Configure Client-to-Site Virtual Private Network (VPN) Connection on the RV34x Series Router

Objective

In a Client-to-Site Virtual Private Network (VPN) connection, clients from the Internet can connect to the server to access the corporate network or Local Area Network (LAN) behind the server but still maintains the security of the network and its resources. This feature is very useful since it creates a new VPN tunnel that would allow teleworkers and business travelers to access your network by using a VPN client software without compromising privacy and security.

The objective of this document is to show you how to configure Client-to-Site VPN connection on the RV34x Series Router.

Applicable Devices

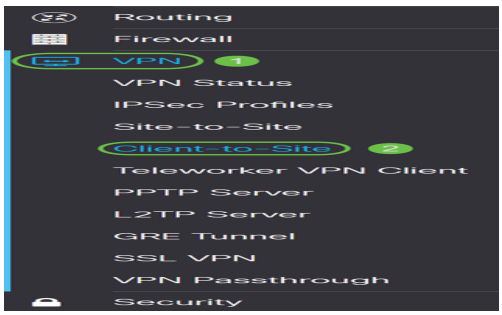
- RV34x Series

Software Version

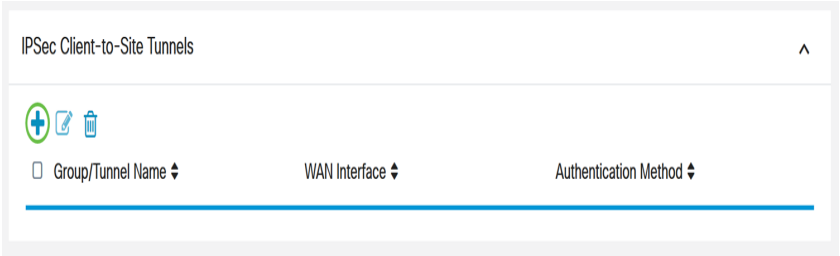
- 1.0.01.16

Configure Client-to-Site VPN

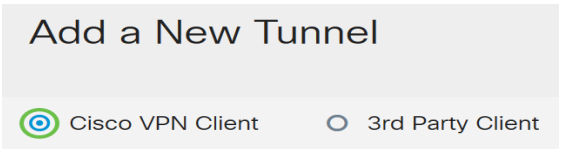
Step 1. Log in to the router web-based utility and choose **VPN > Client-to-Site**.



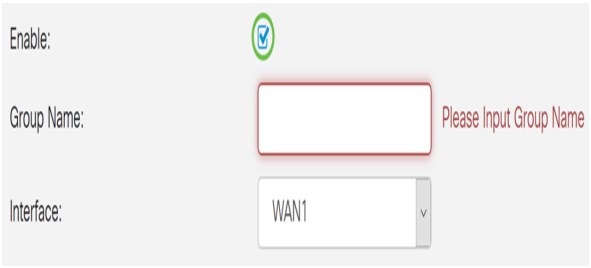
Step 2. Click the **Add** button under IPSec Client-to-Site Tunnels section.



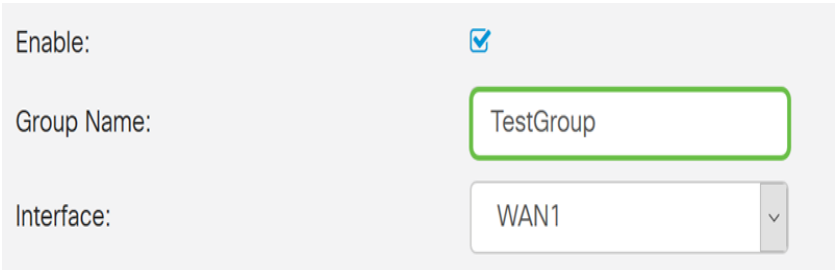
Step 3. In the *Add a New Tunnel* area, click the **Cisco VPN Client** radio button.



Step 4. Check the **Enable** check box to enable the configuration.



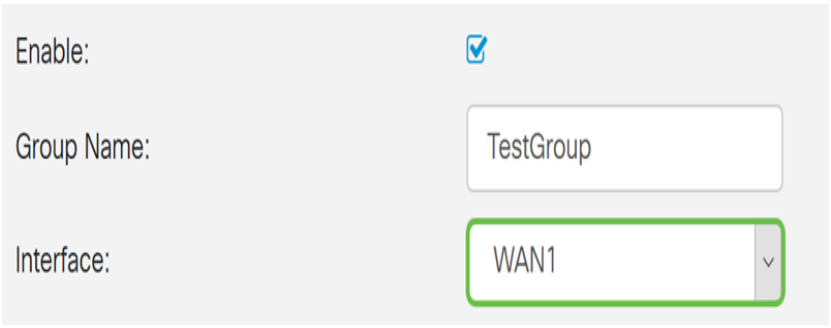
Step 5. Enter a group name in the field provided. This will serve as identifier for all the member of this group during the Internet Key Exchange (IKE) negotiations.



