

Configurazione della VPN da sito a sito sulla RV34x

Obiettivo

L'obiettivo di questo documento è creare una VPN da sito a sito sui router serie RV34x.

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.

La configurazione di una VPN da sito a sito implica l'impostazione del profilo IPsec e della configurazione della VPN da sito a sito sui due router. Il profilo IPsec è già configurato per semplificare la configurazione della VPN da sito a sito, anche con terze parti (ad esempio AWS o Azure). Il profilo IPsec contiene tutta la crittografia necessaria per il tunnel. La VPN da sito a sito è la configurazione in modo che il router sappia a quale altro sito connettersi. Se si sceglie di non utilizzare il profilo IPsec preconfigurato, è possibile crearne uno diverso.

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 sono configurati allo stesso modo. In questo documento viene descritto come configurare il router locale, il router A.

Campo	Router locale (Router A)	Router remoto (Router B)
	Indirizzo IP WAN: 140,x,x,x	Indirizzo IP WAN: 145,x,x,x
	Indirizzo IP privato (locale): 192.168.2.0/24	Indirizzo IP privato (locale): 10.1.1.0/24
Nome connessione	VPNTest	VPNTestRemote
Profilo IPsec	ProfiloProva	ProfiloProva
Interfaccia	WAN1	WAN1

Endpoint remoto	IP statico	IP statico
Indirizzo IP endpoint remoto	145,x,x,x	140,x,x,x
Chiave già condivisa	Cisco Test 123	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

Dispositivi interessati

- RV34x

Versione del software

- 1.0.02.16

Configurazione della connessione VPN da sito a sito

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



Router

cisco



English

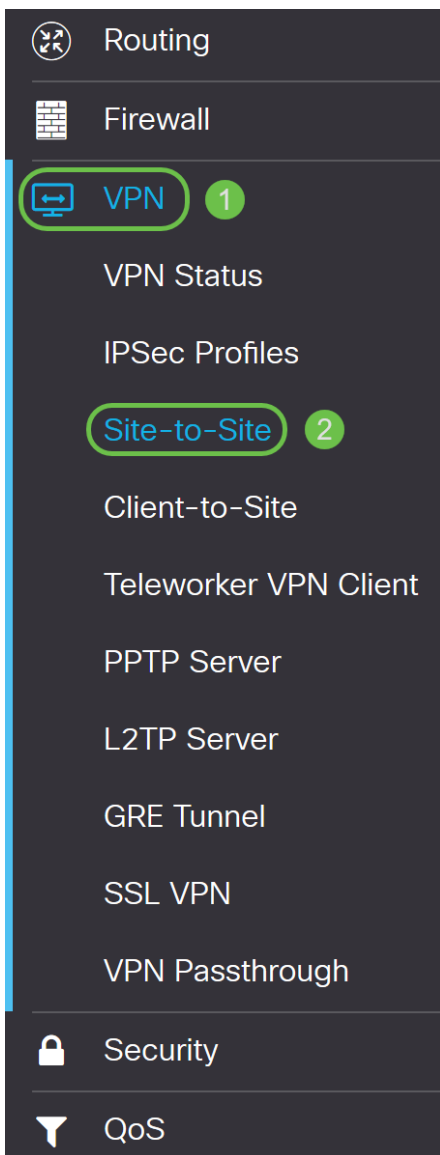


Login

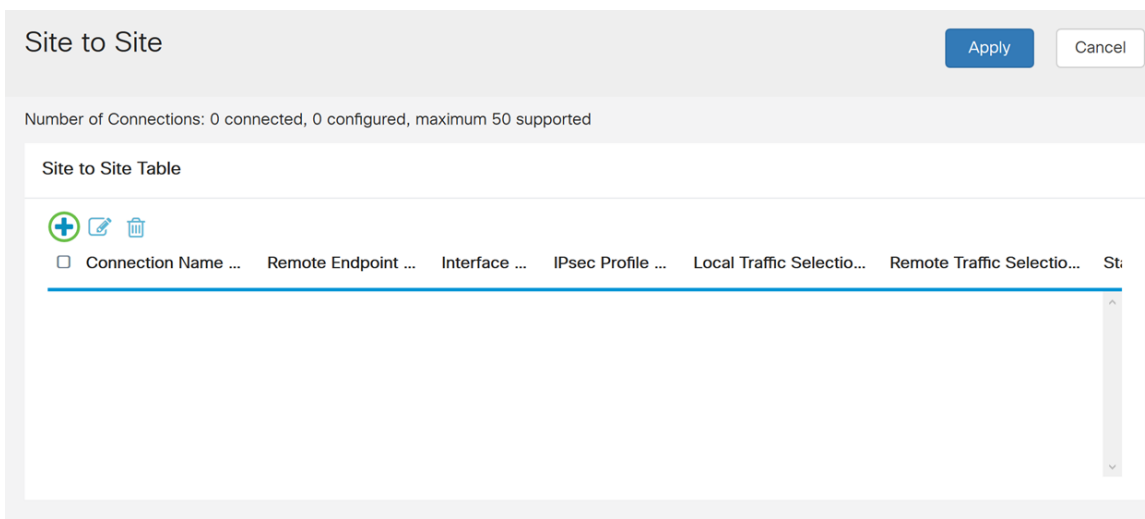
©2017-2018 Cisco Systems, Inc. All rights reserved.

Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Passaggio 2. Passare a 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.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name: Please Input Connection Name

IPsec Profile: Default Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

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.

Basic Settings | Advanced Settings | Failover

Enable:

Connection Name: VPNTest

IPsec Profile: Default Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

Passaggio 6. Selezionare il profilo IPsec che si desidera utilizzare per la VPN. 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.

Per informazioni su come configurare il profilo IPsec utilizzando IKEv2, fare clic sul collegamento: [Configurazione del profilo IPsec con IKEv2 su RV34x](#).

Nota: È possibile utilizzare un profilo IPsec di terze parti (Servizi Web Amazon o Microsoft Azure). Questo profilo IPsec è già configurato con tutte le selezioni necessarie da configurare per Amazon Web Services o Microsoft Azure, quindi non è necessario configurarlo. Se si sta tentando di configurare una VPN da sito a sito tra AWS o Azure per il sito, è necessario utilizzare le informazioni fornite da AWS o Azure e utilizzare il profilo IPsec preconfigurato per la configurazione della VPN da sito a sito su questo lato.

Nell'esempio, verrà selezionato **TestProfile** come profilo IPsec.

Basic Settings | Advanced Settings | Failover

Enable:

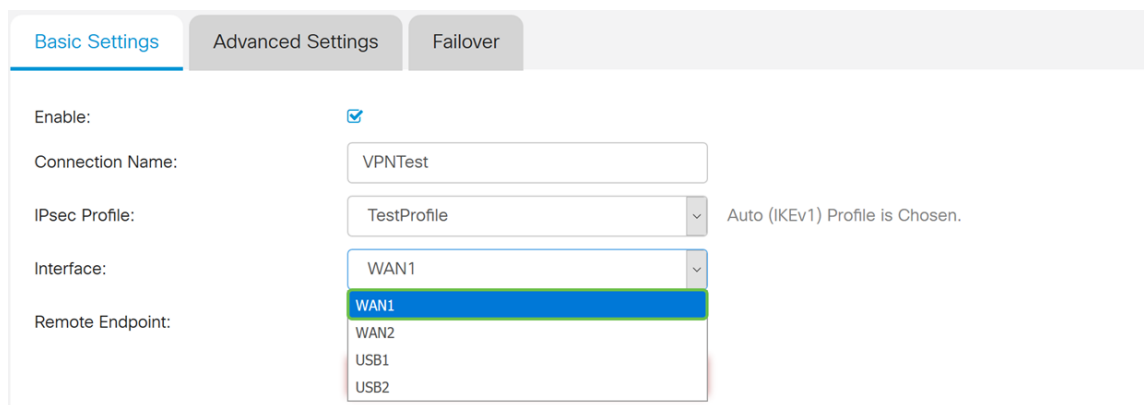
Connection Name: VPNTest

IPsec Profile: TestProfile Auto (IKEv1) Profile is Chosen.

Interface: WAN1

Remote Endpoint: Static IP

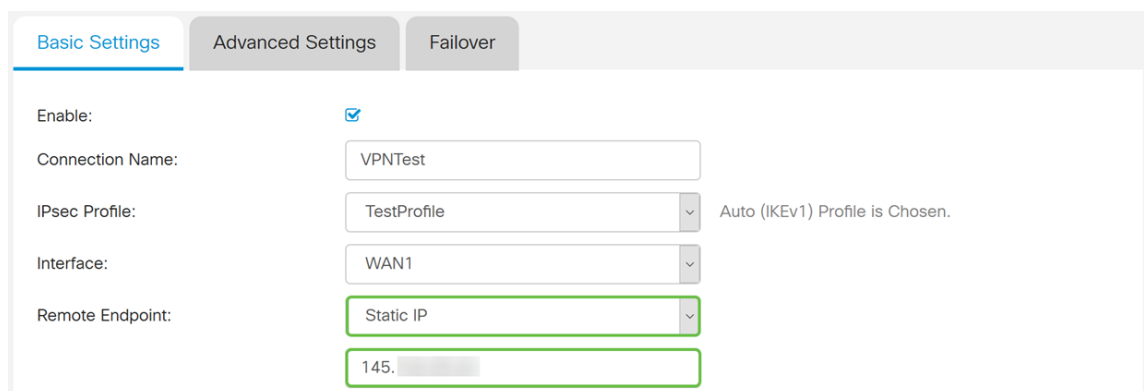
Passaggio 7. Nel campo *Interface* (Interfaccia), selezionare l'interfaccia utilizzata per il tunnel. Nell'esempio, utilizzeremo **WAN1** come interfaccia.



