Configure Easy Client to Gateway Virtual Private Network (VPN) on RV320 and RV325 VPN Router Series

Objective

A Virtual Private Network (VPN) provides security for remote users that connect to the internet from a public or untrusted network. One of the types of VPNs is a client-to-gateway VPN. With client-to-gateway, you can remotely connect different branches of your company located at different geographical areas to transmit and receive the data among the areas more securely. Easy VPN provides quick VPN setup and configuration through the Cisco VPN Client Utility.

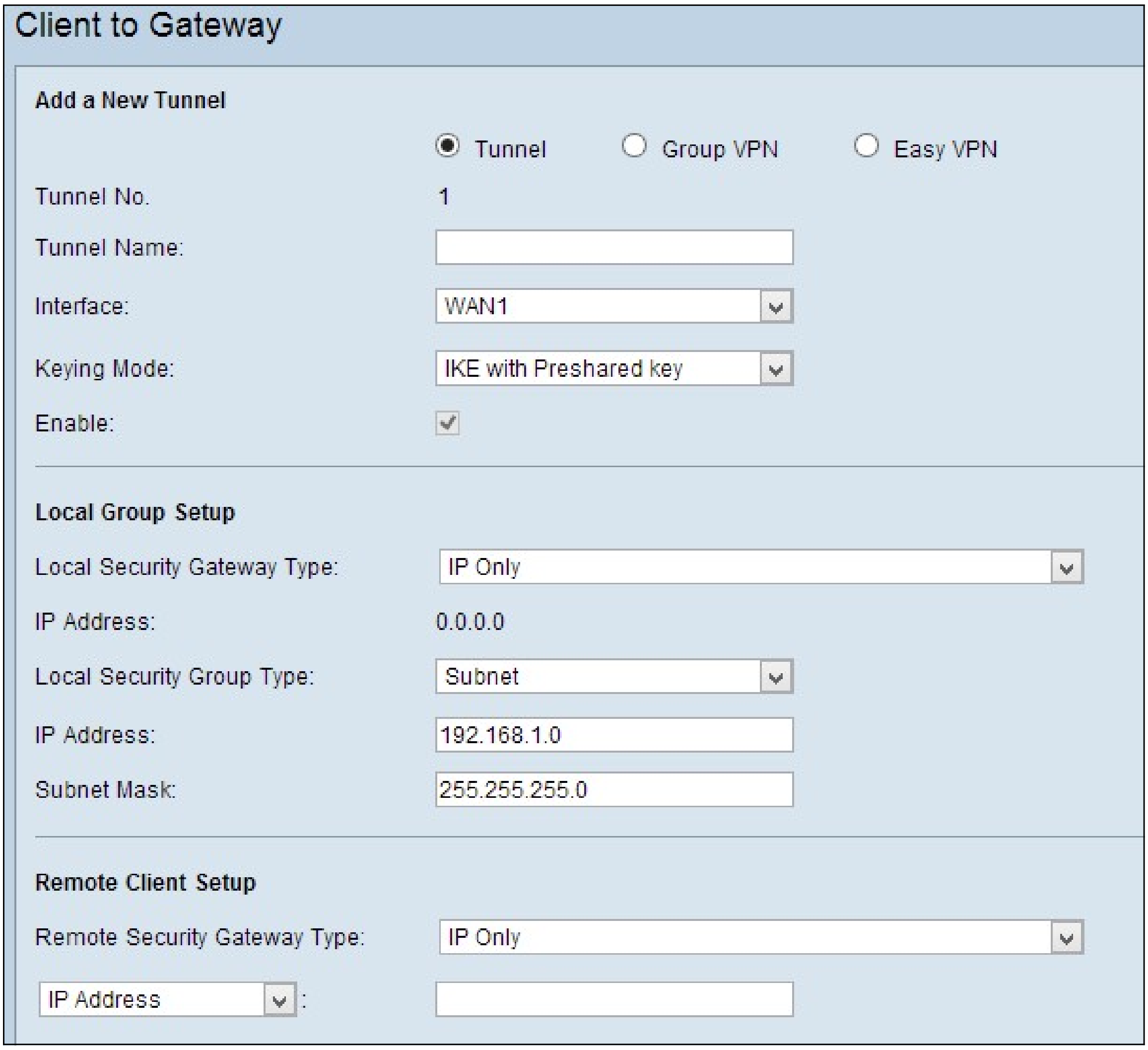
The objective of this document is to show you how to configure an Easy Client to Gateway VPN on RV32x VPN Router Series.