Note: Enter characters between A to Z or 0 to 9. Spaces and special characters are not allowed for the group name. In this example, TestGroup is used.

Step 6. Click on the drop-down list to choose the Interface. The options are:

- WAN1
- WAN2
- USB1
- USB2



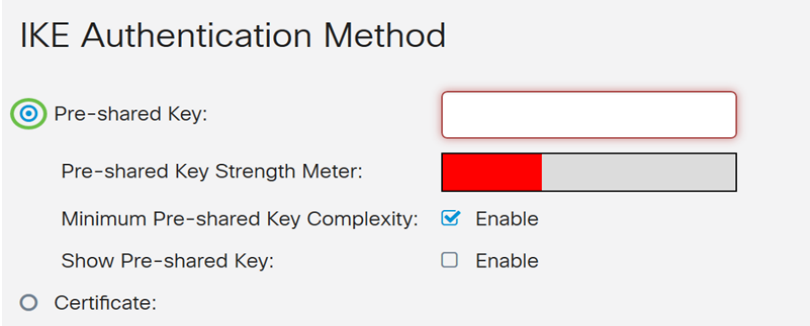
Note: In this example, WAN1 is chosen. This is the default setting.

Step 7. In the IKE Authentication Method area, choose an authentication method to be used in IKE negotiations in IKE-based tunnel. The options are:

- Pre-shared Key — IKE peers authenticate each other by computing and sending a keyed hash of data that includes the Pre-shared Key. If the receiving peer is able to create the same hash independently using its Pre-shared key, it knows that both peers must share the same secret, thus authenticating the other peer. Pre-shared keys do not

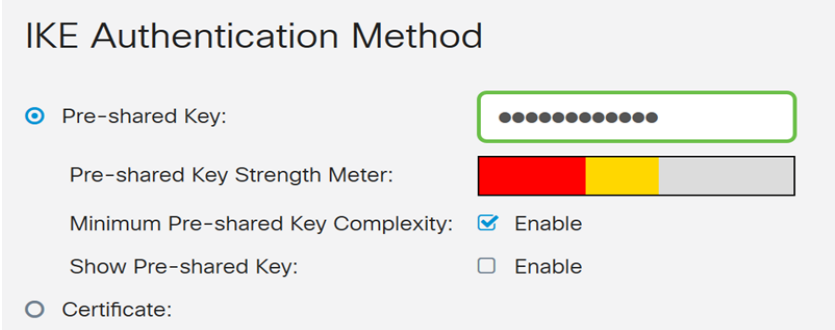
scale well because each IPSec peer must be configured with the Pre-shared key of every other peer with which it establishes a session.

- Certificate — The digital certificate is a package that contains information such as a certificate identity of the bearer: name or IP address, the serial number expiration date of the certificate, and a copy of the public key of the certificate bearer. The standard digital certificate format is defined in the X.509 specification. X.509 version 3 defines the data structure for certificates.



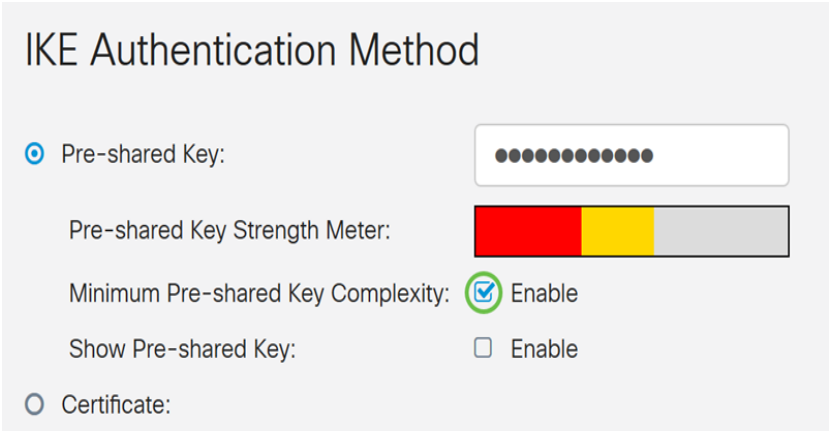
Note: In this example, Pre-shared Key is chosen. This is the default setting.

