

# Configuring IKEv2 on the RV34x Series Router

## Objective

The objective of this document is to show you how to configure IPsec Profile with IKEv2 on RV34x series routers.

## Introduction

Firmware version 1.0.02.16 for RV34x series routers now supports Internet Key Exchange Version 2 (IKEv2) for site-to-site VPN and client-to-site VPN. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the Internet Security Association and Key Management Protocol (ISAKMP) framework. IKE provides authentication of the IPsec peers, negotiates IPsec keys, and negotiates IPsec security associations.

IKEv2 still utilizes UDP port 500, but there are some changes to note. Dead Peer Detection (DPD) is managed differently and is now built-in. Security Association (SA) negotiation is minimized down to 4 messages. This new update also supports Extensible Authentication Protocol (EAP) authentication which is now able to leverage an AAA server and Denial of Service protection.

The table below further illustrates the differences between IKEv1 and IKEv2

IKEv1	IKEv2
SA Two Phase Negotiation (Main Mode vs Aggressive Mode)	SA Single Phase Negotiation (Simplified)
	Local/Remote Certificate Support
	Improved collision handling
	Improved rekeying mechanics
	NAT traversal built-in
	EAP support for AAA servers

IPsec ensures that you have secure private communication over the Internet. It gives two or more hosts privacy, integrity, and authenticity for transmitting sensitive information over the Internet. IPsec is commonly used in a Virtual Private Network (VPN) and is implemented at the IP layer which helps add security to many unsecure applications. A VPN is used to provide a secure communication mechanism for sensitive data and IP information that is transmitted through an unsecure network such as the Internet. It also provides a flexible solution for remote users and the organization to protect any sensitive information from other parties on the same network.

In order for the two ends of a VPN tunnel to be successfully encrypted and established, they both need to agree on the methods of encryption, decryption, and authentication. An IPsec profile is the central configuration in IPsec that defines the algorithms such as encryption, authentication, and Diffie-Hellman (DH) group for Phase I and II negotiation in auto mode as well as manual keying

mode. Phase I establishes the pre-shared keys to create a secure authenticated communication. Phase II is where the traffic gets encrypted. You can configure most of the IPsec parameters such as protocol (Encapsulation Security Payload (ESP)), Authentication Header (AH), mode (tunnel, transport), algorithms (encryption, integrity, Diffie-Hellman), Perfect Forward Secrecy (PFS), SA lifetime, and key management protocol (Internet Key Exchange (IKE) – IKEv1 and IKEv2).

Additional information about Cisco IPsec technology can be found in this link: [Introduction to Cisco IPsec Technology](#).

It is important to note that when you are configuring site-to-site VPN, the remote router requires the same IPsec profile configuration as your local router.

Below is a table of the configuration for both the local router and remote router. In this document, we will be configuring the local router using Router A.

<b>Fields</b>	<b>Local Router (Router A)</b>	<b>Remote Router (Router B)</b>
Profile Name	HomeOffice	RemoteOffice
Keying Mode	Auto	Auto
IKE Version	IKEv2	IKEv2
<b>Phase I Options</b>	<b>Phase I Options</b>	<b>Phase I Options</b>
DH Group	Group2 – 1024 bit	Group2 – 1024 bit
Encryption	AES-192	AES-192
Authentication	SHA2-256	SHA2-256
SA Lifetime	28800	28800
<b>Phase II Options</b>	<b>Phase II Options</b>	<b>Phase II Options</b>
Protocol Selection	ESP	ESP
Encryption	AES-192	AES-192
Authentication	SHA2-256	SHA2-256
SA Lifetime	3600	3600
Perfect Forward Secrecy	Enabled	Enabled
DH Group	Group2 – 1024 bit	Group2 – 1024 bit

To learn how to configure site-to-site VPN on the RV34x, click the link: [Configuring Site-to-Site VPN on the RV34x](#).

#### Applicable Devices

- RV34x

#### Software Version

- 1.0.02.16

#### Configuring IPsec Profile with IKEv2

Step 1. Log in to the web configuration page of your local router (Router A).



