# Configurazione della VPN da sito a sito sugli switch RV160 e RV260

## Obiettivo

L'obiettivo di questo documento è creare una VPN da sito a sito sui router serie RV160 e RV260.

## Introduzione

Una rete privata virtuale (VPN) è un ottimo modo per connettere i dipendenti remoti a una rete protetta. Una VPN consente a un host remoto di agire come se fosse connesso alla rete protetta in loco. In una VPN da sito a sito, il router locale in una posizione si connette a un router remoto tramite un tunnel VPN. Questo tunnel incapsula i dati in modo sicuro utilizzando tecniche di crittografia e autenticazione standard per proteggere i dati inviati.

Notare che quando si configura la VPN da sito a sito, le subnet LAN (Local Area Network) su entrambi i lati del tunnel non possono trovarsi sulla stessa rete. Ad esempio, se la LAN del sito A utilizza la subnet 192.168.***1***.x/24, il sito B non può utilizzare la stessa subnet. Il sito B deve utilizzare una subnet diversa, ad esempio 192.168.***2***.x/24.

Per configurare correttamente un tunnel, immettere le impostazioni corrispondenti (inversione locale e remota) durante la configurazione dei due router. Si supponga che questo router sia identificato come router A. Immettere le relative impostazioni nella sezione Local Group Setup immettendo quelle dell'altro router (router B) nella sezione Remote Group Setup. Quando si configura l'altro router (router B), immetterne le impostazioni nella sezione Local Group Setup e le impostazioni del router A in Remote Group Setup.

Di seguito è riportata una tabella della configurazione del router A e del router B. I parametri evidenziati in grassetto sono l'inverso del router opposto. Tutti gli altri parametri rimangono configurati allo stesso modo. In questo documento, verrà configurata la porta locale con il router A.

| Campi | Router A (locale)<br>Indirizzo IP WAN: 140,x,x,x<br>Indirizzo IP locale: 192.168.2.0/24 | Router B (remoto)<br>Indirizzo IP WAN: 145,x,x,x<br>Indirizzo IP locale: 10.1.1.0/24 |
|---|---|---|
| **Nome connessione** | **VPNTest** | **VPNTestB** |
| **Profilo IPSec** | **HomeOffice (ha la stessa configurazione di RemoteOffice)** | **RemoteOffice (ha la stessa configurazione di HomeOffice)** |
| Interfaccia | WAN | WAN |
| **Endpoint remoto** | **IP statico: 145,x,x,x** | **IP statico: 140,x,x,x** |
| Metodo di autenticazione IKE | Chiave già condivisa<br>Chiave già condivisa: Cisco Test 123 | Chiave già condivisa<br>Chiave già condivisa: Cisco Test 123 |
| Tipo di identificatore locale | IP WAN locale | IP WAN locale |
| **Identificatore locale** | **140,x,x,x** | **145,x,x,x** |
| Tipo IP locale | Subnet | Subnet |

| | | |
|---|---|---|
| **Indirizzo IP locale** | **192.168.2.0** | **10.1.1.0** |
| Subnet mask locale | 255.255.255.0 | 255.255.255.0 |
| Tipo di identificatore remoto | Remote WAN IP | Remote WAN IP |
| **Identificatore remoto** | **145,x,x,x** | **140,x,x,x** |
| Tipo di IP remoto | Subnet | Subnet |
| **Indirizzo IP remoto** | **10.1.1.0** | **192.168.2.0** |
| Subnet mask remota | 255.255.255.0 | 255.255.255.0 |
| Modalità aggressiva | Disattivato | Disattivato |

Per informazioni su come configurare il profilo IPSec, vedere l'articolo relativo a: Configurazione dei profili IPSec (modalità di impostazione automatica della trasparenza) sui modelli RV160 e RV260.

Per configurare la VPN da sito a sito utilizzando la configurazione guidata, vedere l'articolo su: Configurazione della Configurazione guidata VPN su RV160 e RV260.