Step 8. Enter a pre-shared key in the field provided. This will be the authentication key among your group of IKE peers.



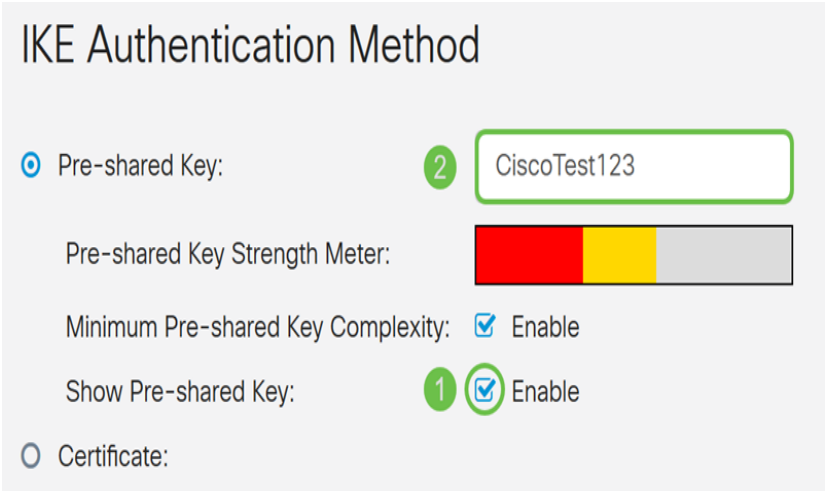
Step 9. (Optional) Check the **Enable** check box for the Minimum Pre-shared Key Complexity to view the Pre-shared Key Strength Meter and determine the strength of your key. The strength of your key are defined as follows:

- Red— The password is weak.
- Orange— The password is fairly strong.
- Green — The password is strong.

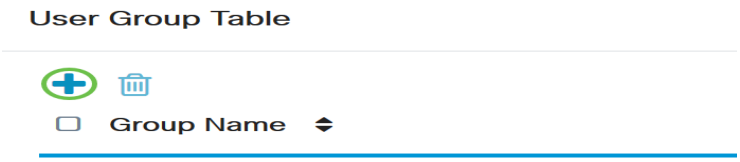


Note: You can check the **Enable** check box in the *Show Pre-shared Key* field to check your

password in plain text.

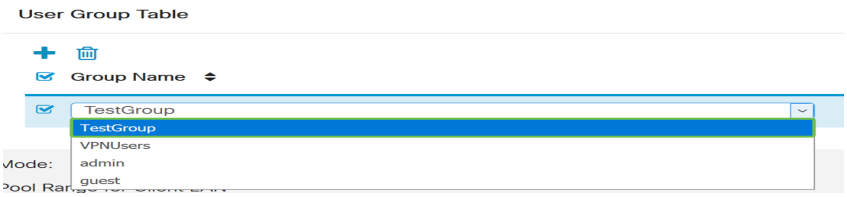


Step 10. (Optional) Click on the **plus** icon in the User Group table to add a group.



Step 11. (Optional) Choose from the drop-down list whether the user group is for admin or for guests. If you created your own user group with user accounts, you can select it. In this example, we will be selecting TestGroup.

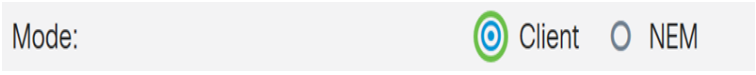
Note: TestGroup is a user group that we have created in **System Configuration** > **User Groups**.



Note: In this example, TestGroup is chosen. You can also check the box beside the user group and then click the **Delete** button if you want to delete a user group.

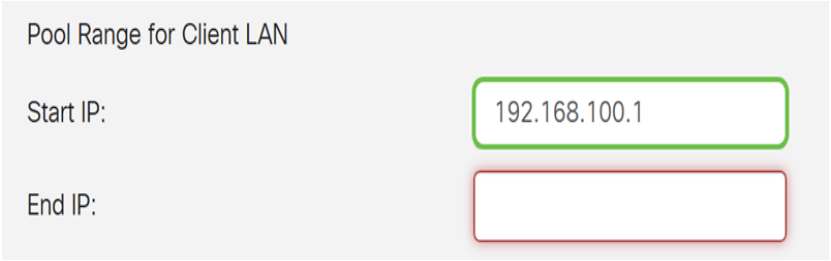
Step 12. Click on a radio button to choose a Mode. The options are:

- Client — This option allows the client to request for an IP address and the server supplies the IP addresses from the configured address range.
- Network Extension Mode (NEM) — This option allows clients to propose their subnet for which VPN services need to be applied on traffic between LAN behind server and subnet proposed by client.



