

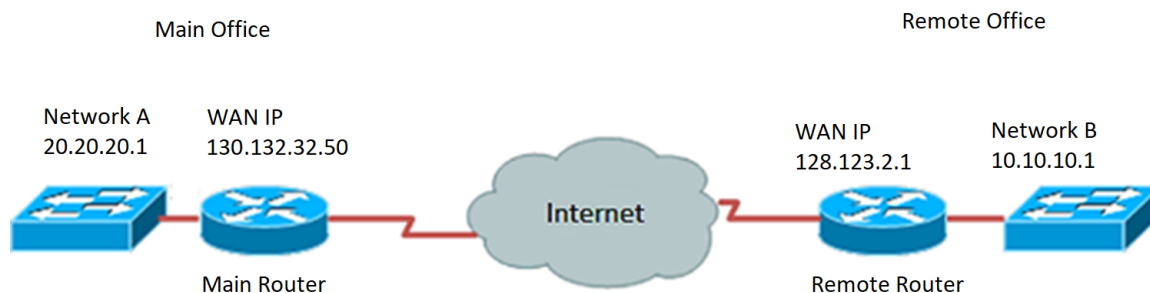
Configurazione della connessione VPN (Virtual Private Network) sul router serie RV34x con la Configurazione guidata

Obiettivo

Una connessione VPN (Virtual Private Network) consente agli utenti di accedere, inviare e ricevere dati da e verso una rete privata tramite una rete pubblica o condivisa, ad esempio Internet, ma garantisce comunque connessioni sicure a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia e l'autenticazione. Le filiali utilizzano per lo più connessioni VPN in quanto è utile e necessario consentire ai dipendenti di accedere alla rete privata anche quando si trovano all'esterno dell'ufficio.

La VPN consente a un host remoto di agire come se si trovasse sulla stessa rete locale. Il router supporta 50 tunnel. L'installazione guidata VPN consente di configurare una connessione protetta per il tunnel IPSec da sito a sito. Questa funzione semplifica la configurazione e impedisce impostazioni complesse e parametri opzionali. In questo modo, chiunque può configurare il tunnel IPSec in modo rapido ed efficiente.



Vantaggi dell'utilizzo di una connessione VPN:

1. L'utilizzo di una connessione VPN consente di proteggere i dati e le risorse di rete riservati.
2. Offre convenienza e accessibilità per i dipendenti remoti o aziendali, in quanto possono accedere facilmente all'ufficio principale senza dover essere fisicamente presenti e mantenere la sicurezza della rete privata e delle sue risorse.
3. La comunicazione tramite una connessione VPN offre un livello di protezione più elevato rispetto ad altri metodi di comunicazione remota. L'elevato livello di tecnologia rende possibile questa operazione, proteggendo la rete privata da accessi non autorizzati.
4. Le posizioni geografiche effettive degli utenti sono protette e non esposte al pubblico o a reti condivise come Internet.
5. Aggiungere nuovi utenti o gruppi di utenti alla rete è facile poiché le VPN sono molto regolabili. È possibile far crescere la rete senza la necessità di nuovi componenti aggiuntivi o configurazioni complicate.

Rischi dell'utilizzo di una connessione VPN:

1. Rischio per la sicurezza dovuto a una configurazione errata. Poiché la progettazione e l'implementazione di una VPN può essere complicata, è necessario affidare il compito di configurare la connessione a un professionista altamente qualificato ed esperto per assicurarsi che la sicurezza della rete privata non venga compromessa.
2. Affidabilità. Poiché una connessione VPN richiede una connessione a Internet, è importante scegliere un provider collaudato e testato per fornire un servizio Internet eccellente e garantire tempi di inattività minimi o nulli.
3. Scalabilità. Se si verifica una situazione che richiede l'aggiunta di una nuova infrastruttura o l'impostazione di nuove configurazioni, è possibile che si verifichino problemi tecnici dovuti all'incompatibilità, in particolare se si tratta di prodotti o fornitori diversi da quelli già in uso.
4. Problemi di sicurezza per i dispositivi mobili. Talvolta, quando si utilizzano dispositivi mobili durante l'avvio della connessione VPN, possono verificarsi problemi di protezione, in particolare quando si utilizza una connessione wireless. Alcuni provider non verificati si presentano come "provider VPN gratuiti" e possono persino installare malware nel computer. Per questo motivo, è possibile aggiungere ulteriori misure di sicurezza per prevenire tali problemi quando si utilizzano dispositivi mobili.
5. Velocità di connessione lente. Se si utilizza un client VPN che fornisce un servizio VPN gratuito, è probabile che la velocità della connessione venga rallentata poiché questi provider non assegnano la priorità alle velocità di connessione.

In questo documento viene spiegato come configurare la connessione VPN sul router serie RV34x con la Configurazione guidata.

Dispositivi interessati

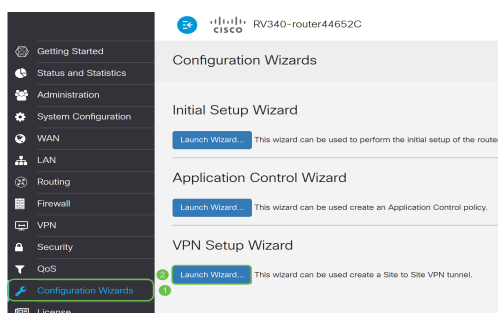
- Serie RV34x

Versione del software

- 1.0.01.16

Configurare la connessione VPN utilizzando l'Installazione guidata

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione guidata**. Quindi fare clic su **Avvia procedura guidata** nella sezione *Installazione guidata VPN*.



Passaggio 2. Nel campo fornito, immettere un nome per identificare la connessione.