# Router

cisco



English

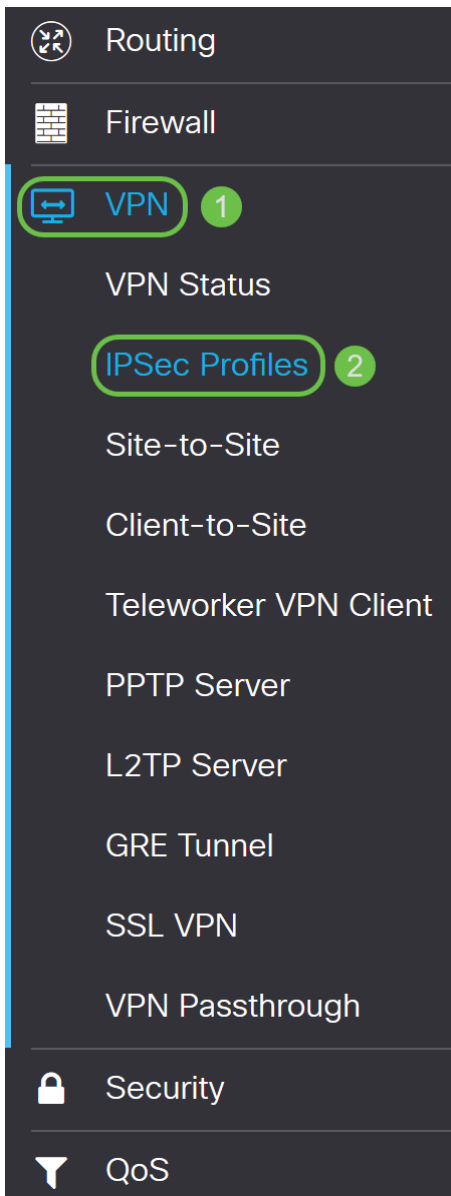


Login

©2017-2018 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Step 2. Navigate to **VPN > IPSec Profiles**.



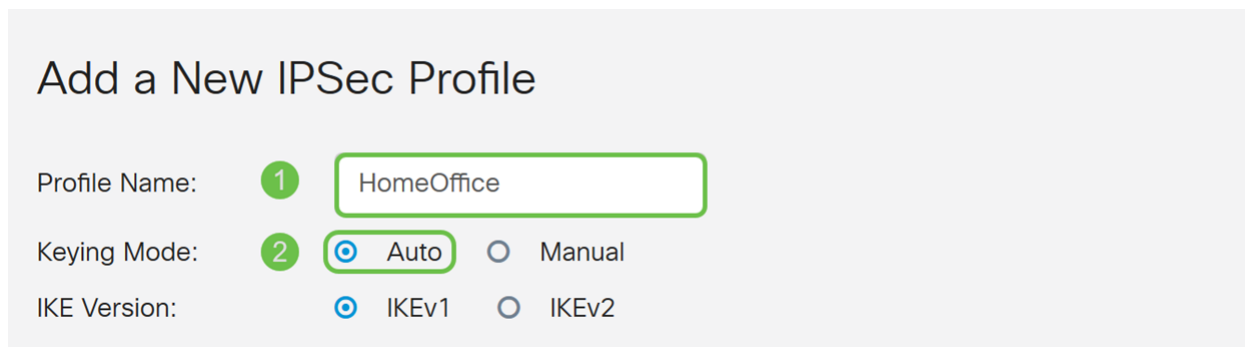
Step 3. In the *IPSec Profiles* table, click **Add** to create a new IPsec profile. There are also options to edit, delete, or clone a profile. Cloning a profile allows you to quickly duplicate a profile that already exists in the *IPSec Profiles Table*. If you ever need to create multiple profiles with the same configuration, cloning would save you some time.

<input type="checkbox"/> Name	IKE Version	Policy	In Use
<input type="checkbox"/> Amazon_Web_Services	IKEv1	Auto	No
<input type="checkbox"/> Default	IKEv1	Auto	Yes
<input type="checkbox"/> Microsoft_Azure	IKEv1	Auto	No

Step 4. Enter a profile name and select the keying mode (Auto or Manual). The profile name does not have to match with your other router but the keying mode needs to match.

**HomeOffice** is entered as the *Profile Name*.

**Auto** is selected for *Keying Mode*.



Add a New IPsec Profile

Profile Name:

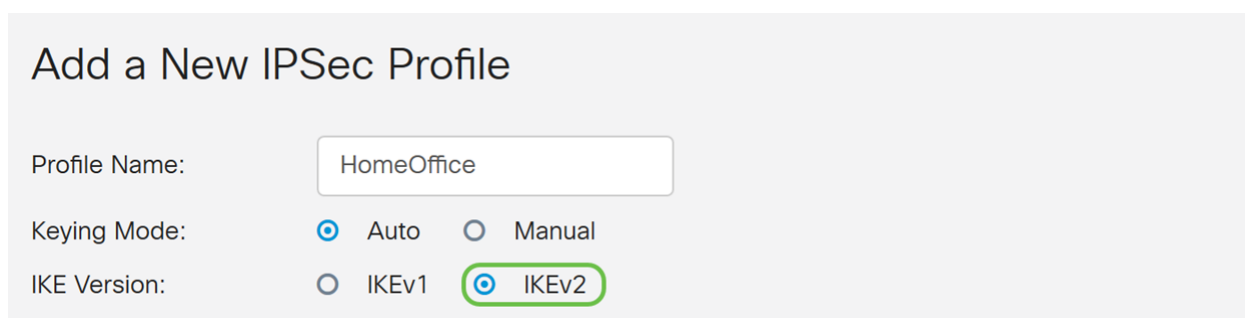
Keying Mode:  Auto  Manual

IKE Version:  IKEv1  IKEv2

Step 5. Choose **IKEv1** or **IKEv2** as your *IKE Version*. IKE is a hybrid protocol that implements the Oakley key exchange and the Skeme key exchange inside the ISAKMP framework. Oakley and Skeme both define how to derive authenticated keying material, but Skeme also includes rapid key refreshment. IKEv2 is more efficient because it takes less packets to do the key exchanges, and supports more authentication options, while IKEv1 only does shared key and certificate based authentication.

In this example, **IKEv2** was selected as our IKE version.

**Note:** If your devices support IKEv2 then it is recommended to use IKEv2. If your devices don't support IKEv2 then use IKEv1.



Add a New IPsec Profile

Profile Name:

Keying Mode:  Auto  Manual

IKE Version:  IKEv1  IKEv2

Step 6. Phase I sets up and exchanges the keys you will be using to encrypt data in phase II. In the *Phase I* section, select a DH group. DH is a key exchange protocol, with two groups of different prime key lengths, **Group 2 – 1024 bit** and **Group 5 – 1536 bit**.

**Group 2 – 1024 bit** was selected for this demonstration.

**Note:** For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected as default.

## Phase I Options

DH Group:	<input type="text" value="Group2 - 1024 bit"/>	
Encryption:	<input type="text" value="3DES"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="28800"/>	sec. (Range: 120 - 86400, Default: 28800)

Step 7. Select an encryption option (**3DS**, **AES-128**, **AES-192**, or **AES-256**) from the drop-down list. This method determines the algorithm used to encrypt and decrypt ESP/ISAKMP packets. Triple Data Encryption Standard (3DES) uses DES encryption three times but is now a legacy algorithm and should only be used when there are no other alternatives, since it still provides a marginal but acceptable security level. Users should only use it if it's required for backwards compatibility as it's vulnerable to some "block collision" attacks. Advanced Encryption Standard (AES) is a cryptographic algorithm that is designed to be more secure than DES. AES uses a larger key size which ensures that the only known approach to decrypt a message is for an intruder to try every possible key. It is recommended to use AES if your device can support it.

In this example, we selected **AES-192** as our encryption option.

**Note:** Click on the hyperlinks for additional information on [Configuring Security for VPNs with IPsec](#) or [Next Generation Encryption](#).

## Phase I Options

DH Group:	<input type="text" value="Group2 - 1024 bit"/>	
Encryption:	<input type="text" value="AES-192"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="28800"/>	sec. (Range: 120 - 86400, Default: 28800)

Step 8. The authentication method determines how the ESP header packets are validated. This is the hashing algorithm used in the authentication to validate that side A and side B really are who they say they are. The MD5 is a one-way hashing algorithm that produces a 128-bit digest and is faster than SHA1. The SHA1 is a one-way hashing algorithm that produces a 160-bit digest while SHA2-256 produces a 256-bit digest. SHA2-256 is recommended because it is more secure. Make sure that both ends of the VPN tunnel use the same authentication method. Select an authentication (**MD5**, **SHA1**, or **SHA2-256**).

**SHA2-256** was selected for this example.

## Phase I Options

DH Group:	Group2 - 1024 bit	▼
Encryption:	AES-192	▼
Authentication:	SHA2-256	▼
SA Lifetime:	28800	sec. (Range: 120 - 86400, Default: 28800)

Step 9. The *SA Lifetime (Sec)* tells you the amount of time an IKE SA is active in this phase. When the SA expires after the respective lifetime, a new negotiation begins for a new one. The range is from 120 to 86400 and the default is 28800.

We will be using the default value of **28800** seconds as our SA Lifetime for Phase I.

**Note:** It is recommended that your SA Lifetime in Phase I is longer than your Phase II SA Lifetime. If you make your Phase I shorter than Phase II, then you will be having to renegotiate the tunnel back and forth frequently as opposed to the data tunnel. Data tunnel is what needs more security so it is better to have the lifetime in Phase II to be shorter than Phase I.

## Phase I Options

DH Group:	Group2 - 1024 bit	▼
Encryption:	AES-192	▼
Authentication:	SHA2-256	▼
SA Lifetime:	28800	sec. (Range: 120 - 86400, Default: 28800)

Step 10. Phase II is where you would be encrypting the data that is being passed back and forth. In the *Phase 2 Options*, select a protocol from the drop-down list:

- Encapsulating Security Payload (ESP) – Select ESP for data encryption and enter the encryption.
- Authentication Header (AH) – Select this for data integrity in situations where data is not secret, in other words, it is not encrypted but must be authenticated. It is only used to validate the source and destination of the traffic.