## Dispositivi interessati

- RV160
- RV260

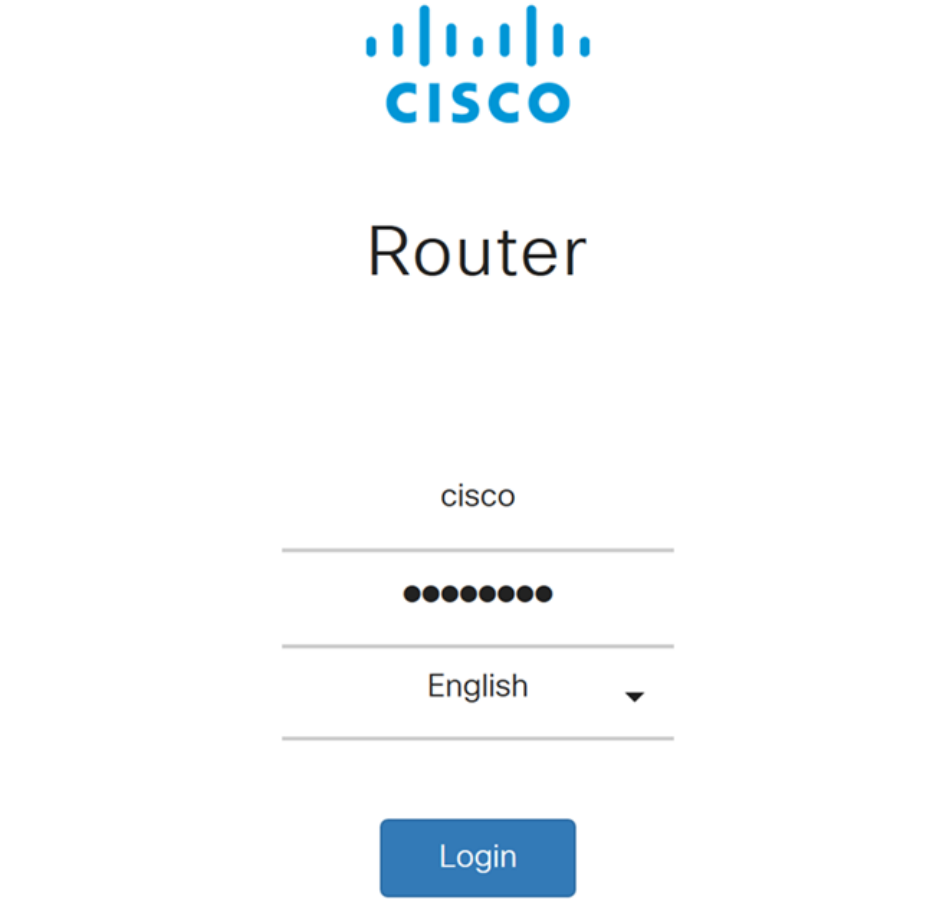
## Versione del software

- 1.0.00.13

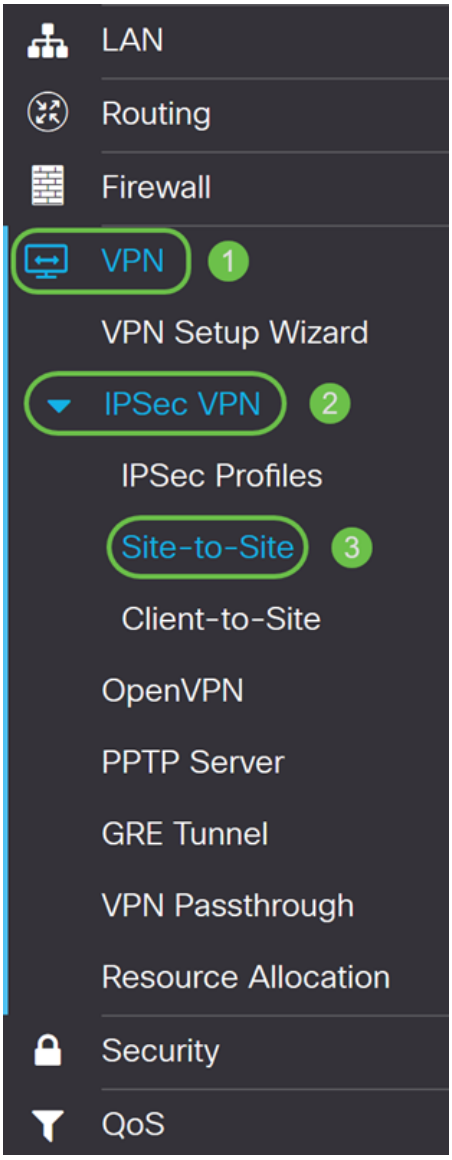
## Configurazione della connessione VPN da sito a sito - Router A

Passaggio 1. Accedere alla pagina di configurazione Web del router A.

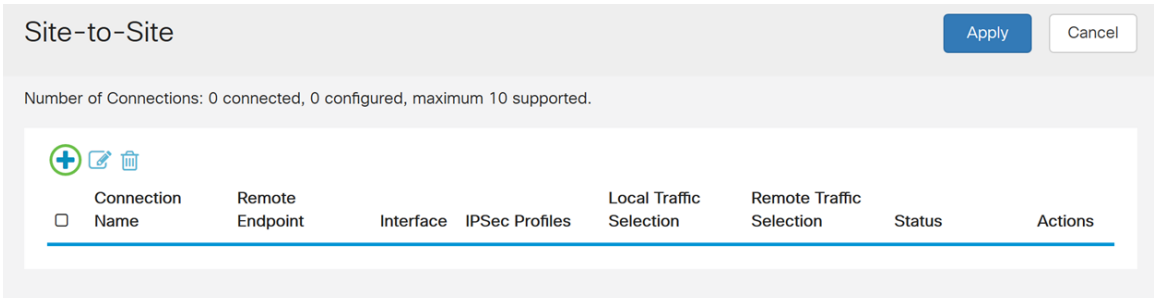
**Nota:** Utilizzeremo RV160 per entrambi i router.



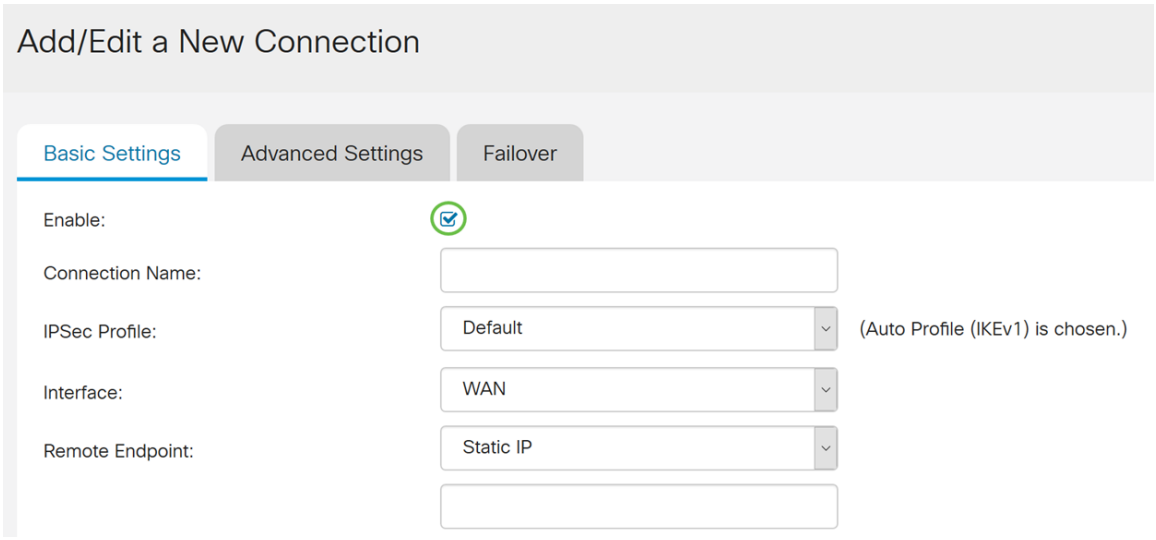

Passaggio 2. Passare a **VPN > IPSec VPN > Da sito a sito**.