Applicable Devices | Firmware Version

- RV320 Dual WAN VPN Router | 1.1.0.09 (Download latest)
- RV325 Gigabit Dual WAN VPN Router | 1.1.0.09 (Download latest)

Configure Easy Client to Gateway VPN

Step 1. Log in to the web configuration utility and choose **VPN > Client to Gateway**. The *Client to Gateway* page opens:



Client to Gateway

Add a New Tunnel

● Tunnel ○ Group VPN ○ Easy VPN

Tunnel No.	1
Tunnel Name:	
Interface:	WAN1
Keying Mode:	IKE with Preshared key
Enable:	☑

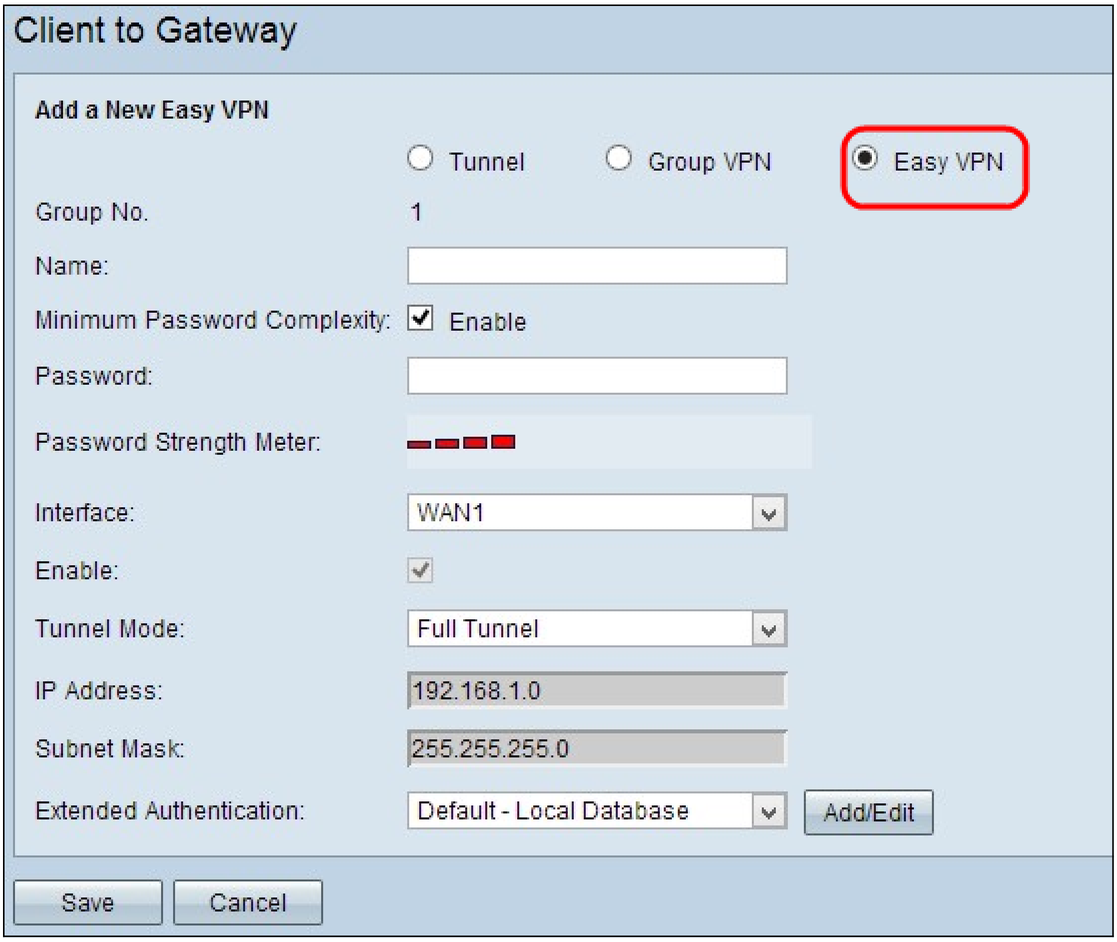
Local Group Setup

Local Security Gateway Type:	IP Only
IP Address:	0.0.0.0
Local Security Group Type:	Subnet
IP Address:	192.168.1.0
Subnet Mask:	255.255.255.0

Remote Client Setup

Remote Security Gateway Type:	IP Only
IP Address :	

Step 2. Click the **Easy VPN** radio button.



