Configurazione della connessione VPN (Virtual Private Network) da client a sito sul router serie RV34x

Obiettivo

In una connessione VPN (Virtual Private Network) da client a sito, i client di Internet possono connettersi al server per accedere alla rete aziendale o alla LAN (Local Area Network) dietro il server, mantenendo tuttavia la sicurezza della rete e delle relative risorse. Questa funzione è molto utile perché crea un nuovo tunnel VPN che consente ai telelavoratori e agli utenti business di accedere alla rete utilizzando un software client VPN senza compromettere la privacy e la sicurezza.

L'obiettivo di questo documento è mostrare come configurare la connessione VPN da client a sito sui router serie RV34x.

Dispositivi interessati

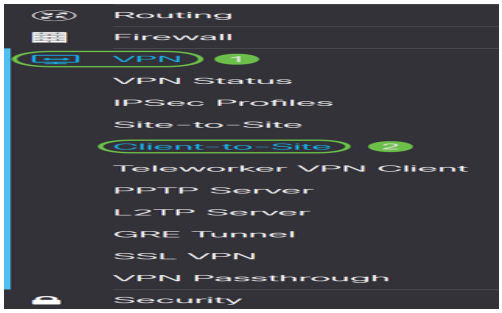
- Serie RV34x

Versione del software

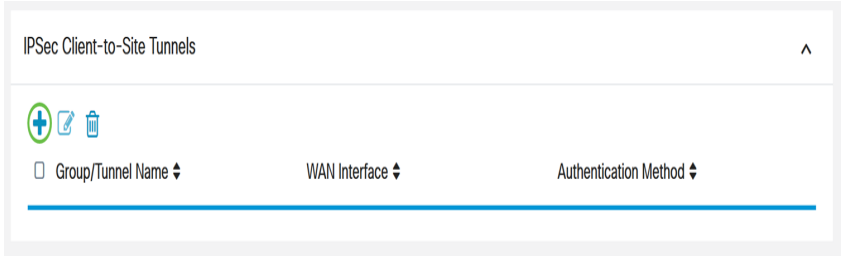
- 1.0.01.16

Configurazione della VPN da client a sito

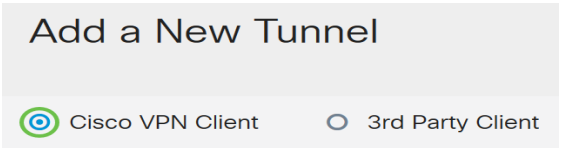
Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **VPN > Da client a sito** .



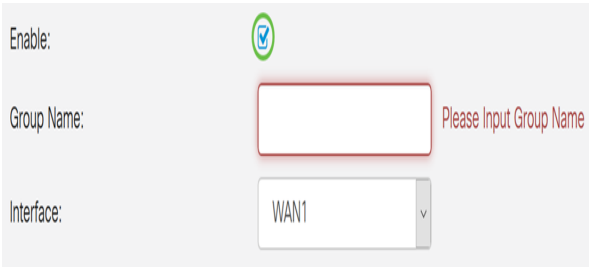
Passaggio 2. Fare clic sul pulsante **Add** (Aggiungi) nella sezione IPSec Client-to-Site Tunnels (Tunnel da client a sito).



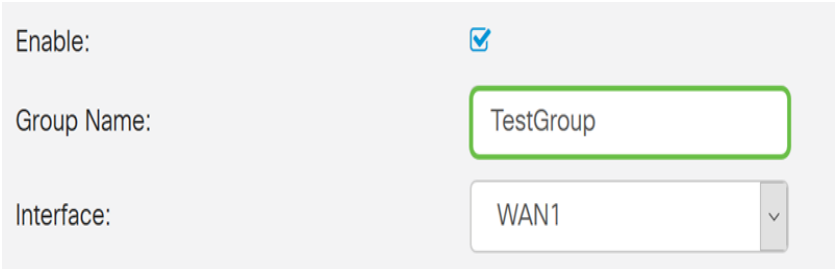
Passaggio 3. Nell'area *Add a New Tunnel*, fare clic sul pulsante di opzione **Cisco VPN Client** .



