

Configuration of an IPSec VPN Server on RV130 and RV130W

Objective

IPSec VPN (Virtual Private Network) enables you to securely obtain remote access to corporate resources by establishing an encrypted tunnel across the Internet.

The objective of this document is to show you how to configure an IPSec VPN Server on RV130 and RV130W.

Note: For information about how to configure an IPSec VPN Server with the Shrew Soft VPN Client on RV130 and RV130W, refer to the article [Use Shrew Soft VPN Client with IPSec VPN Server on RV130 and RV130W](#).

Applicable Devices

- RV130W Wireless-N VPN Firewall
- RV130 VPN Firewall

Software Version

- v1.0.1.3

Setup IPSec VPN Server

Step 1. Log in to the web configuration utility and choose **VPN > IPSec VPN Server > Setup**. The Setup page opens.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Phase 2 Configuration

Local IP: Single

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES

Authentication Algorithm: MD5

PFS Key Group: Enable

DH Group: Group 1(768 bit)

Step 2. Check the **Server Enable** checkbox to enable the certificate.

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Step 3. (Optional) If your VPN router or VPN Client is behind a NAT gateway, click **Edit** to configure NAT Traversal. Otherwise, leave NAT Traversal disabled.

Note: For more information about how to configure NAT Traversal settings, refer to [Internet Key Exchange \(IKE\) Policy Settings on RV130 and RV130W VPN Routers](#).

Setup

Server Enable:

NAT Traversal: Disabled

Phase 1 Configuration

Pre-Shared Key:

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Step 4. Enter a key between 8 to 49 characters long that will be exchanged between your device and the remote endpoint in the *Pre-Shared Key* field.

Phase 1 Configuration

Pre-Shared Key: Testkey

Exchange Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Step 5. From the *Exchange Mode* drop down list, choose the mode for the IPsec VPN connection. **Main** is the default mode. However, if your network speed is low, choose the **Aggressive** mode.

Server Enable:

Phase 1 Configuration

Pre-Shared Key: Testkey

Exchange Mode: Main
Main
Aggressive

Encryption Algorithm: DES

Authentication Algorithm: MD5

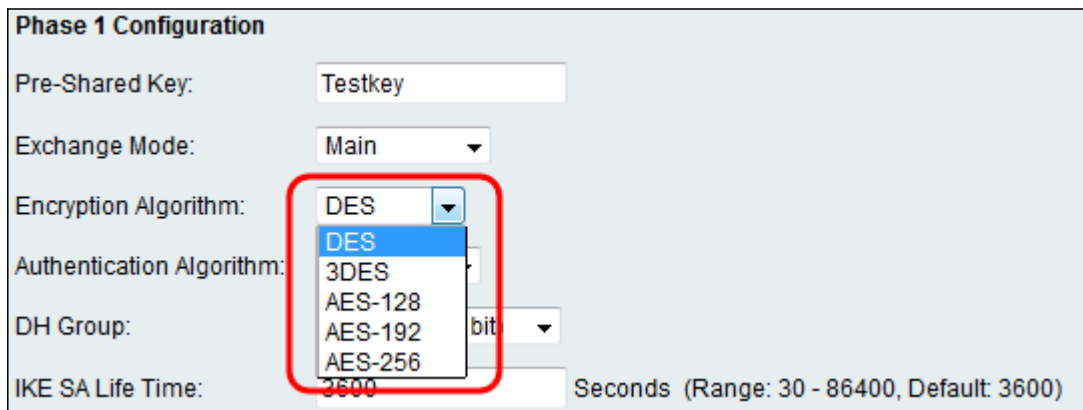
DH Group: Group1 (768 bit)

IKE SA Life Time: 3600 Seconds (Range: 30 - 86400, Default: 3600)

Note: Aggressive mode exchanges the IDs of the end points of the tunnel in clear text during the connection, which requires less time to exchange but is less secure.

Step 6. From the **Encryption Algorithm** drop-down list, choose the appropriate encryption

method to encrypt the Pre-Shared Key in Phase 1. AES-128 is recommended for its high security and fast performance. The VPN tunnel needs to use the same encryption method for both of its ends.