Client to Gateway

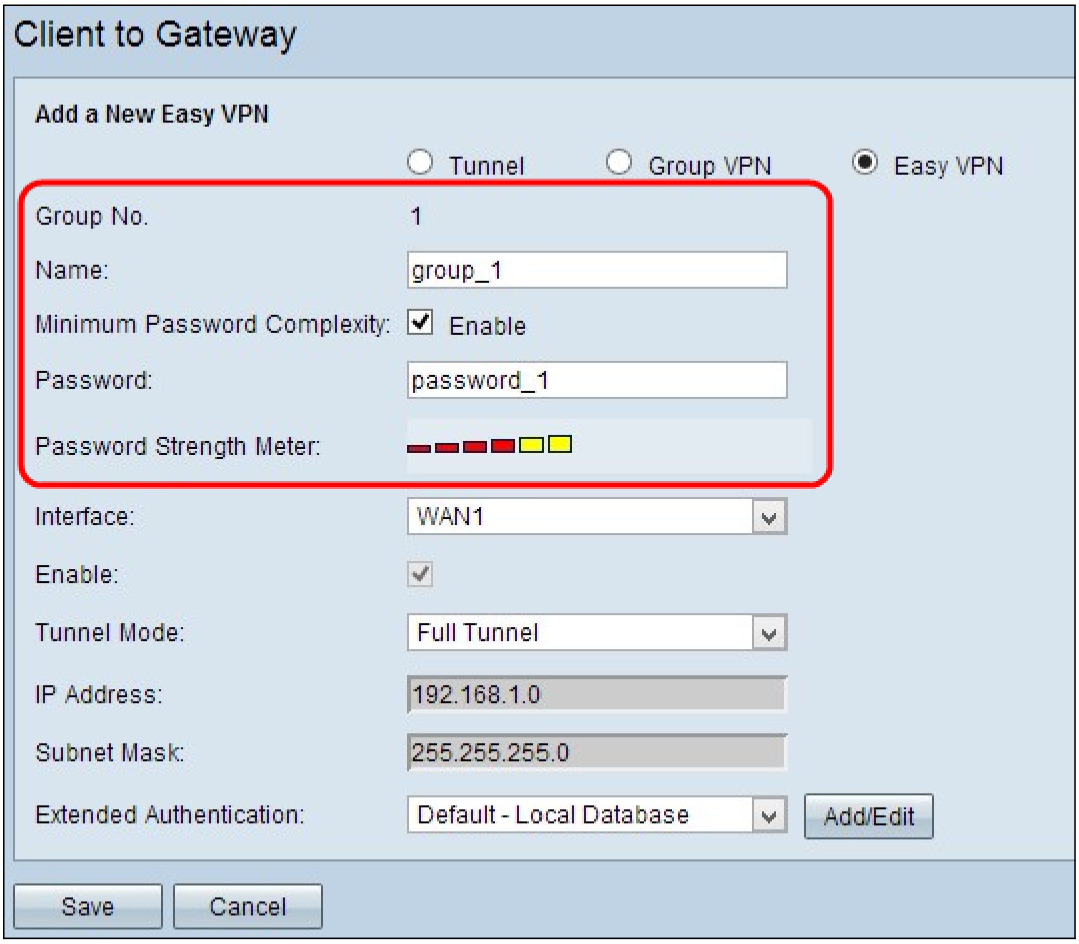
Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No.	1
Name:	
Minimum Password Complexity:	☑ Enable
Password:	
Password Strength Meter:	
Interface:	WAN1
Enable:	☑
Tunnel Mode:	Full Tunnel
IP Address:	192.168.1.0
Subnet Mask:	255.255.255.0
Extended Authentication:	Default - Local Database

Note: The *Group No.* represents the number of the group. It is an auto generated field.