Passaggio 3. Fare clic sul pulsante **add** per aggiungere una nuova connessione VPN da sito a sito.

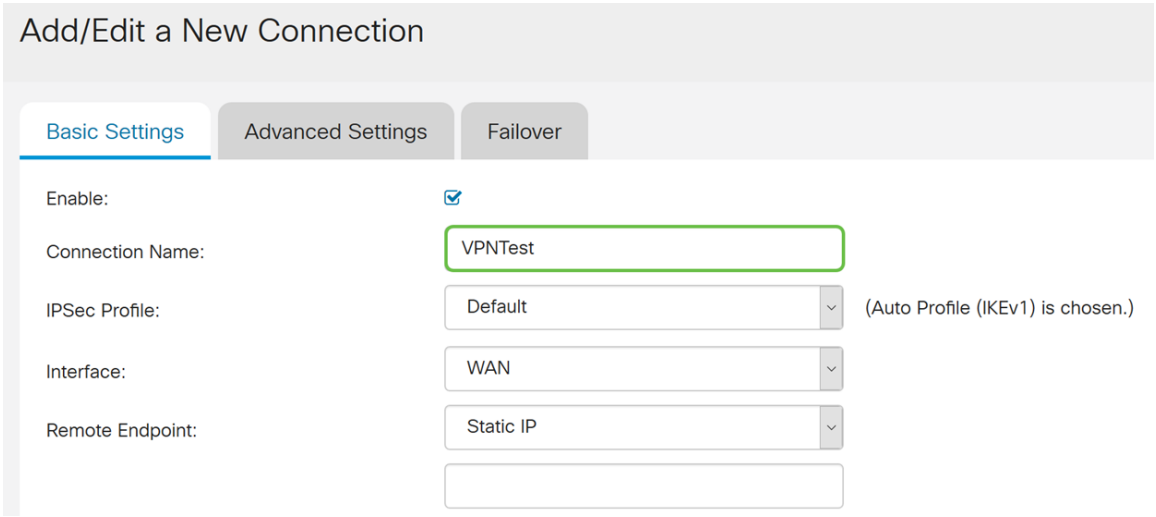



Passaggio 4. Selezionare **Enable** (Abilita) per abilitare la configurazione. L'opzione è abilitata per impostazione predefinita.




Passaggio 5. Immettere un nome di connessione per il tunnel VPN. Questa descrizione è utilizzata a scopo di riferimento e non deve corrispondere al nome utilizzato all'altra estremità del tunnel.

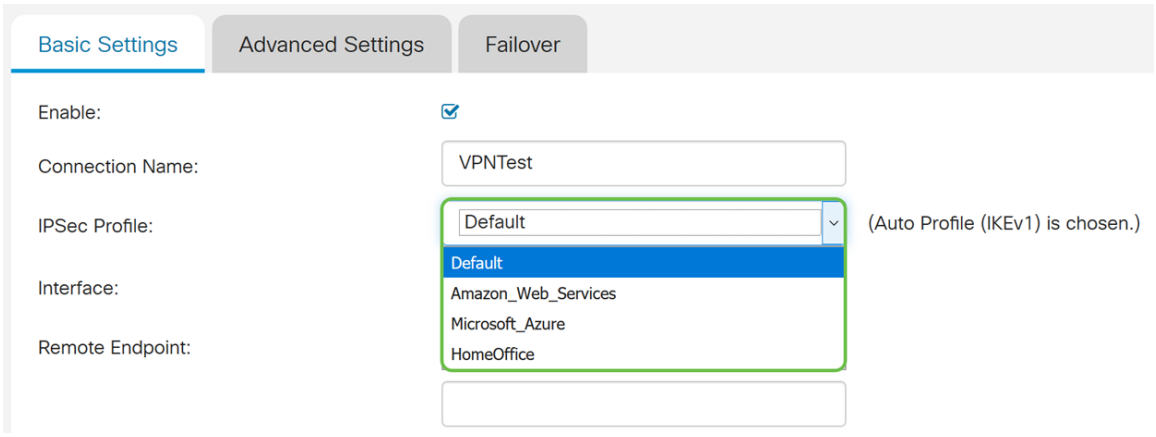
In questo esempio verrà immesso **VPNTest** come nome della connessione.