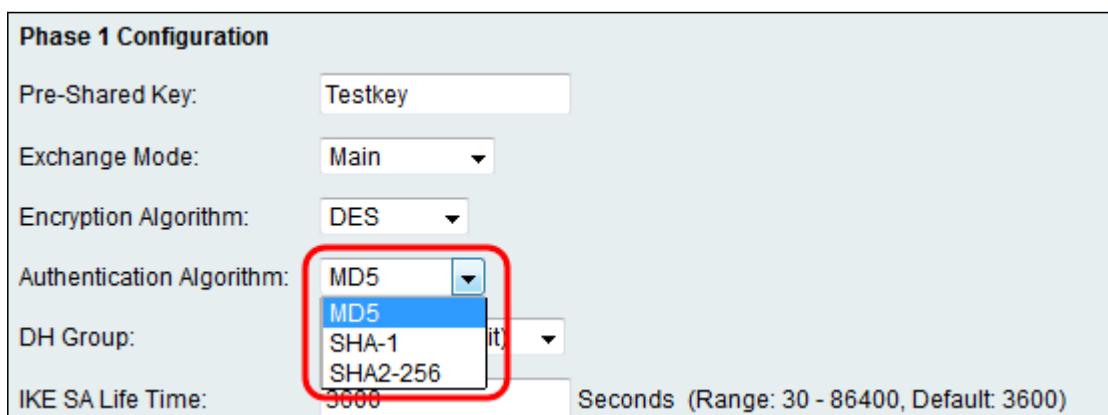


The screenshot shows the 'Phase 1 Configuration' dialog box. The 'Pre-Shared Key' is 'Testkey', 'Exchange Mode' is 'Main', and 'IKE SA Life Time' is '3600' seconds. The 'Encryption Algorithm' dropdown menu is open, showing options: DES, 3DES, AES-128, AES-192, and AES-256. The 'Authentication Algorithm' dropdown menu is also open, showing options: MD5, SHA-1, and SHA2-256. The 'DH Group' dropdown menu is open, showing options: 2048, 3072, 4096, 8192, and 16384. The 'IKE SA Life Time' is set to 3600 seconds, with a range of 30 to 86400 and a default of 3600.

The available options are defined as follows:

- DES — Data Encryption Standard (DES) is a 56-bit, old encryption method which is not very secure, but may be required for backwards compatibility.
- 3DES — Triple Data Encryption Standard (3DES) is a 168-bit, simple encryption method used to increase the key size because it encrypts the data three times. This provides more security than DES but less security than AES.
- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. In general, AES is also faster and more secure than 3DES. AES-128 is faster but less secure than AES-192 and AES-256.
- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and faster but less secure than AES-256.
- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

Step 7. From the *Authentication Algorithm* drop-down list, choose the appropriate authentication method to determine how the Encapsulating Security Payload (ESP) protocol header packets are validated in Phase 1. The VPN tunnel needs to use the same authentication method for both ends of the connection.



The screenshot shows the 'Phase 1 Configuration' dialog box. The 'Pre-Shared Key' is 'Testkey', 'Exchange Mode' is 'Main', and 'IKE SA Life Time' is '3600' seconds. The 'Encryption Algorithm' is set to 'DES'. The 'Authentication Algorithm' dropdown menu is open, showing options: MD5, SHA-1, and SHA2-256. The 'DH Group' dropdown menu is open, showing options: 2048, 3072, 4096, 8192, and 16384. The 'IKE SA Life Time' is set to 3600 seconds, with a range of 30 to 86400 and a default of 3600.

The available options are defined as follows:

- MD5 — MD5 is a one-way hashing algorithm that produces a 128-bit digest. MD5 computes faster than SHA-1, but is less secure than SHA-1. MD5 is not recommended.
- SHA-1 — SHA-1 is a one-way hashing algorithm that produces a 160-bit digest. SHA-1 computes slower than MD5, but is more secure than MD5.
- SHA2-256 — Specifies the Secure Hash Algorithm SHA2 with the 256-bit digest.