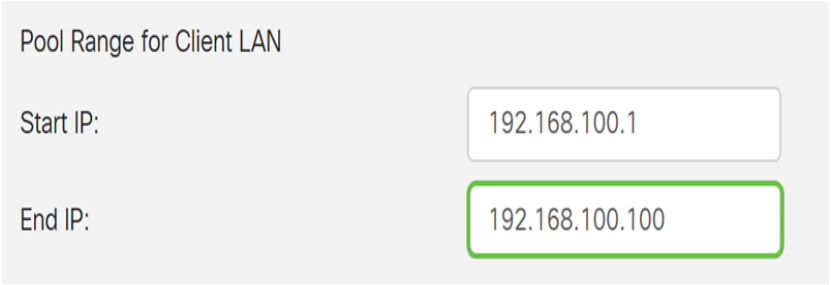
Note: In this example, Client is chosen.

Step 13. Enter the starting IP address in the *Start IP* field. This will be the first IP address in the pool that can be assigned to a client.



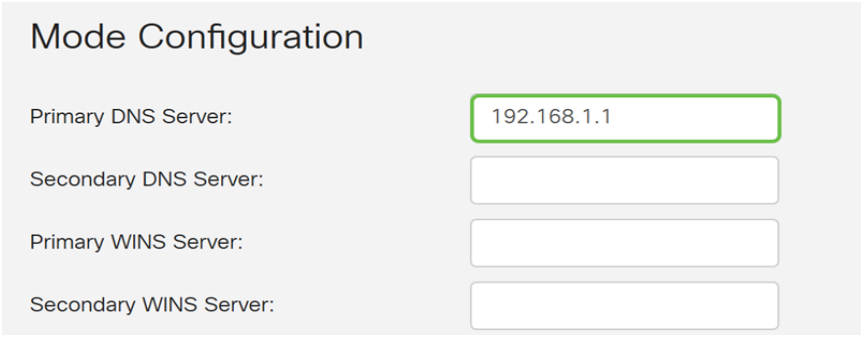
Note: In this example, 192.168.100.1 is used.

Step 14. Enter the ending IP address in the *End IP* field. This will be the last IP address in the pool that can be assigned to a client.



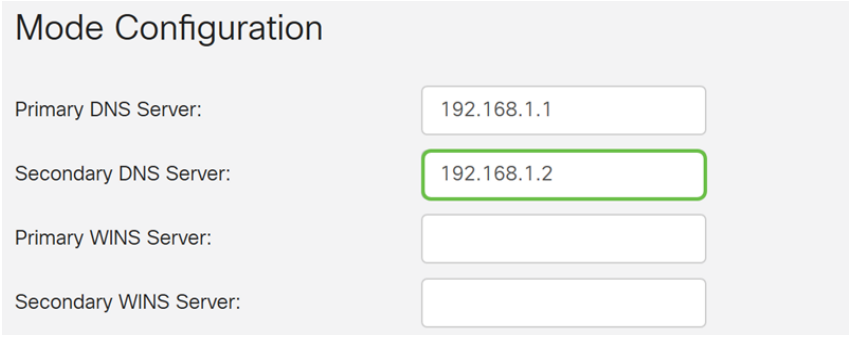
Note: In this example, 192.168.100.100 is used.

Step 15. (Optional) Under the *Mode Configuration* area, enter the IP address of the primary DNS server in the field provided.



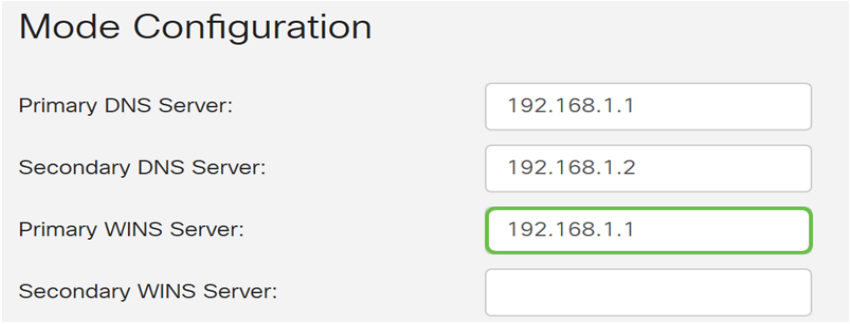
Note: In this example, 192.168.1.1 is used.

