AES更安全。
- AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，AES也比3DES更快，但安全性较低，但某些类型的硬件使3DES更快。AES-128比AES-192和AES-256更快，但安全性较低。
- AES-192 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，而AES-192比AES-256快但不安全。
- AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

### 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)

步骤6.从Authentication Algorithm下拉列表中选择所需的身份验证：

·MD5 — 消息摘要算法5(MD5)使用128位哈希值进行身份验证。MD5的安全性较低，但比SHA-1和SHA2-256快。

·SHA-1 — 安全哈希函数1(SHA-1)使用160位哈希值进行身份验证。SHA-1比MD5慢但更安全，而SHA-1比SHA2-256快但不安全。

·SHA2-256 — 具有256位哈希值(SHA2-256)的安全哈希算法2使用256位哈希值进行身份验证。SHA2-256比MD5和SHA-1慢但安全。

### 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)

步骤7.在Pre-Shared Key字段中，输入IKE策略使用的预共享密钥。

### 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)

步骤8.从Diffie-Hellman(DH)Group下拉列表中，选择IKE使用的DH组。DH组中的主机可以在彼此不知情的情况下交换密钥。组位数越高，组就越安全。

·组1 - 768位 — 强度最低的密钥和最不安全的身份验证组。但是，它需要更少的时间来计算 IKE 密钥。如果网络速度较慢，则首选此选项。



·组2 - 1024位 — 强度较高的密钥和更安全的身份验证组。但是，它需要一些时间来计算 IKE 密钥。

·组5 - 1536位 — 表示最高强度的密钥和最安全的身份验证组。它需要更多时间来计算 IKE 密钥。如果网络速度较快，则首选此选项。

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)

步骤9.在SA-Lifetime字段中，输入VPN的SA在续约SA之前的持续时间(秒)。

第10步。(可选)选中Dead Peer Detection字段中的**Enable**复选框以启用Dead Peer Detection。契对端检测监控IKE对等体，查看对等体是否已停止运行。失效对等体检测可防止网络资源浪费在非活动对等体上。

第11步。(可选)如果在第9步中启用了契据对等体检测，请在“契据对等体延迟”字段中输入检查对等体活动的频率(秒)。

第12步。(可选)如果在第9步中启用了Ded Peer Detection，请在Ded Peer Detection Timeout字段中输入在丢弃非活动对等体之前等待的秒数。

步骤13.单击“保存”以应用所有设置。

## VPN策略配置

步骤1.登录Web配置实用程序并选择VPN> **Advanced VPN Setup (高级VPN设置)**。“高级VPN设置”页打开：

**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

步骤2.从VPN策略表中单击“添加行”。系统将显示Advanced VPN Policy Setup窗口：

**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:  ▼

IP Address:  (Hint: 1.2.3.4)



## 添加/编辑VPN策略配置



Advanced VPN Setup

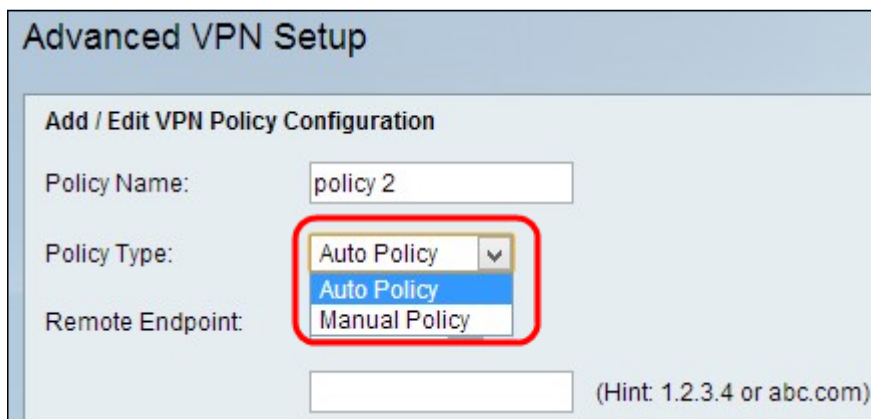
Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