Step 3. In the *Name* field, enter the name of the tunnel.



Client to Gateway

Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

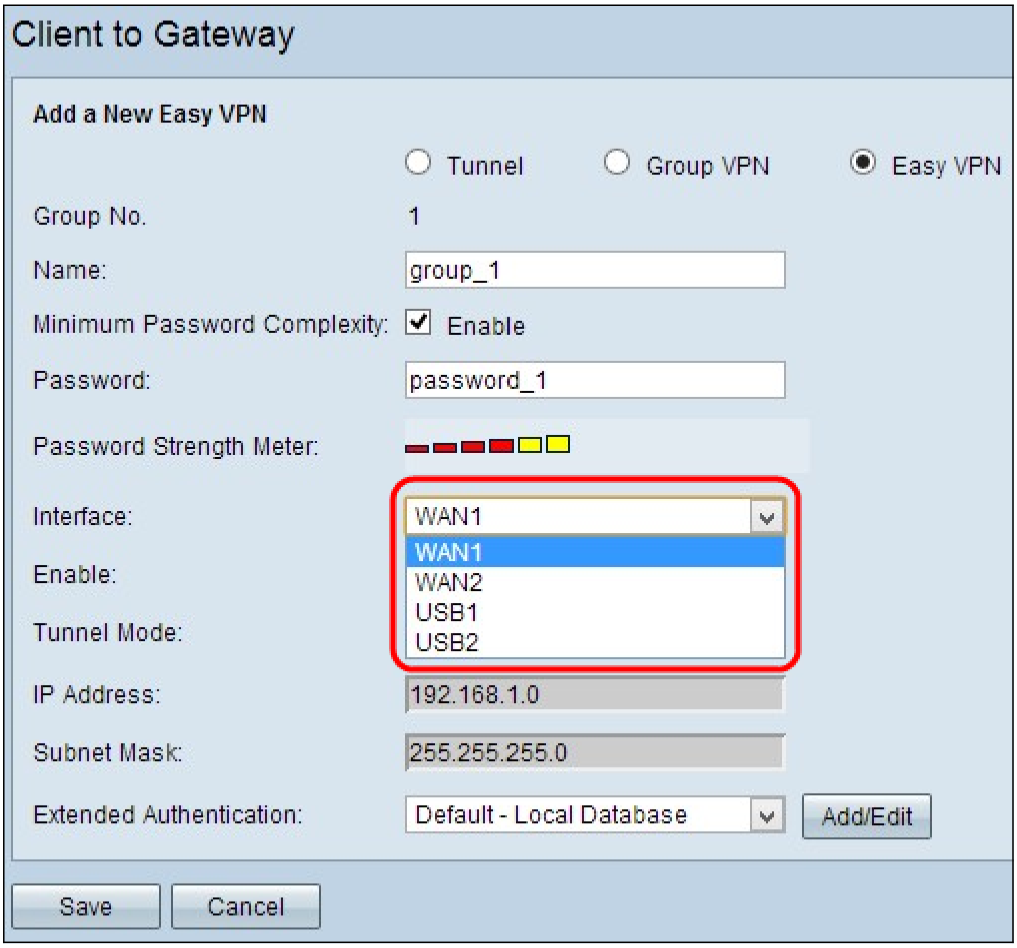
Group No.	1
Name:	group_1
Minimum Password Complexity:	☑ Enable
Password:	password_1
Password Strength Meter:	🟥🟥🟥🟥🟨🟨
Interface:	WAN1
Enable:	☑
Tunnel Mode:	Full Tunnel
IP Address:	192.168.1.0
Subnet Mask:	255.255.255.0
Extended Authentication:	Default - Local Database

Step 4. (Optional) If you want to enable the strength meter for the preshared key, check the **Minimum Password Complexity** check box.

Step 5. In the *Password* field, enter a password.