Step 16. (Optional) Enter the IP address of the secondary DNS server in the field provided.



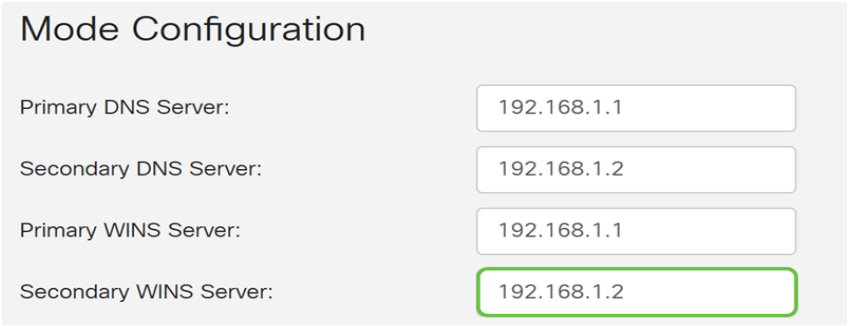
Note: In this example, 192.168.1.2 is used.

Step 17. (Optional) Enter the IP address of the primary WINS server in the field provided.



Note: In this example, 192.168.1.1 is used.

Step 18. (Optional) Enter the IP address of the secondary WINS server in the field provided.

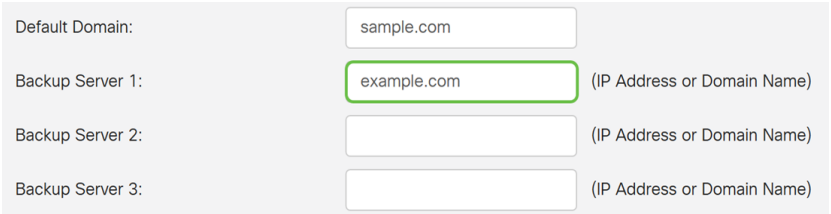


Note: In this example, 192.168.1.2 is used.

Step 19. (Optional) Enter the default domain to be used in the remote network in the field provided.

Note: In this example, sample.com is used.

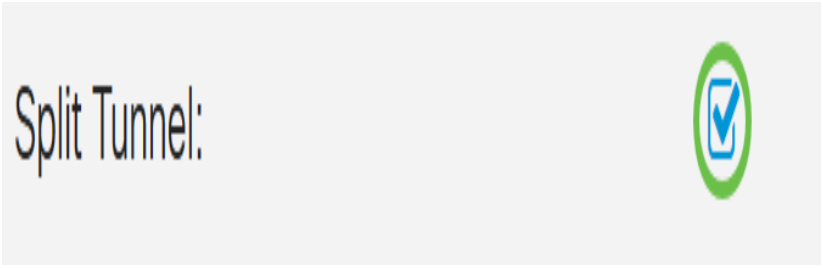
Step 20. (Optional) In the *Backup Server 1* field, enter the IP address or the domain name of the backup server. This will be where the device can start the VPN connection in case the primary IPSec VPN server fails. You can enter up to three backup servers in the fields provided. The Backup Server 1 has the highest priority among the three servers and the Backup Server 3 has the lowest.



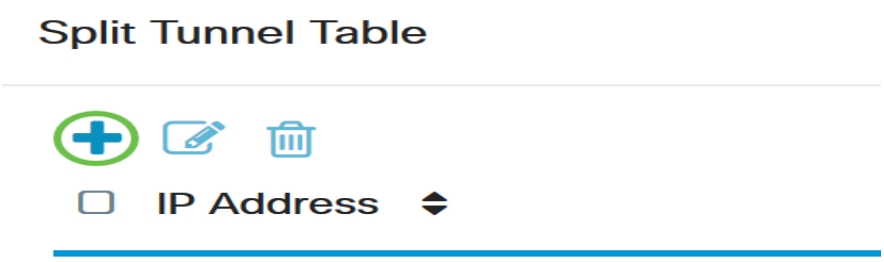
Note: In this example, Example.com is used for Backup Server 1.