The screenshot shows the 'Basic Settings' tab of a VPN configuration interface. The 'Enable' checkbox is checked. The 'Connection Name' is 'VPNTest'. The 'IPsec Profile' is 'TestProfile' with a note 'Auto (IKEv1) Profile is Chosen.'. The 'Interface' dropdown menu is open, showing 'WAN1' selected. Other options include WAN2, USB1, and USB2. The 'Remote Endpoint' field is empty.

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.



The screenshot shows the 'Basic Settings' tab of a VPN configuration interface. The 'Enable' checkbox is checked. The 'Connection Name' is 'VPNTest'. The 'IPsec Profile' is 'TestProfile' with a note 'Auto (IKEv1) Profile is Chosen.'. The 'Interface' dropdown menu is set to 'WAN1'. The 'Remote Endpoint' dropdown menu is set to 'Static IP'. The IP address '145.' is entered in the adjacent field.

Configurazione del metodo di autenticazione IKE

Passaggio 1. Selezionare **Chiave già condivisa** o **Certificato**.


Chiave già condivisa: 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. Entrambi i peer devono condividere la stessa chiave segreta. Se il peer ricevente è in grado di creare lo stesso hash in modo indipendente utilizzando la chiave già condivisa, autentica 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 titolare del certificato, incluso un nome o un indirizzo IP, il numero di serie del certificato, la data di scadenza 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. 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.

In questa dimostrazione verrà selezionata la **chiave già condivisa** come metodo di autenticazione IKE.

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable

Show Pre-shared Key: Enable


Certificate:

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

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

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: Enable


Show Pre-shared Key: Enable

Certificate:

Passaggio 3. 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. La complessità della chiave già condivisa viene controllata per impostazione predefinita. Se si desidera visualizzare la chiave già condivisa, selezionare la casella di controllo **Abilita**.

IKE Authentication Method:

Pre-shared Key:

Pre-shared Key Strength Meter: 

Minimum Pre-shared Key Complexity: 1 Enable

Show Pre-shared Key: 2 Enable

Certificate:

Installazione 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.

Local Group Setup

Local Identifier Type: 1

Local Identifier: 2

Local IP Type:

IP Address:

Subnet Mask:

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**.

Local Group Setup

Local Identifier Type:

Local Identifier:

Local IP Type:

IP Address:

Subnet Mask:

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.

Local Group Setup

Local Identifier Type:	<input type="text" value="Local WAN IP"/>
Local Identifier:	<input type="text" value="140."/>
Local IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text" value="192.168.2.0"/>
Subnet Mask:	<input type="text" value="255.255.255.0"/>

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.

Remote Group Setup

Remote Identifier Type:	<input type="text" value="Remote WAN IP"/>
Remote Identifier:	<input type="text" value="145."/>
Remote IP Type:	<input type="text" value="Subnet"/>
IP Address:	<input type="text"/>
Subnet Mask:	<input type="text"/>

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.

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 145.

Remote IP Type: Subnet

IP Address:

Subnet Mask:

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

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 145.

Remote IP Type: Subnet

IP Address: 1 10.1.1.0

Subnet Mask: 2 255.255.255.0

Passaggio 4. Fare clic su **Applica** per creare una nuova connessione VPN da sito a sito.

Add/Edit a New Connection Apply Cancel

Local IP Type: Subnet

IP Address: 192.168.2.0

Subnet Mask: 255.255.255.0

Remote Group Setup

Remote Identifier Type: Remote WAN IP

Remote Identifier: 145.

Remote IP Type: Subnet

IP Address: 10.1.1.0

Subnet Mask: 255.255.255.0

Tutte le configurazioni immesse sul router si trovano nel file della configurazione in

esecuzione, che è volatile e non viene conservato tra un riavvio e l'altro.

Passaggio 5. Nella parte superiore della pagina, fare clic sul pulsante **Save** per accedere a *Configuration Management* (Gestione configurazione) e salvare la configurazione in esecuzione nella configurazione di avvio. in modo da conservare la configurazione dopo un riavvio.



Passaggio 6. 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. Il file della configurazione di avvio conserverà tutte le configurazioni dopo un riavvio.

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.