- Password Strength Meter - Shows the strength of the password through colored bars. Red indicates weak strength, yellow indicates acceptable strength and green indicates strong strength. If you did not check the **Minimum Password Complexity** check box in Step 4, then the Password Strength Meter does not appear.

Step 6. Choose the appropriate interface through which the client establishes Easy VPN to the gateway from the *Interface* drop-down list.



Client to Gateway

Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No. 1

Name: group_1

Minimum Password Complexity: ☑ Enable

Password: password_1

Password Strength Meter: 🟥🟥🟥🟥🟨🟨

Interface: WAN1

Enable:

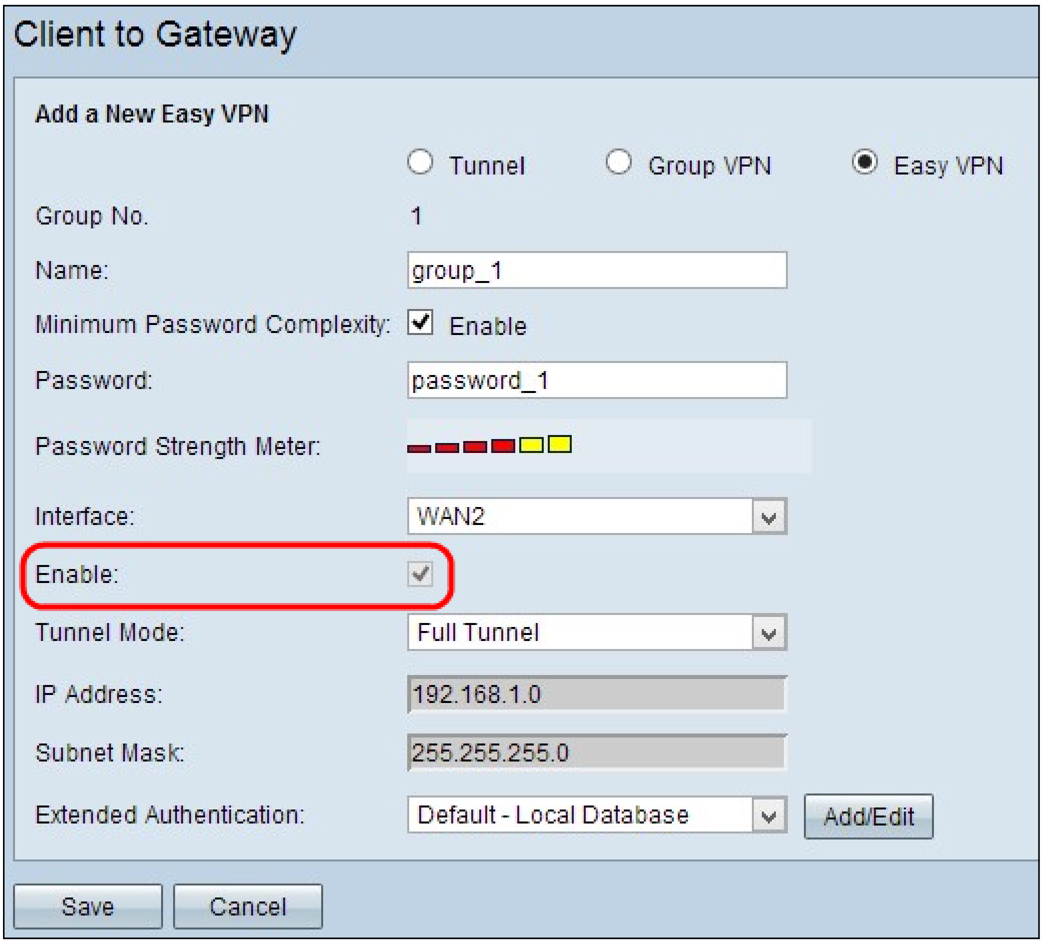
Tunnel Mode:

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Extended Authentication: Default - Local Database

Step 7. Check the **Enable** check box to enable client to gateway VPN. By default it is enabled.