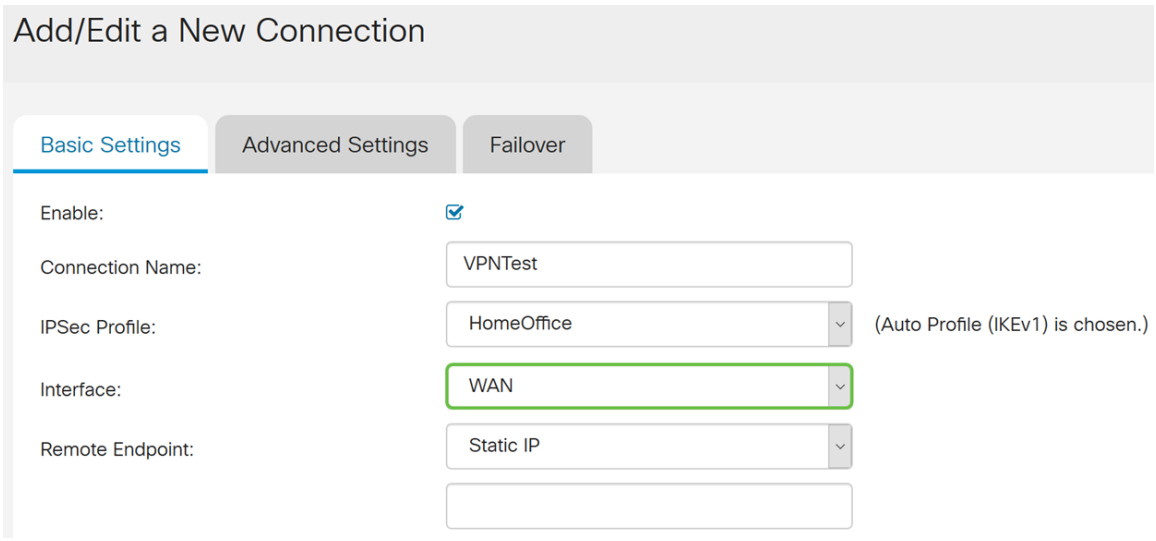

Passaggio 6. Se è stato creato un nuovo profilo IPSec o si desidera utilizzarne uno predefinito (Amazon_Web_Services, Microsoft_Azure), selezionare il profilo IPSec da utilizzare per la VPN. L'opzione Default - Profilo automatico (Default - Auto Profile) è selezionata per default. Il profilo IPSec è la configurazione centrale di IPSec che definisce algoritmi quali la crittografia, l'autenticazione e il gruppo Diffie-Hellman (DH) per la negoziazione di Fase I e Fase II.

In questo esempio verrà selezionato **HomeOffice** come profilo IPsec.

**Nota:** Per ulteriori informazioni sulla creazione di un profilo IPSec, vedere l'articolo: Configurazione dei profili IPSec (modalità di impostazione automatica della trasparenza) sui modelli RV160 e RV260.

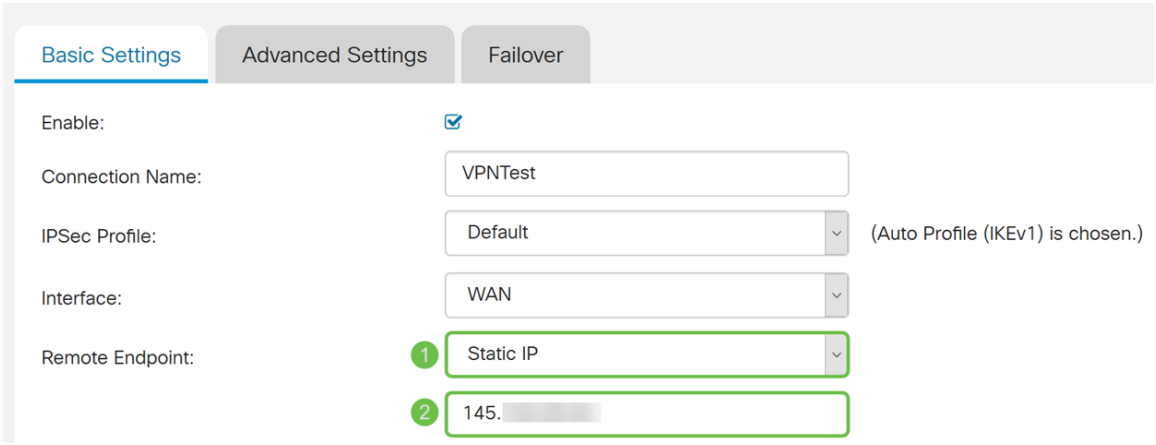



Passaggio 7. Nel campo *Interface* (Interfaccia), selezionare l'interfaccia utilizzata per il tunnel. Nell'esempio, utilizzeremo **WAN** come interfaccia.




Passaggio 8. Selezionare **IP statico**, **nome di dominio completo (FQDN)** o **IP dinamico** per l'*endpoint remoto*. Immettere l'indirizzo IP o il nome di dominio completo (FQDN) dell'endpoint remoto in base alla selezione effettuata.

È stato selezionato **Static IP** (IP statico) ed è stato immesso l'indirizzo IP dell'endpoint remoto.




## Configurazione del metodo di autenticazione IKE

Passaggio 1. Selezionare **Chiave già condivisa** o **Certificato**. In questa dimostrazione verrà selezionata la **chiave già condivisa** come metodo di autenticazione IKE.