Step 8. From the *DH Group* drop-down list, choose the appropriate Diffie-Hellman (DH) group to be used with the key in Phase 1. Diffie-Hellman is a cryptographic key exchange protocol which is used in the connection to exchange pre-shared key sets. The strength of the algorithm is determined by bits.

The screenshot shows the 'Phase 1 Configuration' section of a network configuration interface. The fields are as follows:

- Pre-Shared Key: Testkey
- Exchange Mode: Main
- Encryption Algorithm: DES
- Authentication Algorithm: MD5
- DH Group: A dropdown menu is open, showing options: Group1 (768 bit), Group1 (768 bit), Group2 (1024 bit), and Group5 (1536 bit). The first 'Group1 (768 bit)' option is highlighted in blue.
- IKE SA Life Time: A text input field containing '3600' followed by the text 'Seconds (Range: 30 - 86400, Default: 3600)'. This entire row is circled in red.

The available options are defined as follows:

- Group1 (768-bit) — Computes the key the fastest, but is the least secure.
- Group2 (1024-bit) — Computes the key slower, but is more secure than Group1.
- Group5 (1536-bit) — Computes the key the slowest, but is the most secure.

Step 9. In the *IKE SA Life Time* field, enter the time, in seconds, that the automatic IKE key is valid. Once this time expires, a new key is negotiated automatically.

This screenshot is similar to the previous one, but the 'DH Group' dropdown is now closed and set to 'Group1 (768 bit)'. The 'IKE SA Life Time' field, which contains the value '3600' and the text 'Seconds (Range: 30 - 86400, Default: 3600)', is circled in red.

Step 10. From the *Local IP* drop down list, choose **Single** if you would like a single local LAN user to access the VPN tunnel, or choose **Subnet** if you would like multiple users to be able to access it.

Phase 2 Configuration

Local IP: Single ▼

IP Address: Single
Subnet (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Step 11. If **Subnet** was chosen in Step 10, enter the Network IP address of the sub-network in the IP Address field. If **Single** was chosen in Step 10, enter the IP address of the single user and skip to Step 13.

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

Step 12. (Optional) If **Subnet** was chosen in Step 10, enter the subnet mask of the local network in the *Subnet Mask* field.