In this example, we will be using **ESP** as our *Protocol Selection*.

## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="3DES"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Step 11. Select an encryption option (**3DES**, **AES-128**, **AES-192**, or **AES-256**) from the drop-down list. This method determines the algorithm used to encrypt and decrypt ESP/ISAKMP packets.

In this example, we will use **AES-192** as our encryption option.

**Note:** Click on the hyperlinks for additional information on [Configuring Security for VPNs with IPsec](#) or [Next Generation Encryption](#).

## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	
Encryption:	<input type="text" value="AES-192"/>	
Authentication:	<input type="text" value="MD5"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Step 12. The authentication method determines how the Encapsulating Security Payload Protocol (ESP) header packets are validated. Select an authentication (**MD5**, **SHA1**, or **SHA2-256**).

**SHA2-256** was selected for this example.



## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	sec. (Range: 120 - 28800, Default: 3600)
Encryption:	<input type="text" value="AES-192"/>	
Authentication:	<input type="text" value="SHA2-256"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Step 13. Enter the amount of time a VPN tunnel (IPsec SA) is active in this phase. The default value for Phase 2 is 3600 seconds. We will be using the default value for this demonstration.

## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	sec. (Range: 120 - 28800, Default: 3600)
Encryption:	<input type="text" value="AES-192"/>	
Authentication:	<input type="text" value="SHA2-256"/>	
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	

Step 14. Check **Enable** to enable the perfect forward secrecy. When Perfect Forward Secrecy (PFS) is enabled, IKE Phase 2 negotiation generates new key material for IPsec traffic encryption and authentication. PFS is used to improve the security of communications transmitted across the Internet using public key cryptography. This is recommended if your device can support it.

## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	▼
Encryption:	<input type="text" value="AES-192"/>	▼
Authentication:	<input type="text" value="SHA2-256"/>	▼
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	▼

Step 15. Select a Diffie-Hellman (DH) Group. DH is a key exchange protocol, with two groups of different prime key lengths, **Group 2 - 1024 bit** and **Group 5 - 1536 bit**. We selected **Group 2 - 1024 bit** for this demonstration.

**Note:** For faster speed and lower security, choose Group 2. For slower speed and higher security, choose Group 5. Group 2 is selected by default.

## Phase II Options

Protocol Selection:	<input type="text" value="ESP"/>	▼
Encryption:	<input type="text" value="AES-192"/>	▼
Authentication:	<input type="text" value="SHA2-256"/>	▼
SA Lifetime:	<input type="text" value="3600"/>	sec. (Range: 120 - 28800, Default: 3600)
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable	
DH Group:	<input type="text" value="Group2 - 1024 bit"/>	▼

Step 16. Click **Apply** to add a new IPsec profile.

### IPSec Profiles

Encryption:

Authentication:

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

### Phase II Options

Protocol Selection:

Encryption:

Authentication:

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

Perfect Forward Secrecy:  Enable

DH Group:

Step 17. After clicking *Apply*, your new IPsec profile should be added.

### IPSec Profiles

IPSec Profiles Table

<input type="checkbox"/> Name	IKE Version	Policy	In Use
<input type="checkbox"/> Amazon_Web_Services	IKEv1	Auto	No
<input type="checkbox"/> Default	IKEv1	Auto	Yes
<input type="checkbox"/> Microsoft_Azure	IKEv1	Auto	No
<input checked="" type="checkbox"/> HomeOffice	IKEv2	Auto	No

Step 18. At the top of the page, click the **Save** icon to navigate to the *Configuration Management* to save your running configuration to the startup configuration. This is to retain the configuration between reboots.



Step 19. In the *Configuration Management*, make sure the *Source* is **Running Configuration** and the *Destination* is **Startup Configuration**. Then press **Apply** to save your running configuration to the startup configuration. All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. Copying the running configuration file to the startup configuration file will retain all the configuration between reboots.

Configuration Management 3 Apply Cancel Disabled Save Icon Blinking

### Configuration File Name

Last Change Time

Running Configuration: 2018-Dec-08, 00:17:01 GMT  
Startup Configuration: 2018-Dec-07, 21:54:43 GMT  
Mirror Configuration: 2018-Dec-07, 21:54:33 GMT  
Backup Configuration: N/A

---

### Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

Source:  1

Destination:  2

Save Icon Blinking: Enabled

Step 20. Follow all steps again to set up Router B.

## Conclusion

You should now have successfully created a new IPsec profile using IKEv2 as your IKE version for both routers. You are ready to configure a site-to-site VPN.