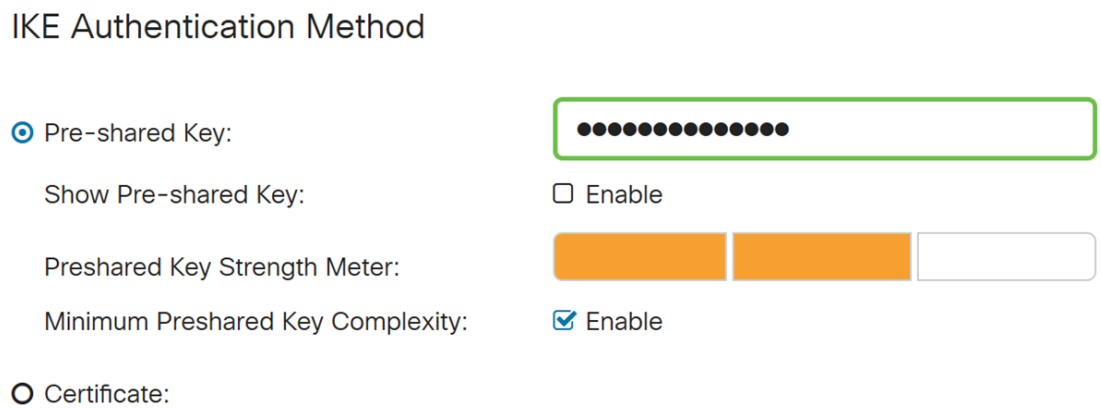
I peer IKE si autenticano a vicenda tramite il calcolo e l'invio di hash di dati con chiave che include la chiave precondivisa. Se il peer ricevente è in grado di creare lo stesso hash in

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.

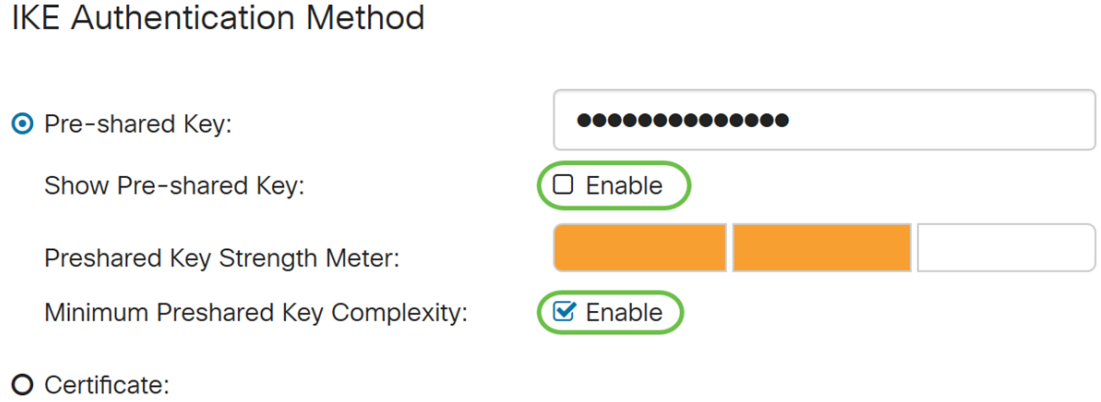
Il certificato digitale è un pacchetto che contiene informazioni quali l'identificazione di un titolare di certificato: nome o indirizzo IP, numero di serie del certificato, data di scadenza del certificato e copia della chiave pubblica del titolare del certificato. Il formato del certificato digitale standard è definito nella specifica X.509. X.509 versione 3 definisce la struttura di dati per i certificati. Se è stato selezionato **Certificato**, verificare che il certificato firmato sia stato importato in **Amministrazione > Certificato**. Selezionare il certificato dall'elenco a discesa per locale e remoto.


Passaggio 2. Nel campo *Chiave già condivisa*, immettere una chiave già condivisa.

**Nota:** Verificare che il router remoto utilizzi la stessa chiave già condivisa.

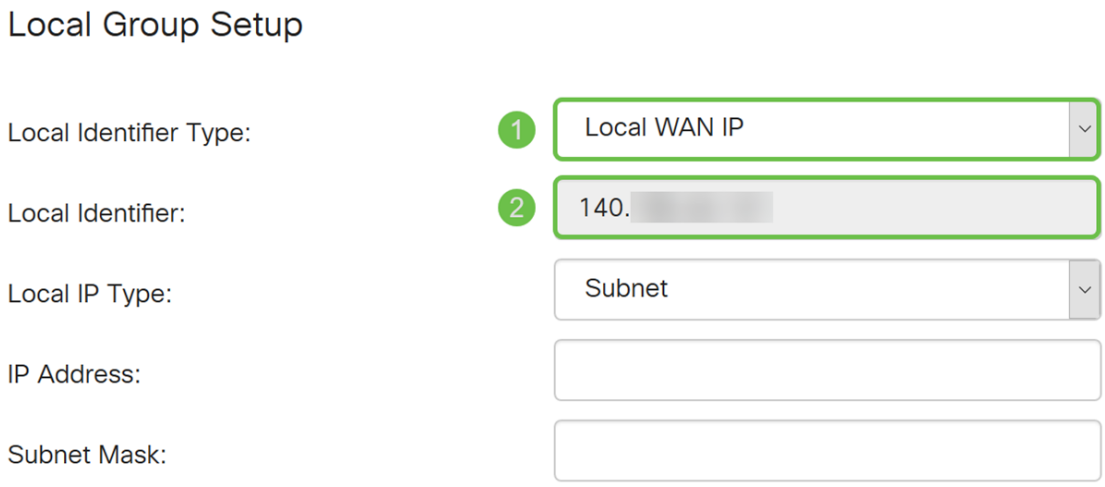



Passaggio 3. Selezionare la casella di controllo **Abilita** se si desidera visualizzare la chiave già condivisa. Il *Misuratore dell'intensità della chiave già condivisa* mostra l'intensità della chiave già condivisa tramite barre colorate. Selezionare **Abilita** per abilitare la complessità minima della chiave già condivisa. Passare quindi alla sezione *For Local Group Setup*.