Phase 2 Configuration

Local IP: Subnet ▼

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

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

Encryption Algorithm: DES ▼

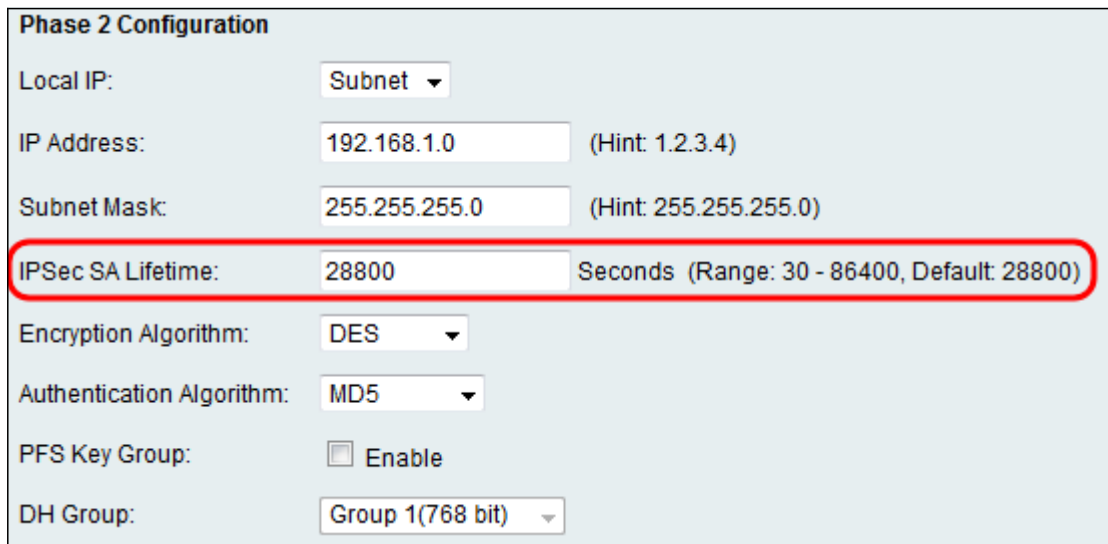
Authentication Algorithm: MD5 ▼

PFS Key Group: Enable

DH Group: Group 1(768 bit) ▼

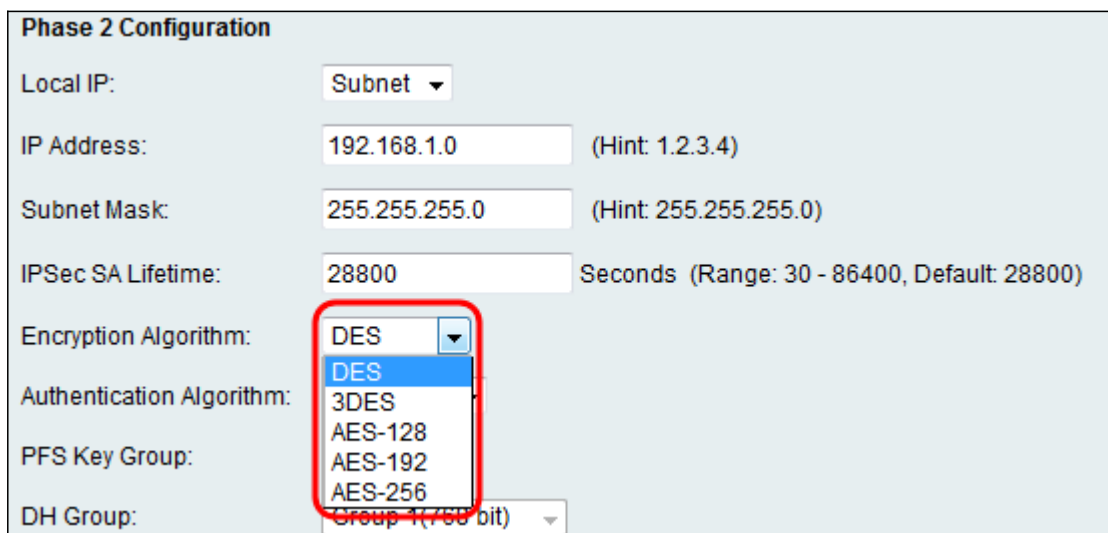
Step 13. In the *IPSec SA Lifetime* field, enter the time in seconds that the VPN connection

remains active in Phase 2. Once this time expires, the IPSec Security Association for the VPN connection is renegotiated.



The screenshot shows the 'Phase 2 Configuration' window. The 'IPsec SA Lifetime' field is highlighted with a red rectangle. The value is '28800' and the unit is 'Seconds (Range: 30 - 86400, Default: 28800)'. Other fields include 'Local IP' (Subnet), 'IP Address' (192.168.1.0), 'Subnet Mask' (255.255.255.0), 'Encryption Algorithm' (DES), 'Authentication Algorithm' (MD5), 'PFS Key Group' (unchecked), and 'DH Group' (Group 1(768 bit)).

Step 14. From the *Encryption Algorithm* drop-down list, choose the appropriate encryption method to encrypt the Pre-Shared key in Phase 2. AES-128 is recommended for its high security and fast performance. The VPN tunnel needs to use the same encryption method for both of its ends.



The screenshot shows the 'Phase 2 Configuration' window with the 'Encryption Algorithm' dropdown menu open. The dropdown list is highlighted with a red rectangle and shows the following options: DES, 3DES, AES-128, AES-192, and AES-256. The 'IPsec SA Lifetime' field is set to 28800. Other fields are the same as in the previous screenshot.