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

步骤1.在Policy Name字段中为策略输入唯一的名称，以便轻松识别。



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

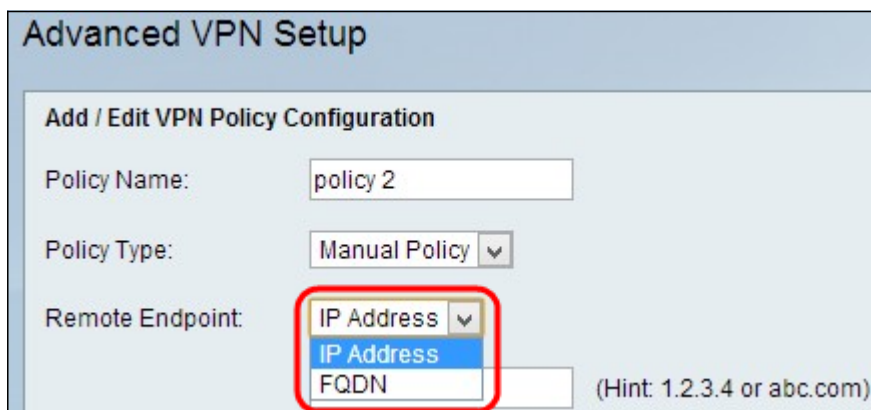
Policy Type:

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

步骤2.从Policy Type下拉列表中选择适当的策略类型。

·自动策略 — 可以自动设置参数。在这种情况下，除策略外，还需要IKE（互联网密钥交换）协议在两个VPN终端之间进行协商。

·手动策略 — 在这种情况下，包括VPN隧道密钥设置的所有设置都为每个终端手动输入。



Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

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

步骤3.从Remote Endpoint下拉列表中选择用于标识远程终端处网关的IP标识符的类型。

·IP Address — 远程终端上网关的IP地址。如果选择此选项，请在字段中输入IP地址。

·FQDN（完全限定域名） — 输入远程终端上网关的完全限定域名。如果选择此选项，请在提供的字段中输入完全限定域名。

### 本地流量选择

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

步骤1.从Local IP (本地IP) 下拉列表中选择要为终端提供的标识符类型。

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·单一 — 这将策略限制为一台主机。如果选择此选项，请在IP地址字段中输入IP地址。

**Local Traffic Selection**

Local IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·子网 — 这是定义IP边界的掩码。这仅允许指定子网中的主机连接到VPN。要连接到VPN，计算机通过逻辑AND操作进行选择。如果IP位于所需的相同范围，则选择计算机。如果选择此选项，请在IP地址和子网字段中输入IP地址和子网。

## 远程流量选择

**Remote Traffic Selection**

Remote IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

步骤1.从本地IP下拉列表中选择要为终端提供的标识符的类型：

**Remote Traffic Selection**

Remote IP:  (Hint: 1.2.3.4)

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

·单一 — 这将策略限制为一台主机。如果选择此选项，请在IP地址字段中输入IP地址。

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)

·子网 — 这是定义IP边界的掩码。这仅允许指定子网中的主机连接到VPN。要连接到VPN，计算机通过逻辑AND操作进行选择。如果IP位于所需的相同范围，则选择计算机。如果选择此选项，请在IP地址和子网字段中输入IP地址和子网。

## 手动策略参数

要配置手动策略参数，请从“添加/编辑VPN策略配置”部分的策略类型下拉列表中选择“手动策略”。

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:	

步骤1.在SPI-Incoming字段中输入一个介于3和8之间的十六进制值。状态包检测(SPI)是一种称为深度包检测的技术。SPI实施了许多安全功能，有助于保证计算机网络安全。SPI-Incoming值与上一设备的SPI-Outgoing对应。如果远程VPN终端的SPI-Outgoing字段中具有相同的值，则任何值都可接受。

步骤2.在“SPI-Outgoing”字段中输入一个介于3和8之间的十六进制值。

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="014C"/>
SPI-Outgoing:	<input type="text" value="014C"/>
Encryption Algorithm:	<div style="border: 2px solid red; padding: 2px;">           AES-128 ▼            3DES            DES            AES-128            AES-192            AES-256         </div>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	SHA-1 ▼
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

步骤3.从Encryption Algorithm下拉列表中选择适当的加密算法。

·DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持DES 时，才应使用此方法。

·3DES — 三重数据加密标准(3DES)执行DES三次，但根据执行的DES轮，密钥大小从168位到112位，从112位到56位不等。3DES比DES和AES更安全。

·AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，AES也比3DES更快，但安全性较低，但某些类型的硬件使3DES更快。AES-128比AES-192和AES-256更快，但安全性较低。

·AES-192 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，而AES-192比AES-256快但不安全。

·AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="014C"/>
SPI-Outgoing:	<input type="text" value="014C"/>
Encryption Algorithm:	DES ▼
Key-In:	<input style="border: 2px solid red;" type="text" value="1452"/>
Key-Out:	<input style="border: 2px solid red;" type="text" value="1452"/>
Integrity Algorithm:	SHA-1 ▼
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

步骤4.在Key-In字段中输入入站策略的加密密钥。密钥的长度取决于步骤3中选择的算法。

步骤5.在Key-Out字段中输入出站策略的加密密钥。

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="014C"/>
SPI-Outgoing:	<input type="text" value="014C"/>
Encryption Algorithm:	<div style="border: 2px solid red; padding: 2px;">           AES-128 ▼            3DES            DES            AES-128            AES-192            AES-256         </div>
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>
Integrity Algorithm:	SHA-1 ▼
Key-In:	<input type="text"/>
Key-Out:	<input type="text"/>

步骤6.从Integrity Algorithm下拉列表中选择适当的完整性算法。此算法将验证数据的完整性：

- MD5 — 此算法将密钥长度指定为16个字符。消息摘要算法五(MD5)不防冲突，适用于依赖此属性的SSL证书或数字签名等应用。MD5将任何字节流压缩为128位值，但SHA将其压缩为160位值。MD5的计算成本稍低，但MD5是哈希算法的较旧版本，容易受到冲突攻击。

- SHA1 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全，但计算时间更长。

- SHA2-256 — 此算法将密钥长度指定为32个字符。

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="014C"/>
SPI-Outgoing:	<input type="text" value="014C"/>
Encryption Algorithm:	DES ▼
Key-In:	<input type="text" value="1452"/>
Key-Out:	<input type="text" value="1452"/>
Integrity Algorithm:	SHA2-256 ▼
Key-In:	<input style="border: 2px solid red;" type="text" value="1234"/>
Key-Out:	<input style="border: 2px solid red;" type="text" value="1234"/>

步骤7.输入入站策略的完整性密钥（对于具有完整性模式的ESP）。密钥的长度取决于步骤6中选择的算法。

步骤8.在Key-Out字段中输入出站策略的完整性密钥。VPN连接已设置为出站到入站，因此来自一端的出站密钥需要匹配另一端的入站密钥。

**注意：** SPI传入和传出、加密算法、完整性算法和密钥在VPN隧道的另一端需要相同才能成功连接。

。

## 自动策略参数



**Auto Policy Parameters**

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

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable  
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步骤1.在SA Lifetime字段中输入安全关联(SA)的持续时间 (以秒为单位)。SA生存期是指当任何密钥达到其生存期时，自动重新协商任何相关的SA。

**Auto Policy Parameters**

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

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

PFS Key Group:  Enable  
DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步骤2.从Encryption Algorithm下拉列表中选择适当的Encryption Algorithm:

- DES — 数据加密标准(DES)使用56位密钥大小进行数据加密。DES 已过时，仅当一个终端仅支持DES 时，才应使用此方法。
- 3DES — 三重数据加密标准(3DES)执行DES三次，但根据执行的DES轮，密钥大小从168位到112位，从112位到56位不等。3DES比DES和AES更安全。
- AES-128 — 高级加密标准，带128位密钥(AES-128)，使用128位密钥进行AES加密。AES比DES更快、更安全。通常，AES也比3DES更快，但安全性较低，但某些类型的硬件使3DES更快。AES-128比AES-192和AES-256更快，但安全性较低。
- AES-192 - AES-192使用192位密钥进行AES加密。AES-192比AES-128慢但更安全，而AES-192比AES-256快但不安全。
- AES-256 - AES-256使用256位密钥进行AES加密。AES-256比AES-128和AES-192慢，但更安全。

**Auto Policy Parameters**

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

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group: (empty)