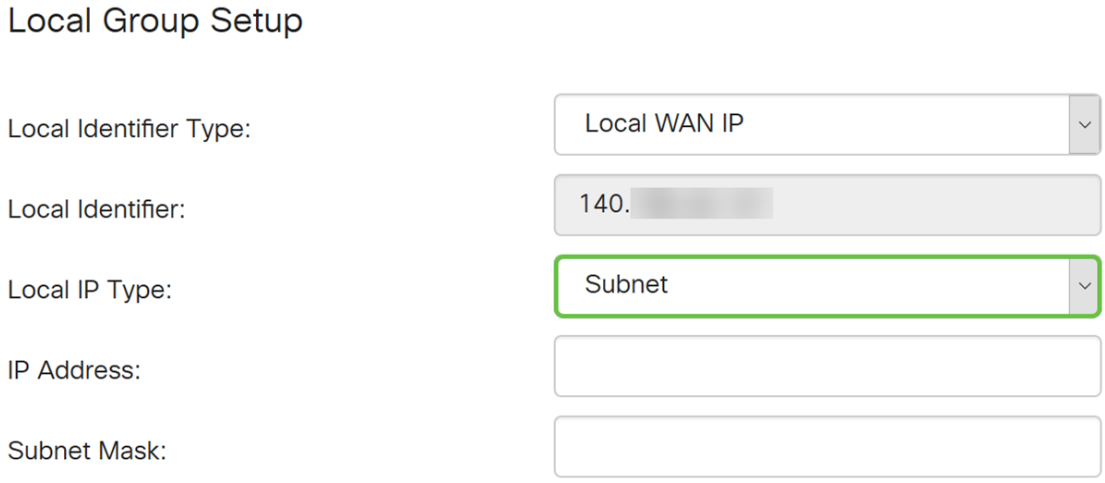
### Per l'installazione del gruppo locale

Passaggio 1. Selezionare **Local WAN IP**, **IP Address**, **Local FQDN** o **Local User FQDN** dall'elenco a discesa. Immettere il nome o l'indirizzo IP dell'identificatore in base alla selezione effettuata. Se è stato selezionato **Local WAN IP**, l'indirizzo IP WAN del router deve essere immesso automaticamente.



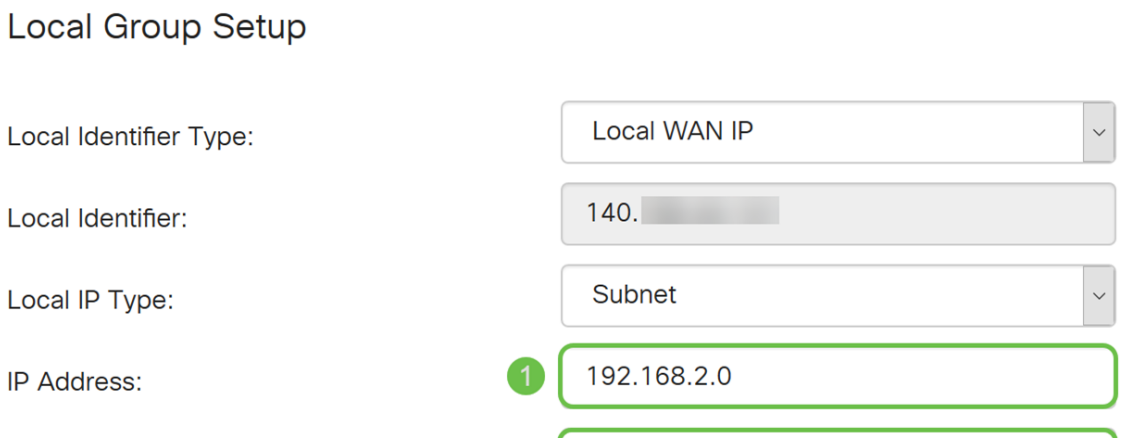

Passaggio 2. Per il tipo di IP locale, selezionare Subnet, Single, **Any**, **IP Group** o **GRE Interface** dall'elenco a discesa.

Nell'esempio riportato di seguito è stata scelta **la subnet**.




Passaggio 3. Immettere l'indirizzo IP del dispositivo che può utilizzare il tunnel. Immettere quindi la subnet mask.

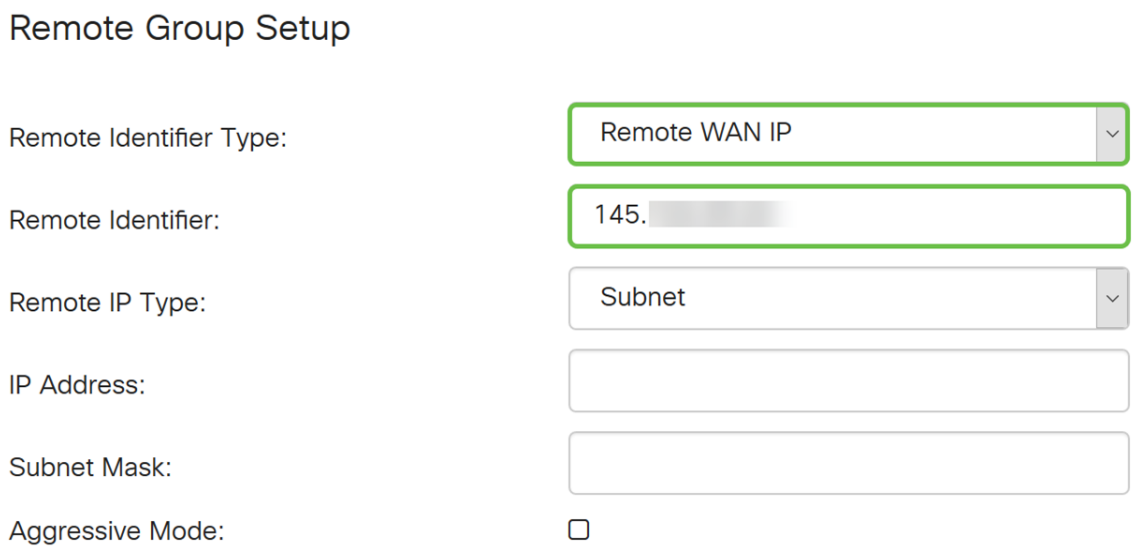
Per questa dimostrazione, immetteremo **192.168.2.0** come indirizzo IP locale e **255.255.255.0** come subnet mask.