Passaggio 4. Selezionare la casella di controllo **Abilita** per abilitare la configurazione.



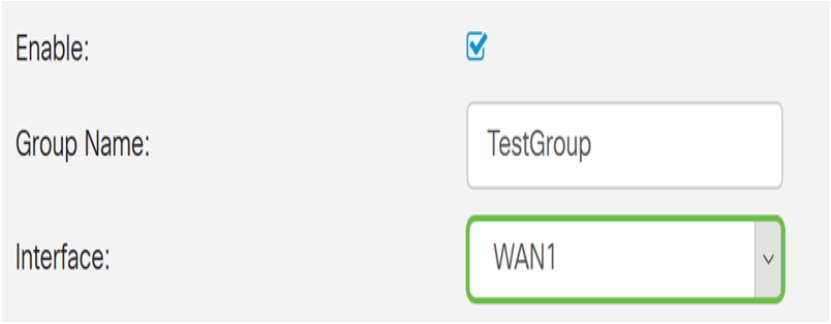
Passaggio 5. Inserire un nome di gruppo nel campo fornito. Questo identificatore verrà utilizzato da tutti i membri del gruppo durante le negoziazioni IKE (Internet Key Exchange).



Nota: Immettere caratteri compresi tra A e Z o tra 0 e 9. Non sono consentiti spazi e caratteri speciali per il nome del gruppo. Nell'esempio viene utilizzato TestGroup.

Passaggio 6. Fare clic sull'elenco a discesa per scegliere l'interfaccia. Le opzioni sono:

- WAN1
- WAN2
- USB1
- USB2



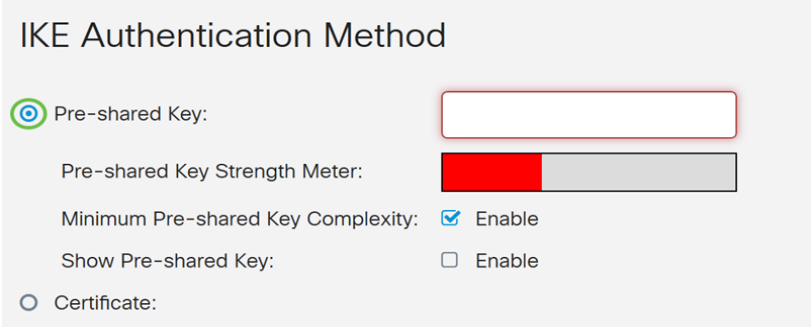
Nota: Nell'esempio, viene scelta WAN1. Si tratta dell'impostazione predefinita.

Passaggio 7. Nell'area Metodo di autenticazione IKE scegliere un metodo di autenticazione da utilizzare nelle negoziazioni IKE nel tunnel basato su IKE. Le opzioni sono:

- Chiave precondivisa: i peer IKE si autenticano a vicenda tramite il calcolo e l'invio di un hash di dati con chiave che include la chiave precondivisa. Se il peer ricevente è in

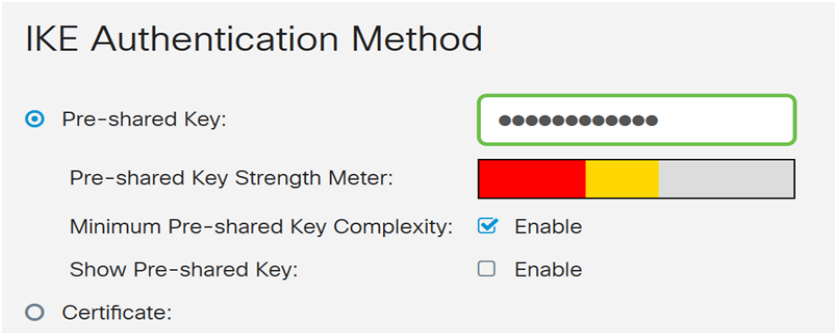
grado di creare lo stesso hash in modo indipendente utilizzando la propria chiave già condivisa, sa che entrambi i peer devono condividere lo stesso segreto, autenticando così l'altro peer. Le chiavi già condivise non sono scalabili correttamente perché ogni peer IPSec deve essere configurato con la chiave già condivisa di ogni altro peer con cui stabilisce una sessione.