The available options are defined as follows:

- DES — Data Encryption Standard (DES) is a 56-bit, old encryption method which is the least secure, but may be required for backwards compatibility.
- 3DES — Triple Data Encryption Standard (3DES) is a 168-bit, simple encryption method used to increase the key size because it encrypts the data three times. This provides more security than DES but less security than AES.
- AES-128 — Advanced Encryption Standard with 128-bit key (AES-128) uses a 128-bit key for AES encryption. AES is faster and more secure than DES. In general, AES is also faster and more secure than 3DES. AES-128 is faster but less secure than AES-192 and AES-256.
- AES-192 — AES-192 uses a 192-bit key for AES encryption. AES-192 is slower but more secure than AES-128, and faster but less secure than AES-256.

- AES-256 — AES-256 uses a 256-bit key for AES encryption. AES-256 is slower but more secure than AES-128 and AES-192.

Step 15. From the *Authentication Algorithm* drop-down list, choose the appropriate authentication method to determine how the Encapsulating Security Payload (ESP) protocol header packets are validated in Phase 2. The VPN tunnel needs to use the same authentication method for both of its ends.

The screenshot shows the 'Phase 2 Configuration' window. The 'Authentication Algorithm' dropdown menu is open, showing options: MD5 (selected), MD5, SHA-1, and SHA2-256. A red box highlights the dropdown menu.

The available options are defined as follows:

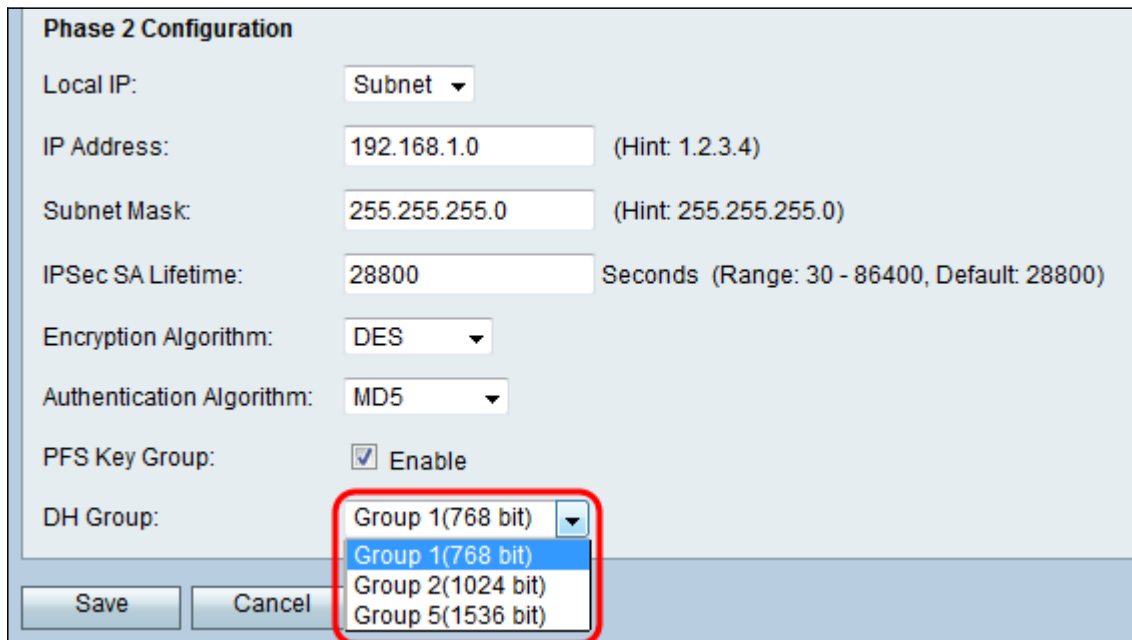
- MD5 — MD5 is a one-way hashing algorithm that produces a 128-bit digest. MD5 computes faster than SHA-1, but is less secure than SHA-1. MD5 is not recommended.
- SHA-1 — SHA-1 is a one-way hashing algorithm that produces a 160-bit digest. SHA-1 computes slower than MD5, but is more secure than MD5.
- SHA2-256 — Specifies the Secure Hash Algorithm SHA2 with the 256-bit digest.

Step 16. (Optional) In the *PFS Key Group* field, check the **Enable** checkbox. Perfect Forward Secrecy (PFS) creates an additional layer of security in protecting your data by ensuring a new DH key in Phase 2. The process is done in case the DH key generated in Phase 1 is compromised in transit.