## Installazione gruppo remoto

Passaggio 1. Selezionare **Remote WAN IP**, **Remote FQDN** o **Remote User FQDN** dall'elenco a discesa. Immettere il nome o l'indirizzo IP dell'identificatore in base alla selezione effettuata.

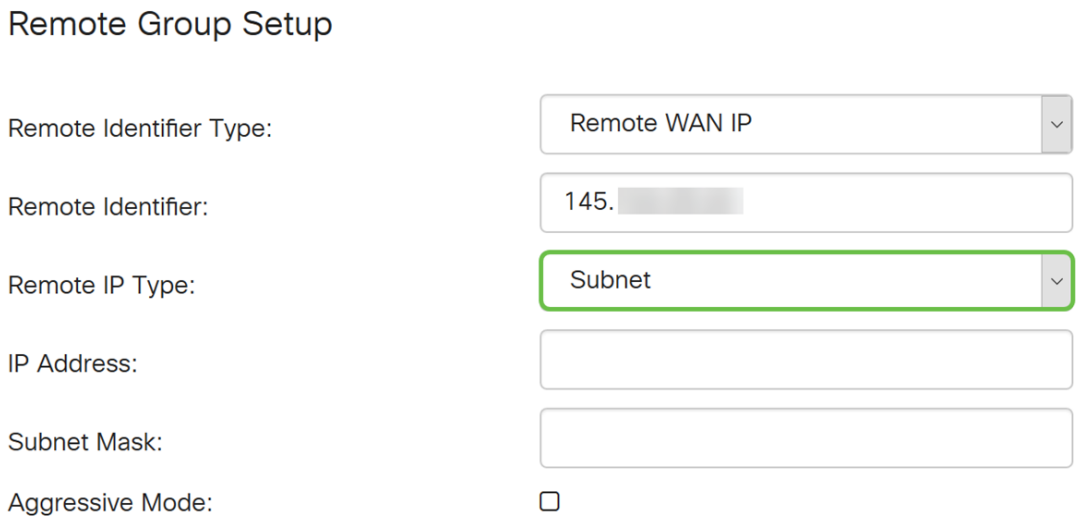
Abbiamo selezionato **Remote WAN IP** come *Remote Identifier Type* e abbiamo immesso l'indirizzo IP del router remoto.




Passaggio 2. Selezionare Subnet, **Single**, **Any**, **IP Group** dall'elenco a discesa *Remote IP Type*.

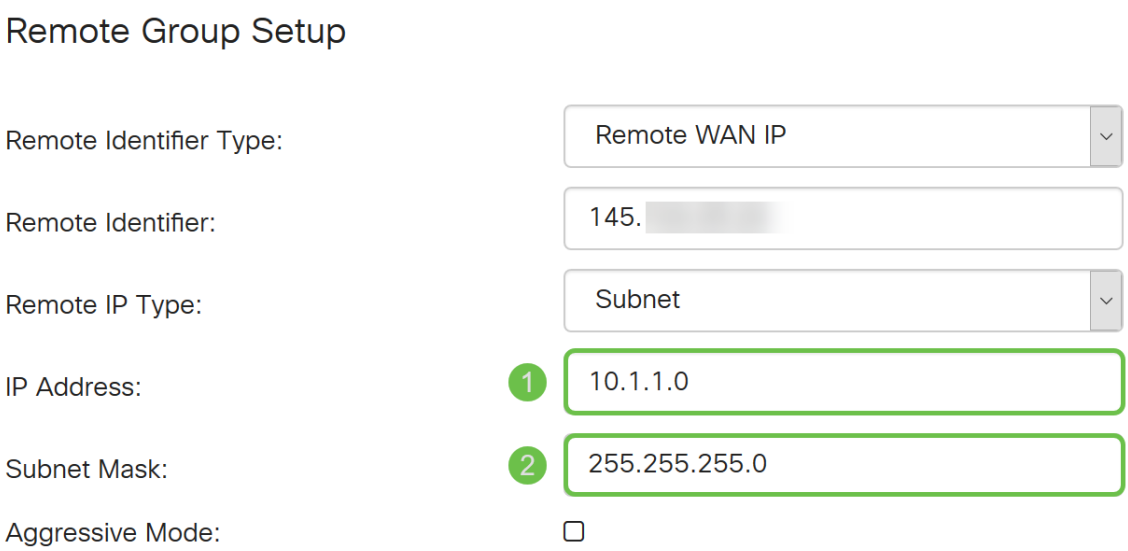
In questo esempio verrà selezionata la **subnet**.

**Nota:** Se è stato selezionato Gruppo IP come tipo di IP remoto, viene visualizzata una finestra popup per creare un nuovo gruppo IP.




Passaggio 3. Immettere l'indirizzo IP locale remoto e la subnet mask del dispositivo che può utilizzare questo tunnel.