- Certificato — il certificato digitale è un pacchetto che contiene informazioni quali l'identità del certificato del titolare: nome o indirizzo IP, la data di scadenza del numero di serie del certificato e una copia della chiave pubblica del titolare del certificato. Il formato del certificato digitale standard è definito nella specifica X.509. X.509 versione 3 definisce la struttura di dati per i certificati.



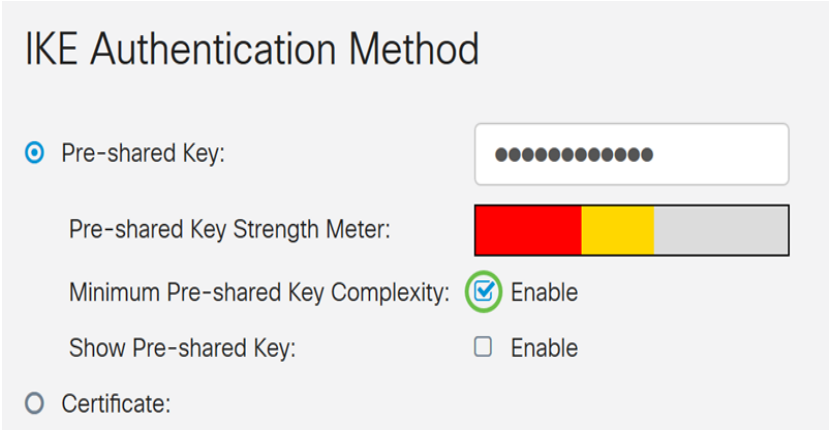
Nota: In questo esempio viene scelta Chiave già condivisa. Si tratta dell'impostazione predefinita.

Passaggio 8. Inserire una chiave già condivisa nel campo fornito. Questa sarà la chiave di autenticazione tra il gruppo di peer IKE.

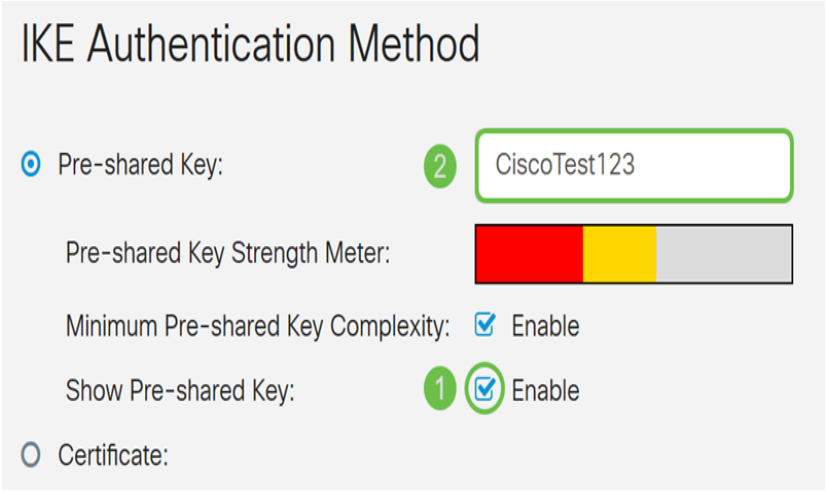


Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Abilita** per la complessità minima della chiave precondivisa per visualizzare il misuratore di forza della chiave precondivisa e determinare la forza della chiave. La forza della chiave viene definita come segue:

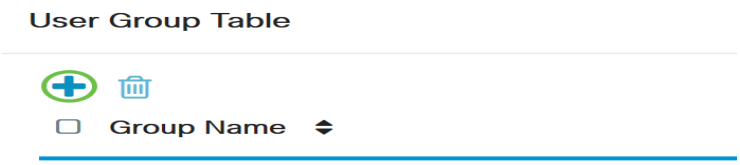
- Rosso: la password è debole.
- Arancione: la password è abbastanza complessa.
- Verde: la password è complessa.