Step 21. (Optional) Check the **Split Tunnel** check box to enable split tunnel. Split Tunneling

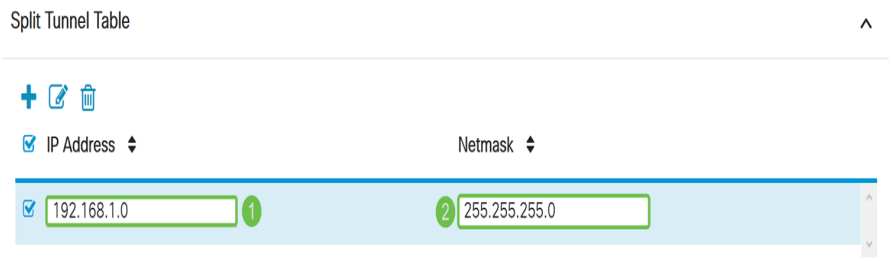
allows you to access the resources of a private network and the Internet at the same time.



Step 22. (Optional) Under the *Split Tunnel Table*, click the **plus** icon to add an IP address for split tunnel.

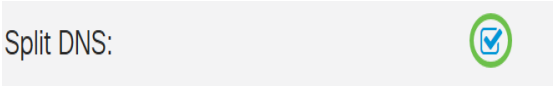


Step 23. (Optional) Enter the IP address and netmask of the split tunnel in the fields provided.

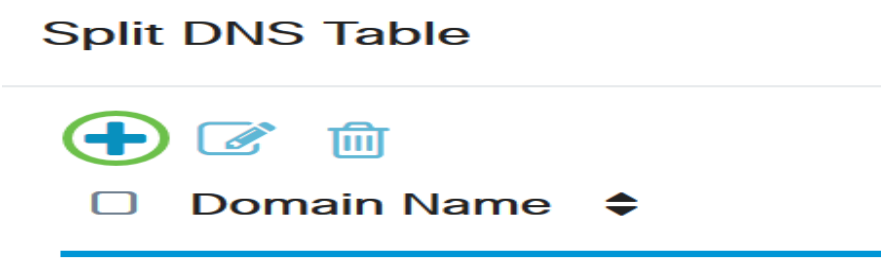


Note: In this example, 192.168.1.0 and 255.255.255.0 are used. You can also check the box and click on the **Add**, **Edit**, and **Delete** buttons to add, edit, or delete a split tunnel, respectively.

Step 24. (Optional) Check the **Split DNS** check box to enable split DNS. Split DNS allows you to create separate DNS servers for internal and external networks to maintain security and privacy of network resources.



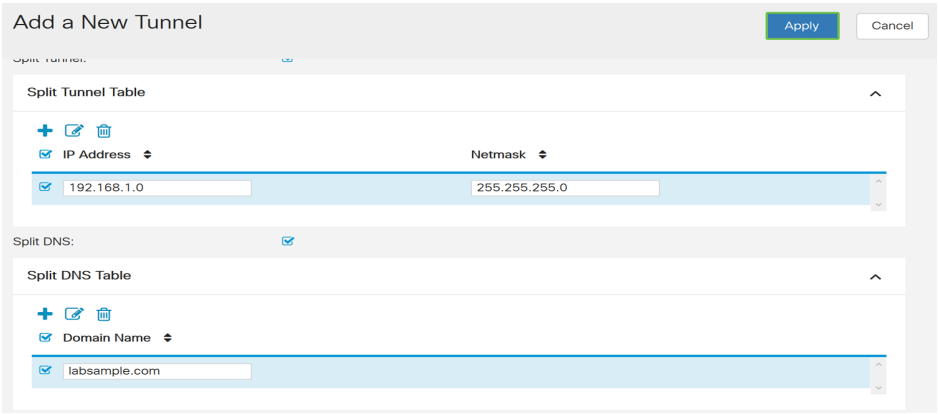
Step 25. (Optional) Click the **plus** icon under the *Split DNS Table* to add a domain name for split DNS.



Step 26. (Optional) Enter the domain name of the split DNS in the field provided.

Note: In this example, labsample.com is used. You can also check the box and click on the **Add**, **Edit**, and **Delete** buttons to add, edit, or delete a split DNS, respectively.

Step 27. Click **Apply**.



Conclusion

You should now have successfully configured Client-to-Site connection on the RV34x Series Router.

Click on the following articles to learn more on the following topics:

- Configure a Teleworker VPN Client on the RV34x Series Router
- Use TheGreenBow VPN Client to Connect with RV34x Series Router
- Create a User Account for VPN Client Setup on the RV34x Router
- Create a User Group for VPN Setup on the RV34x Router

View a video related to this article...

Click here to view other Tech Talks from Cisco