Client to Gateway

Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No. 1

Name: group_1

Minimum Password Complexity: ☑ Enable

Password: password_1

Password Strength Meter: 🟥🟥🟥🟥🟨🟨

Interface: WAN2

Enable: ☑

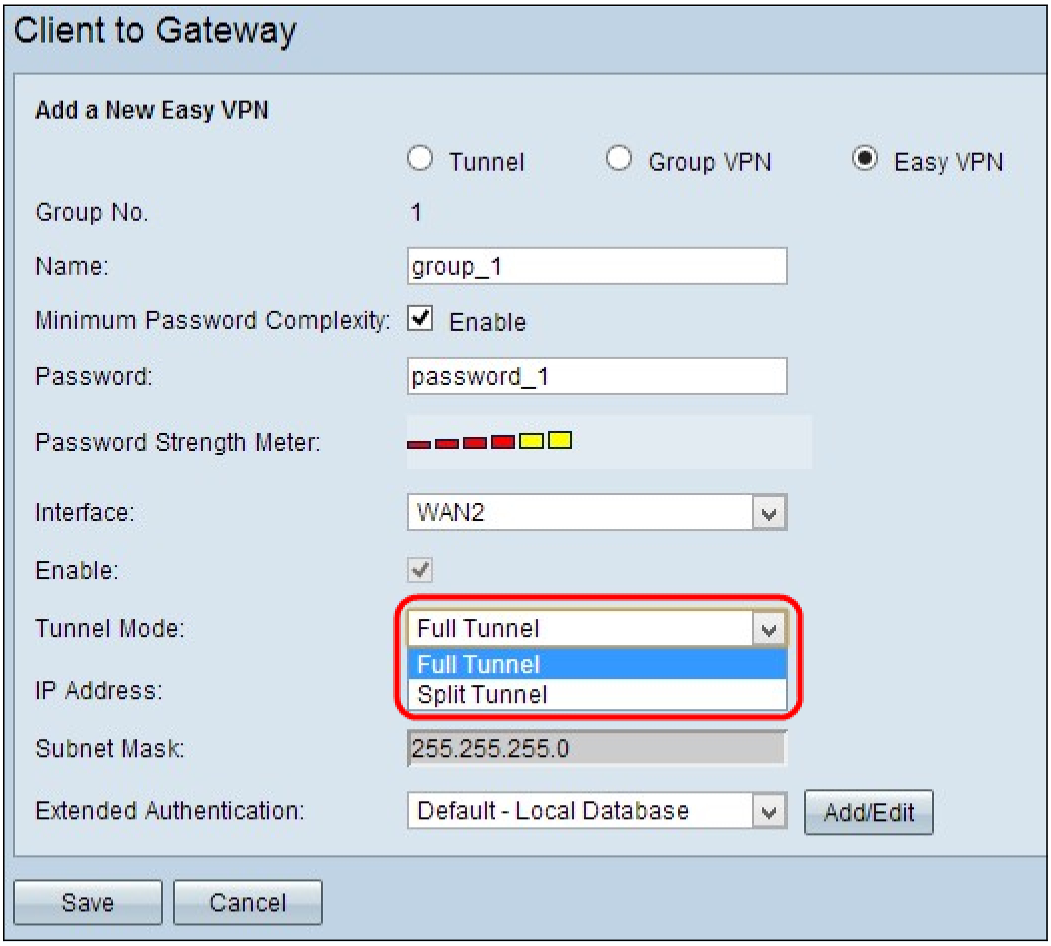
Tunnel Mode: Full Tunnel

IP Address: 192.168.1.0

Subnet Mask: 255.255.255.0

Extended Authentication: Default - Local Database

Step 8. Choose the appropriate tunneling mode from the *Tunnel Mode* drop-down list.



Client to Gateway

Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No. 1

Name: group_1

Minimum Password Complexity: ☑ Enable

Password: password_1

Password Strength Meter: 🟥🟥🟥🟥🟨🟨

Interface: WAN2

Enable: ☑

Tunnel Mode: Full Tunnel

IP Address:

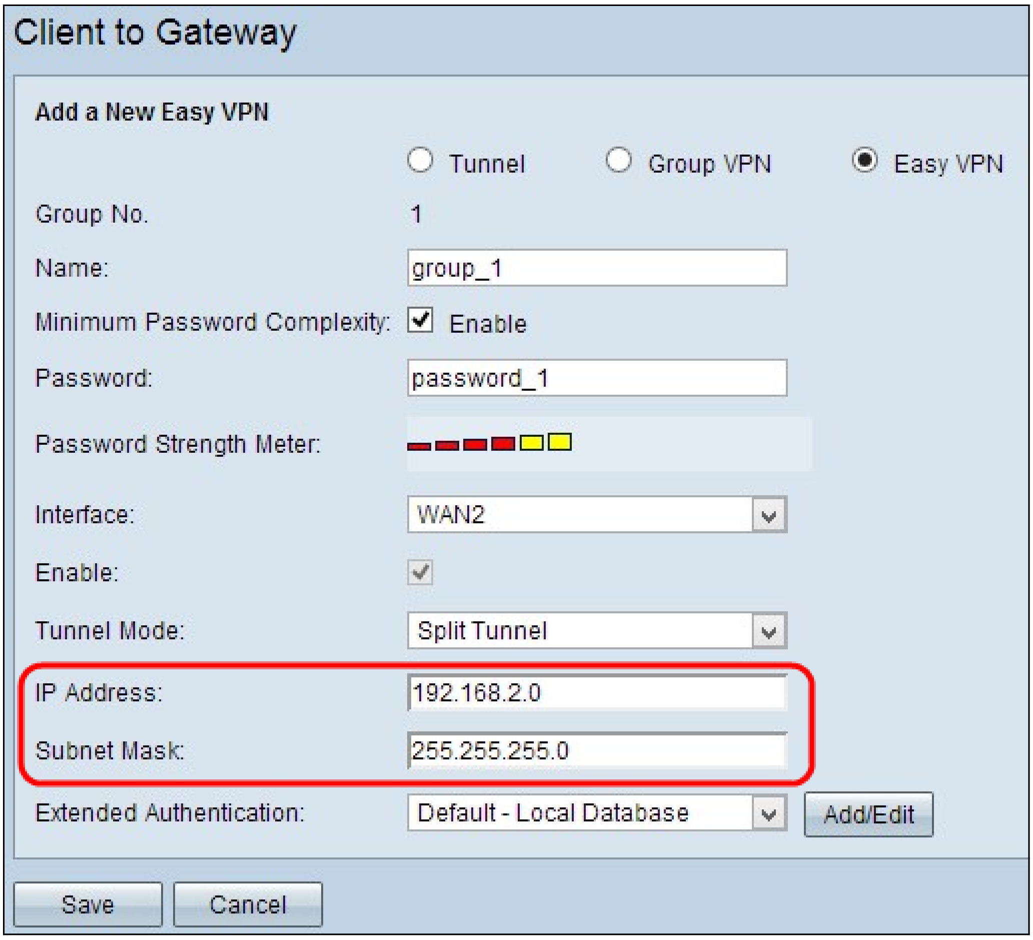
Subnet Mask: 255.255.255.0

Extended Authentication: Default - Local Database

The available options are defined as follows:

- Full Tunnel - Sends all traffic over the VPN tunnel, which provides more security to the traffic. If you choose this option, skip to Step 11.
- Split Tunnel - Allows the VPN client to access the public Internet as well as the VPN resources at the same time, which conserves bandwidth.

Step 9. In the *IP Address* field, enter the IP address you want to assign to the interface of the Easy VPN.