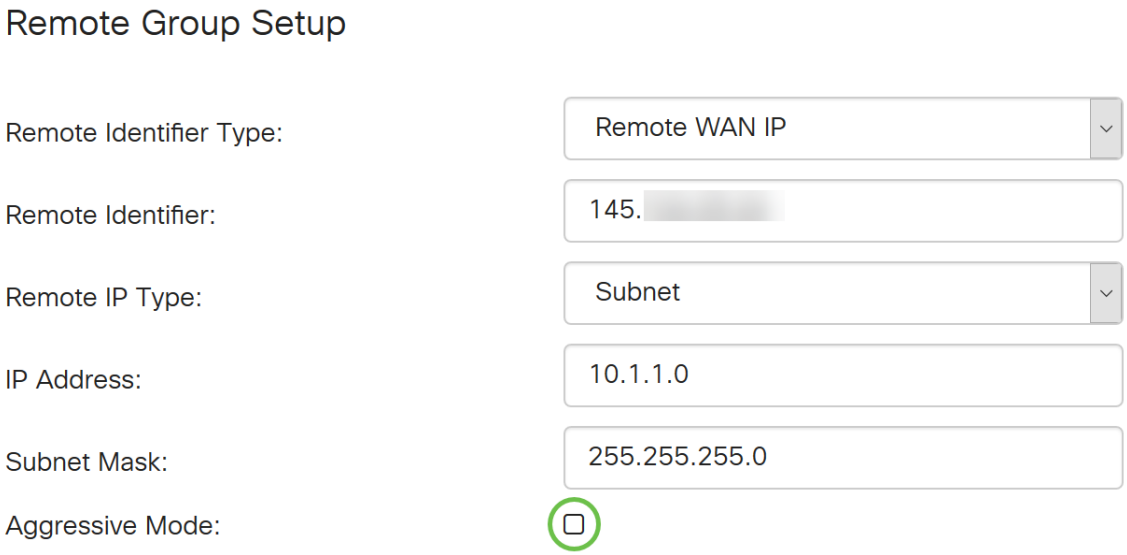
Abbiamo immesso **10.1.1.0** per l'indirizzo IP locale remoto che può usare questo tunnel e la subnet mask **255.255.255.0**.



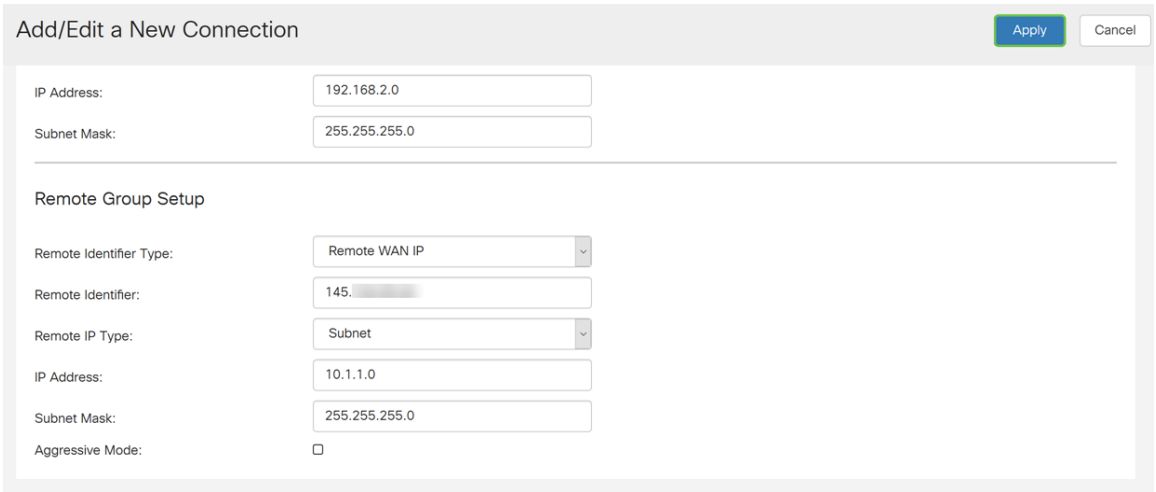

Passaggio 4. Selezionare la casella per abilitare la modalità aggressiva. La modalità aggressiva si ha quando la negoziazione per l'associazione di protezione IKE viene compressa in tre pacchetti, con tutti i dati dell'associazione di protezione che devono essere passati dall'iniziatore. I negoziati sono più rapidi, ma presentano una vulnerabilità di identità di scambio in testo chiaro.

In questo esempio non verrà selezionata.

**Nota:** Per ulteriori informazioni sulla modalità principale o aggressiva, vedere: Modalità Principale E Modalità Aggressiva




Passaggio 5. Fare clic su **Applica** per creare una nuova connessione VPN da sito a sito.

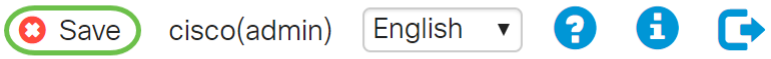


## Conclusioni

A questo punto dovrebbe essere stata aggiunta una nuova connessione VPN da sito a sito per il router locale. È necessario configurare il router remoto (router B) utilizzando le informazioni di inversione.

Tutta la configurazione attualmente in uso sul router si trova nel file della configurazione in esecuzione, che è volatile nel senso che non viene conservata tra un riavvio e l'altro.

Passaggio 1. Nella parte superiore della pagina, fare clic sul pulsante **Save** per accedere a *Configuration Management* e salvare la configurazione in esecuzione nella configurazione di avvio. In questo modo, la configurazione viene conservata tra un riavvio e l'altro.




Passaggio 2. Nella gestione della configurazione, verificare che l'*origine* sia **Configurazione in esecuzione** e che la *destinazione* sia **Configurazione di avvio**. Quindi, premere **Apply** per salvare la configurazione in esecuzione nella configurazione di avvio. Tutta la configurazione attualmente in uso sul router si trova nel file della configurazione in esecuzione, che è volatile e non viene conservata tra un riavvio e l'altro. Se si copia il file della configurazione di esecuzione nel file della configurazione di avvio, tutte le configurazioni verranno mantenute tra un riavvio e l'altro.