Nota: È possibile selezionare la casella di controllo **Abilita** nel campo *Mostra chiave già condivisa* per controllare la password in testo normale.

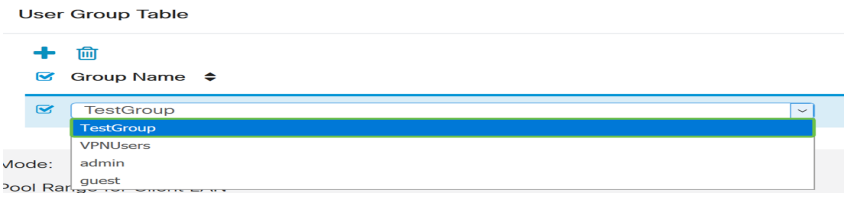


Passaggio 10. (Facoltativo) Fare clic sull'icona **più** nella tabella Gruppo di utenti per aggiungere un gruppo.



Passaggio 11. (Facoltativo) Scegliere dall'elenco a discesa se il gruppo di utenti è per admin o per guest. Se è stato creato un gruppo di utenti con account utente, è possibile selezionarlo. In questo esempio verrà selezionato TestGroup.

Nota: TestGroup è un gruppo di utenti creato in **Configurazione di sistema > Gruppi di utenti**.

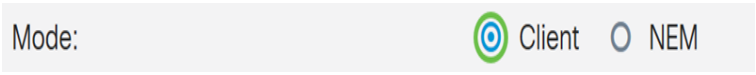


Nota: In questo esempio viene scelto TestGroup. È inoltre possibile selezionare la casella accanto al gruppo di utenti e quindi fare clic sul pulsante **Elimina** per eliminare un gruppo di utenti.

Passaggio 12. Fare clic su un pulsante di opzione per scegliere una modalità. Le opzioni

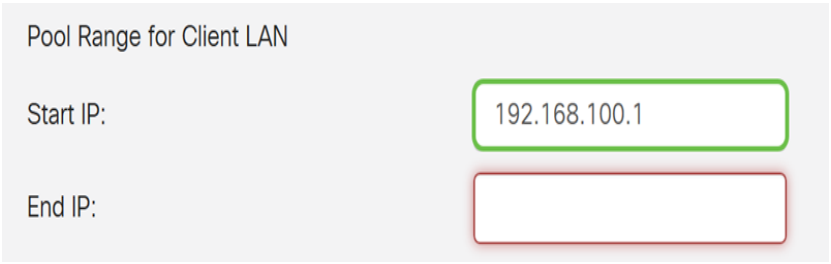
sono:

- Client: questa opzione consente al client di richiedere un indirizzo IP e al server di fornire gli indirizzi IP dell'intervallo di indirizzi configurato.
- Network Extension Mode (NEM): questa opzione consente ai client di proporre la propria subnet per la quale è necessario applicare i servizi VPN al traffico tra la LAN dietro il server e la subnet proposta dal client.



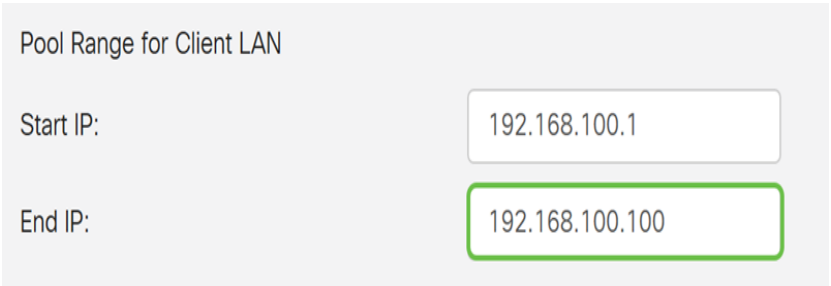
Nota: In questo esempio, viene scelto Client.