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

步骤3.从Integrity Algorithm下拉列表中选择适当的Integrity Algorithm。此算法验证数据的完整性。

·MD5 — 此算法将密钥长度指定为16个字符。消息摘要算法五(MD5)不防冲突，适用于依赖此属性的SSL证书或数字签名等应用。MD5将任何字节流压缩为128位值，但SHA将其压缩为160位值。MD5的计算成本稍低，但MD5是哈希算法的较旧版本，容易受到冲突攻击。

·SHA1 — 安全散列算法版本1(SHA1)是160位散列函数，比MD5更安全，但计算时间更长。

·SHA2-256 — 此算法将密钥长度指定为32个字符。

**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

步骤4. ( 可选 ) 选中PFS Key Group ( PFS密钥组 ) 字段中的Enable ( 启用 ) 复选框，以启用完全向前保密 ( 即提高安全性 )。

**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: (empty)

View

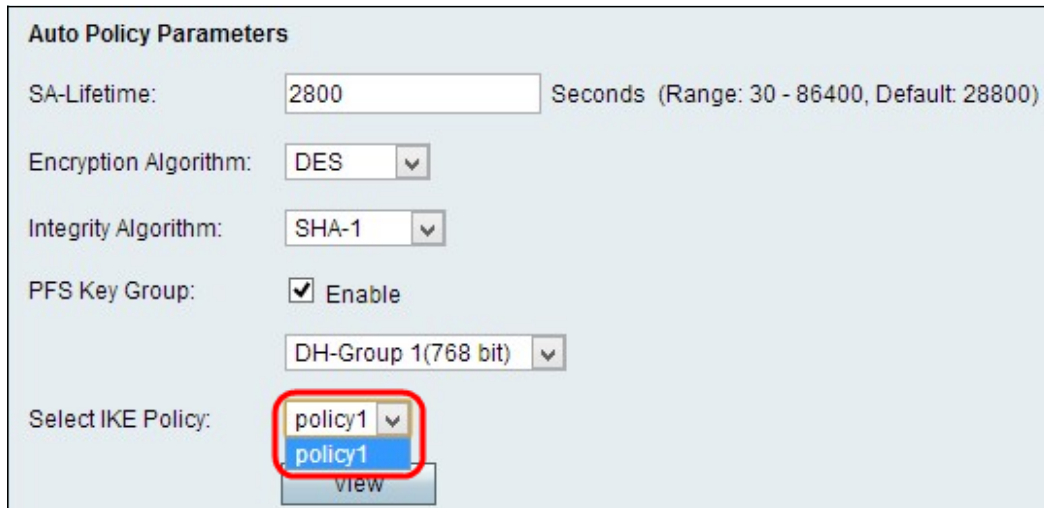
步骤5.如果在步骤4中选中了启用，请从PFS Key Group字段下拉列表中选择适当的Diffie-

Hellman密钥交换。

·组1 - 768位 — 表示强度最低的密钥和最不安全的身份验证组。但是，它需要更少的时间来计算 IKE 密钥。如果网络速度较慢，则首选此选项。

·组2 - 1024位 — 表示更高强度的密钥和更安全的身份验证组。但是，它需要一些时间来计算 IKE 密钥。

·组5 - 1536位 — 表示最高强度的密钥和最安全的身份验证组。它需要更多时间来计算 IKE 密钥。如果网络速度较快，则首选此选项。



The screenshot shows the 'Auto Policy Parameters' configuration window. The 'Select IKE Policy' dropdown menu is open, showing 'policy1' as the selected option. A red circle highlights the dropdown menu. The other parameters are: SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800); Encryption Algorithm: DES; Integrity Algorithm: SHA-1; PFS Key Group: Enable (checked); DH-Group 1(768 bit); and a 'view' button below the dropdown.

步骤6.从Select IKE Policy下拉列表中选择适当的IKE Policy。互联网密钥交换(IKE)是用于在VPN中建立通信安全连接的协议。此已建立的安全连接称为安全关联(SA)。要使VPN正常运行，两个端点的IKE策略应相同。

步骤7.单击“保存”以应用所有设置。

**注意：**SA -Lifetime、Encryption Algorithm、Integrity Algorithm、PFS密钥组和IKE策略需要在VPN隧道的另一端相同才能成功连接。

如果您想查看有关RV110W的更多文章，请单击[此处](#)。