The screenshot shows the 'Phase 2 Configuration' window. The 'PFS Key Group' field has the 'Enable' checkbox checked. A red box highlights the 'PFS Key Group' field.

Step 17. From the *DH Group* drop-down list, choose the appropriate Diffie-Hellman (DH)

group to be used with the key in Phase 2.

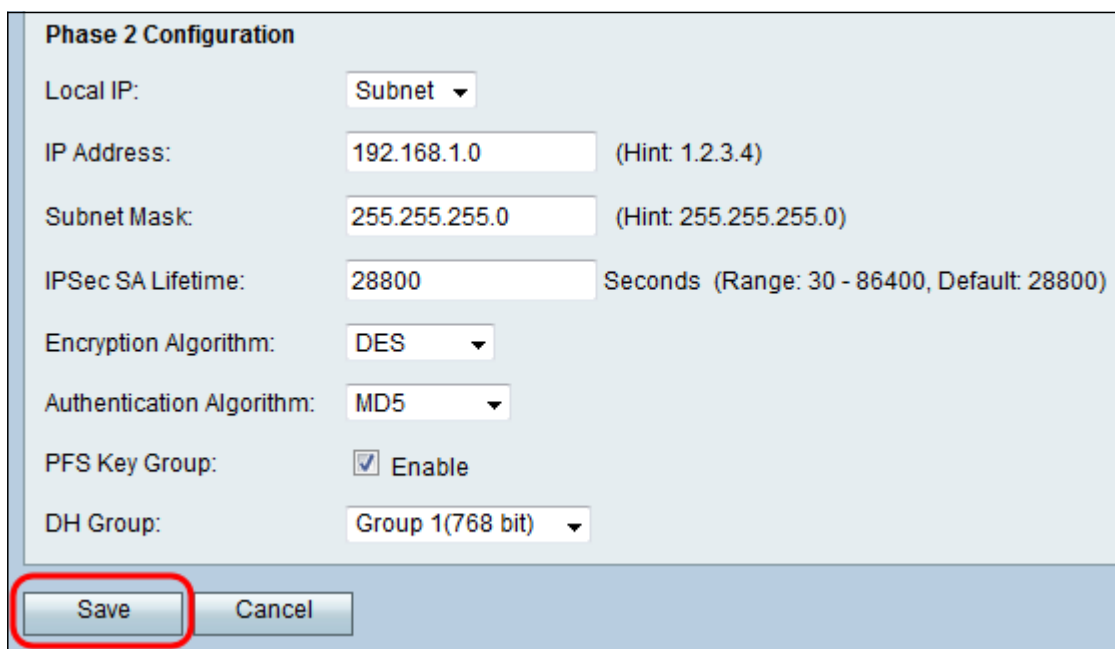


The screenshot shows the 'Phase 2 Configuration' dialog box. The fields are: Local IP: Subnet; IP Address: 192.168.1.0 (Hint: 1.2.3.4); Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0); IPsec SA Lifetime: 28800 Seconds (Range: 30 - 86400, Default: 28800); Encryption Algorithm: DES; Authentication Algorithm: MD5; PFS Key Group: Enable; DH Group: Group 1(768 bit). The dropdown menu for DH Group is open, showing options: Group 1(768 bit), Group 2(1024 bit), and Group 5(1536 bit). The 'Save' button is highlighted with a red box.

The available options are defined as follows:

- Group1 (768-bit) — Computes the key the fastest, but is the least secure.
- Group2 (1024-bit) — Computes the key slower, but is more secure than Group1.
- Group5 (1536-bit) — Computes the key the slowest, but is the most secure.

Step 18. Click **Save** to save your settings.



The screenshot shows the 'Phase 2 Configuration' dialog box with the same settings as the previous image. The 'DH Group' is now set to 'Group 1(768 bit)'. The 'Save' button is highlighted with a red box.

For more information, check out the following documentation:

- [RV130 Data sheet](#) - explains the VPN capabilities for the RV130 series routers
- [RV130 Product Page](#) - includes links for all RV130 articles from Cisco