Passaggio 13. Immettere l'indirizzo IP iniziale nel campo *IP iniziale*. Questo sarà il primo indirizzo IP del pool che può essere assegnato a un client.



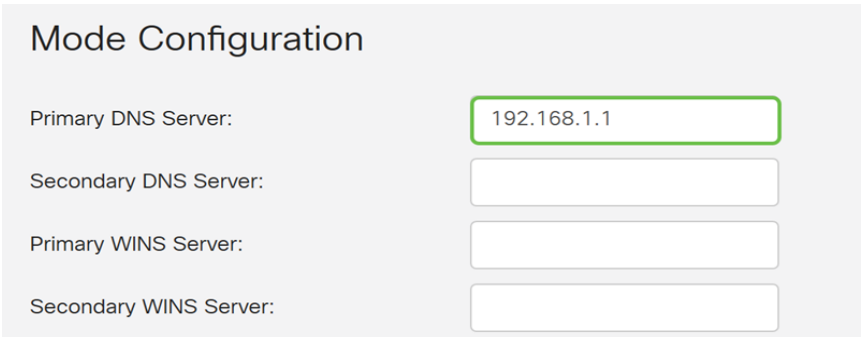
Nota: nell'esempio viene usato 192.168.100.1.

Passaggio 14. Inserire l'indirizzo IP finale nel campo *End IP*. Questo sarà l'ultimo indirizzo IP del pool che può essere assegnato a un client.



Nota: nell'esempio viene usato 192.168.100.100.

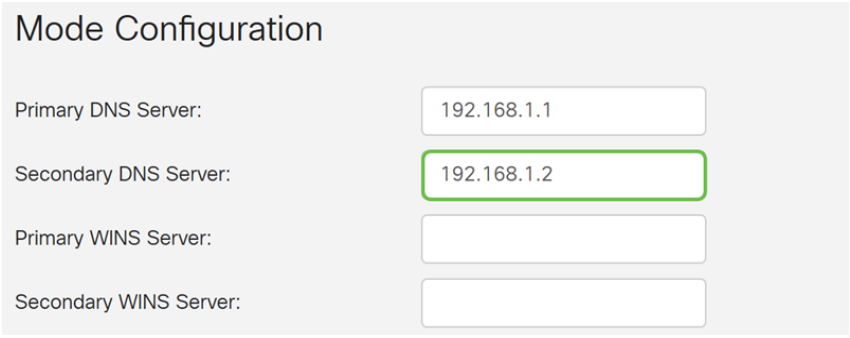
Passaggio 15. (Facoltativo) Nell'area *Configurazione modalità* immettere l'indirizzo IP del server DNS primario nell'apposito campo.



Nota: nell'esempio viene usato 192.168.1.1.

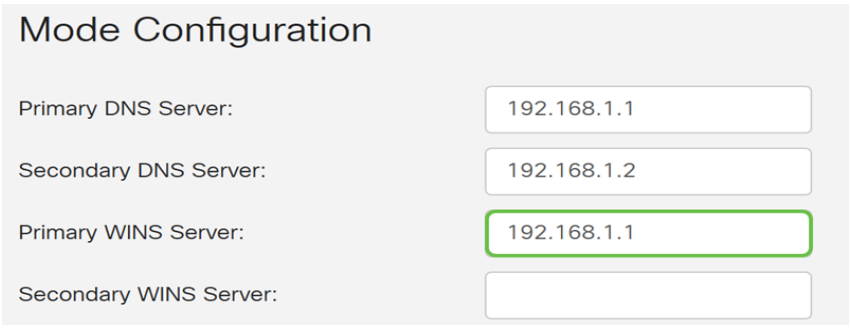
Passaggio 16. (Facoltativo) Immettere l'indirizzo IP del server DNS secondario nell'apposito

campo.