This Setup Wizard helps you to configure a secure connection between two routers that physically separated over the IPSec VPN tunnel.
Before your begin, you need to know the subnet addresses of your local and remote networks, and import the digital certificates for authentication between two peers if needed.
Give this connection a name: E.g Homeoffice

Nota: Nell'esempio viene utilizzato TestVPN.

Passaggio 3. Nell'area Interfaccia, fare clic sul menu a discesa e scegliere l'interfaccia per cui abilitare la connessione. Le opzioni sono:

- WAN1
- WAN2
- USB1
- USB2



Nota: nell'esempio viene usata la WAN1.

Passaggio 4. Fare clic su **Avanti**.

Give this connection a name: E.g Homeoffice

Interface:

Next

Cancel

Passaggio 5. Scegliere il tipo di connessione remota facendo clic sulla freccia dell'elenco a discesa. Le opzioni sono:

- Indirizzo IP: scegliere questa opzione se si desidera utilizzare l'indirizzo IP del router remoto all'altra estremità del tunnel VPN.
- FQDN: (nome di dominio completo) scegliere questa opzione se si desidera utilizzare il nome di dominio del router remoto all'altra estremità del tunnel VPN.

Remote Connection Type:

Remote Connection: Enter WAN IP Address

Nota: Nell'esempio, viene scelto IP Address (Indirizzo IP).

Passaggio 6. Immettere l'indirizzo IP WAN della connessione remota nel campo fornito e fare clic su **Avanti**.

Remote Connection Type: IP Address

Remote Connection: 128.123.2.1 Enter WAN IP Address

Back **Next** Cancel

Nota: nell'esempio viene usato 128.123.2.1.

Passaggio 7. Nell'area Selezione traffico locale, fare clic sull'elenco a discesa per scegliere l'indirizzo IP locale. Le opzioni sono:

- Subnet: selezionare questa opzione se si desidera immettere sia l'indirizzo IP che la subnet mask della rete locale.
- Indirizzo IP: scegliere questa opzione se si desidera immettere solo l'indirizzo IP della rete locale.
- Qualsiasi - Scegliete questo se volete uno dei due.

Local Traffic Selection

Local IP: Subnet

IP Address: Subnet
IP Address

Subnet Mask: Any

Remote Traffic Selection:

Remote IP: Subnet

IP Address:

Subnet Mask:

Nota: Nell'esempio, viene scelto Qualsiasi.

Passaggio 8. Nell'area di selezione del traffico remoto, fare clic sulla freccia dell'elenco a discesa per scegliere l'indirizzo IP remoto. Immettere l'indirizzo IP remoto e la subnet mask nell'apposito campo, quindi fare clic su **Avanti**. Le opzioni sono:

- Subnet: selezionare questa opzione se si desidera immettere sia l'indirizzo IP che la subnet mask della rete remota.
- Indirizzo IP: scegliere questa opzione se si desidera immettere solo l'indirizzo IP della rete remota.

Local Traffic Selection

Local IP: Any

Remote Traffic Selection:

Remote IP: Subnet

IP Address: 10.10.10.0

Subnet Mask: 255.255.255.0

Back **Next** Cancel

Nota: Nell'esempio riportato di seguito, viene scelto Subnet. 10.10.10.0 è stato immesso come indirizzo IP e 255.255.255.0 come subnet mask.

Passaggio 9. Per scegliere il profilo da utilizzare, fare clic sulla freccia nell'area Profilo IPsec.

IPSec Profile:


IKE Version: IKEv1 IKEv2

Nota: In questo esempio, viene selezionato Default.

Passaggio 10. Nell'area Opzioni fase 1, immettere la chiave già condivisa per questa connessione nell'apposito campo. Questa è la chiave già condivisa da utilizzare per autenticare il peer IKE (Internet Key Exchange) remoto. Entrambe le estremità del tunnel VPN devono utilizzare la stessa chiave precondivisa. Per questa chiave è consentito l'utilizzo di un massimo di 30 caratteri o valori esadecimali.

Nota: Si consiglia di modificare regolarmente la chiave già condivisa per mantenere la sicurezza della connessione VPN.

Pre-Shared Key:

Pre-shared Key Strength Meter: 


Show Pre-shared Key: Enable

Nota: L'indicatore di livello chiave già condivisa indica l'intensità della chiave immessa in base a quanto segue:

- Rosso — la password è debole.
- Ambra — La password è abbastanza complessa.
- Verde: la password è complessa.

Passaggio 11. (Facoltativo) È inoltre possibile selezionare la casella di controllo **Abilita** in Mostra testo normale durante la modifica per visualizzare la password in testo normale.

Pre-Shared Key:

Pre-shared Key Strength Meter: 

Show Pre-shared Key: Enable

Passaggio 12. Fare clic su **Avanti**.



Passaggio 13. Nella pagina verranno visualizzati tutti i dettagli di configurazione della connessione VPN. Fare clic su **Invia**.

VPN Setup Wizard



Getting Started

Remote Router Settings

Local and Remote Networks

Profile

Summary

Connection Name: TestVPN

Local Interface: WAN1

IPSec Profile: Default

Phase I Options

DH Group: Group5 - 1536 bit

Encryption: AES 128

Authentication: SHA1

Lifetime(sec) 28800

Pre-Shared Key: CiscoTest123!

Perfect Forward Secrecy: Enable

Phase II Options:

DH Group: Group5 - 1536 bit

Protocol Selection: ESP

Back

Submit

Cancel

La connessione VPN sul router serie RV34x dovrebbe essere stata configurata correttamente con la Configurazione guidata. Per connettere correttamente una VPN da sito a sito, è necessario configurare l'Installazione guidata sul router remoto.