Client to Gateway

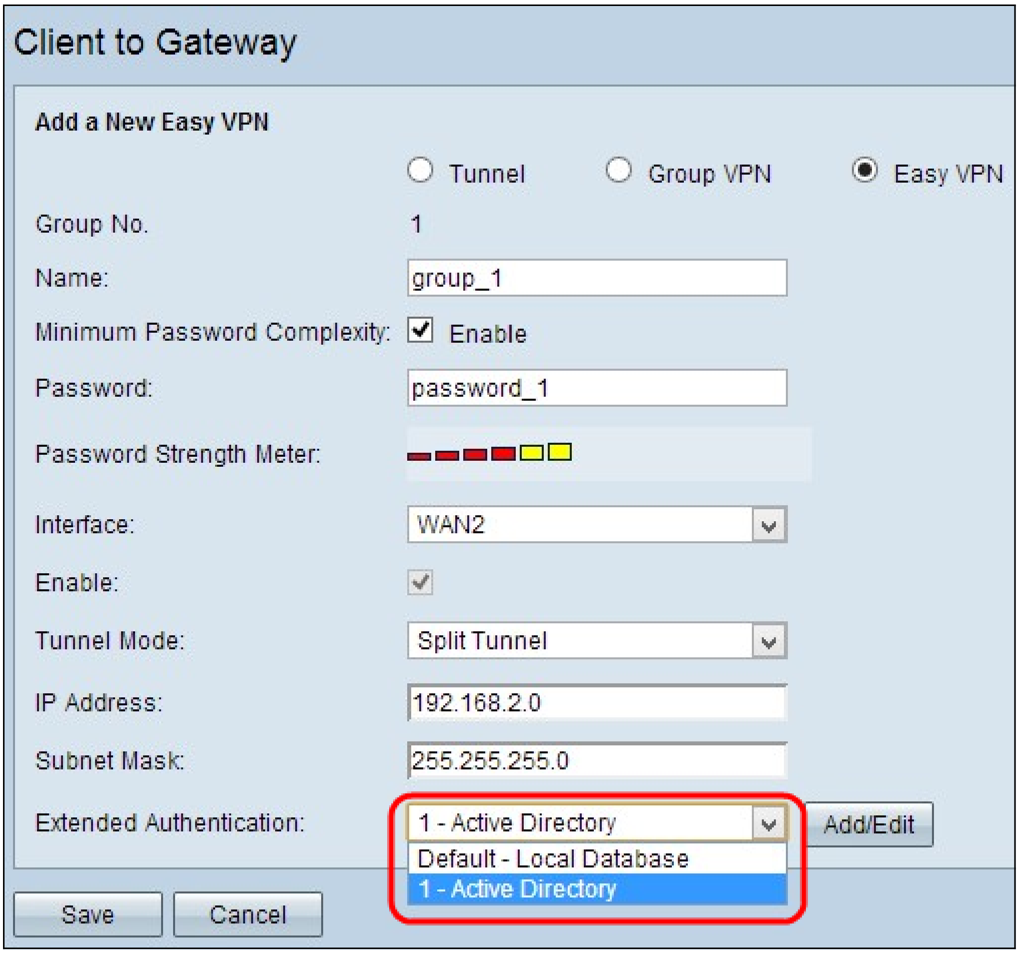
Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No.	1
Name:	group_1
Minimum Password Complexity:	☑ Enable
Password:	password_1
Password Strength Meter:	🟥🟥🟥🟥🟨🟨
Interface:	WAN2
Enable:	☑
Tunnel Mode:	Split Tunnel
IP Address:	192.168.2.0
Subnet Mask:	255.255.255.0
Extended Authentication:	Default - Local Database

Step 10. In the *Subnet Mask* field, enter the subnet mask of the assigned IP address of the Easy VPN interface.

Step 11. Choose the appropriate authentication for the VPN client from the *Extended Authentication* drop-down list to use an IPSec host username and password to authenticate VPN clients, or to use the database found in User Management. This must be enabled on both devices for it to work.



Client to Gateway

Add a New Easy VPN

○ Tunnel ○ Group VPN ● Easy VPN

Group No.	1
Name:	group_1
Minimum Password Complexity:	☑ Enable
Password:	password_1
Password Strength Meter:	🟥🟥🟥🟥🟨🟨
Interface:	WAN2
Enable:	☑
Tunnel Mode:	Split Tunnel
IP Address:	192.168.2.0
Subnet Mask:	255.255.255.0
Extended Authentication:	1 - Active Directory

The available options are defined as follows:

- 1 - Active Directory - Authentication is extended through active directory. Active directory is a service that provides network security on a Windows domain network. Click **Add/Edit** if you want to add a new directory or edit the existing directory.
- Default - Local Database - Authentication is performed by the router. Click **Add/Edit** if you want to add or edit the database.

Note: If you want to find out more about how to add or edit the active directory or the local database, refer to the document entitled, *User and Domain Management Configuration on RV320 and RV325 VPN Router Series*.

Step 12. Click **Save** to save the settings.