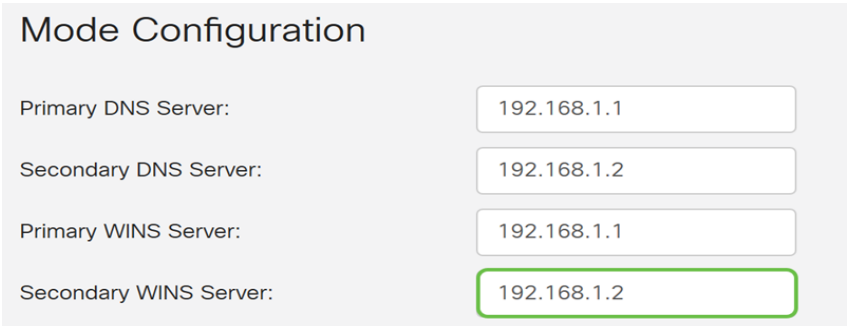
Nota: nell'esempio viene usato 192.168.1.2.

Passaggio 17. (Facoltativo) Immettere l'indirizzo IP del server WINS primario nell'apposito campo.



Nota: nell'esempio viene usato 192.168.1.1.

Passaggio 18. (Facoltativo) Immettere l'indirizzo IP del server WINS secondario nell'apposito campo.



Nota: nell'esempio viene usato 192.168.1.2.

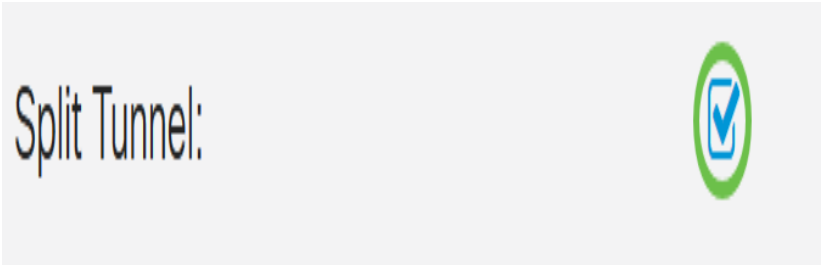
Passaggio 19. (Facoltativo) Immettere il dominio predefinito da utilizzare nella rete remota nell'apposito campo.

Nota: Nell'esempio viene utilizzato sample.com.

Passaggio 20. (Facoltativo) Nel campo *Server di backup 1*, immettere l'indirizzo IP o il nome di dominio del server di backup. In questo modo il dispositivo può avviare la connessione VPN in caso di errore del server VPN IPSec primario. È possibile immettere fino a tre server di backup negli appositi campi. Il server di backup 1 ha la priorità più alta tra i tre server e il server di backup 3 ha la priorità più bassa.

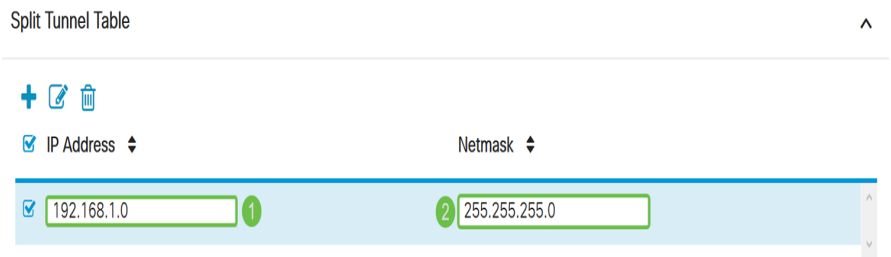
Nota: In questo esempio, Example.com viene utilizzato per Backup Server 1.

Passaggio 21. (Facoltativo) Selezionare la casella di controllo **Split Tunnel** per abilitare lo split tunnel. Il tunneling ripartito consente di accedere contemporaneamente alle risorse di una rete privata e a Internet.



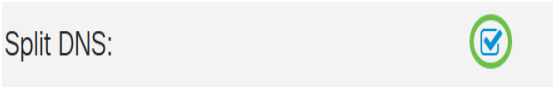
Passaggio 22. (Facoltativo) Sotto la *tabella del tunnel suddiviso*, fare clic sul pulsante **più** per aggiungere un indirizzo IP per il tunnel suddiviso.

Passaggio 23. (Facoltativo) Immettere l'indirizzo IP e la maschera di rete del tunnel suddiviso negli appositi campi.

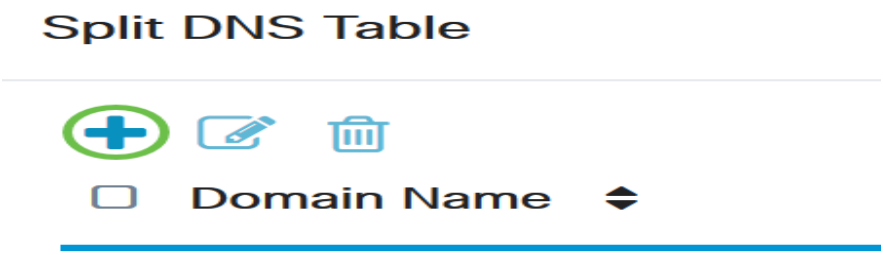


Nota: nell'esempio vengono usati 192.168.1.0 e 255.255.255.0. È inoltre possibile selezionare la casella e fare clic sui pulsanti **Add**, **Edit** ed **Delete** rispettivamente per aggiungere, modificare o eliminare un tunnel diviso.

Passaggio 24. (Facoltativo) Selezionare la casella di controllo **Dividi DNS** per abilitare la divisione del DNS. La suddivisione del DNS consente di creare server DNS separati per le reti interne ed esterne per mantenere la sicurezza e la privacy delle risorse di rete.



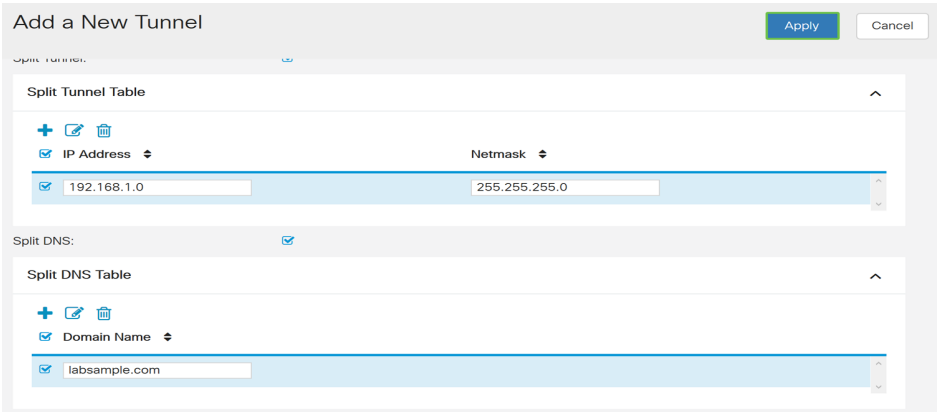
Passaggio 25. (Facoltativo) Fare clic sull'icona **più** sotto la *tabella DNS divisa* per aggiungere un nome di dominio per il DNS diviso.



Passaggio 26. (Facoltativo) Immettere il nome di dominio del DNS suddiviso nell'apposito campo.

Nota: Nell'esempio viene utilizzato labsample.com. È inoltre possibile selezionare la casella e fare clic sui pulsanti **Add**, **Edit** ed **Delete** rispettivamente per aggiungere, modificare o eliminare un DNS diviso.

Passaggio 27. Fare clic su **Applica**.



Conclusioni

A questo punto, è necessario configurare la connessione client-sito sul router serie RV34x.

Fare clic sui seguenti articoli per ulteriori informazioni sui seguenti argomenti:

- Configurazione di un client VPN Teleworker sul router serie RV34x

- Uso del client VPN GreenBow per la connessione con il router serie RV34x
- Creare un account utente per la configurazione del client VPN sul router RV34x
- Creare un gruppo di utenti per la configurazione della VPN sul router RV34x

Qui è disponibile un video relativo a questo articolo...

Fare clic qui per visualizzare altre Tech Talks di Cisco