

Configurazione delle impostazioni avanzate e del failover della VPN da sito a sito sugli switch RV160 e RV260

Obiettivo

L'obiettivo di questo documento è mostrare come configurare le impostazioni avanzate e il failover della VPN da sito a sito sugli switch 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. Affinché la connessione VPN da sito a sito venga stabilita correttamente, è necessario eseguire una configurazione identica su entrambi i lati della connessione. La configurazione VPN da sito a sito avanzata offre la flessibilità necessaria per configurare configurazioni opzionali per il tunnel VPN.

Il failover è una potente funzionalità che assicura una connessione costante tra questi due siti. Ciò è utile quando è importante la tolleranza d'errore. Il failover si verifica quando il router principale è inattivo. A questo punto, subentra un router secondario o di backup che fornisce una connessione. In questo modo è possibile evitare un singolo punto di errore.

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.00.13

Prerequisiti

Prima di configurare le impostazioni avanzate e il failover per la VPN da sito a sito sugli switch RV160 e RV260, è necessario configurare il profilo IPsec e la VPN da sito a sito sul router locale e remoto. Di seguito è riportato un elenco di articoli che consentono di configurarli. È possibile utilizzare la Configurazione guidata VPN, che consente di configurare sia il profilo IPsec che la VPN da sito a sito, oppure è possibile configurarli separatamente e seguire i due documenti forniti di seguito.

1. [Configurazione guidata VPN Setup su RV160 e RV260](#)

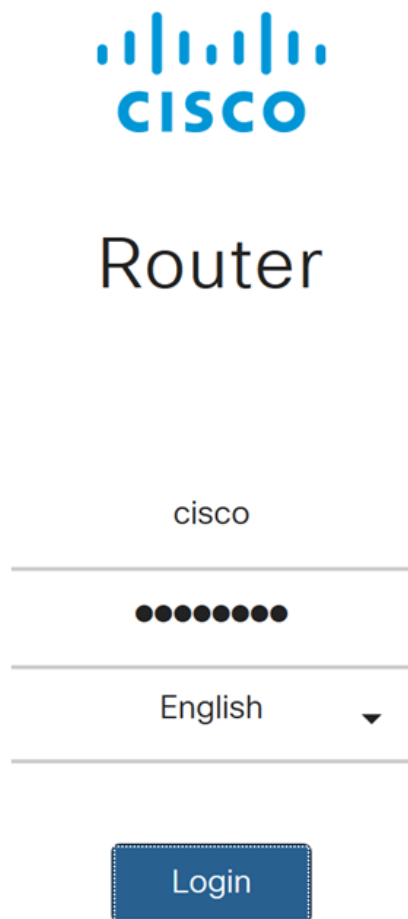
O

1. [Configurazione dei profili IPsec \(modalità di impostazione automatica della chiave\) sui modelli RV160 e RV260](#) (opzionale)
2. [Configurazione della VPN da sito a sito sugli switch RV160 e RV260](#)

Configurazione delle impostazioni avanzate della VPN da sito a sito

Le impostazioni avanzate devono essere configurate allo stesso modo su entrambi i lati della connessione VPN.

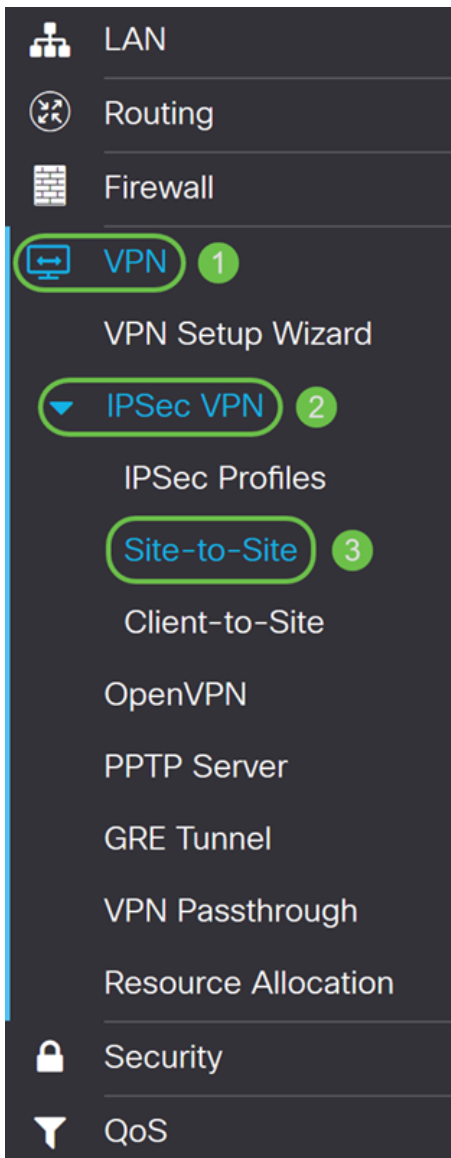
Passaggio 1. Accedere all'utility di configurazione Web.



©2018 Cisco Systems, Inc. All Rights Reserved.

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

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






Passaggio 3. Selezionare la casella di controllo della connessione che si desidera modificare. Premere quindi l'icona **penna e carta** per modificare la connessione. In questo esempio viene selezionata la connessione denominata HomeOffice.

Site-to-Site Apply Cancel

Number of Connections: 1 connected, 1 configured, maximum 10 supported.

2

+  

<input type="checkbox"/>	Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
1 <input checked="" type="checkbox"/>	HomeOffice	140. [redacted]	WAN	VPNTest	10.1.1.0/24	192.168.2.0/24	Connected	

Passaggio 4. Fare clic sulla scheda **Impostazioni avanzate**.

Add/Edit a New Connection Apply Cancel

Basic Settings **Advanced Settings** Failover

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Passaggio 5. Selezionare la casella di controllo **Comprimi (Support IP Payload Compression Protocol (IPComp))** per consentire al router di proporre la compressione quando avvia una connessione. Questo protocollo riduce le dimensioni dei datagrammi IP. Se il risponditore rifiuta questa proposta, il router non implementa la compressione. Quando il router è il risponditore, accetta la compressione, anche se non è abilitata. Se si abilita questa funzionalità per questo router, sarà necessario abilitarla sul router remoto (l'altra estremità del tunnel).

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Passaggio 6. I messaggi broadcast vengono utilizzati per la risoluzione dei nomi nelle reti Windows per identificare risorse quali computer, stampanti e file server. Questi messaggi vengono utilizzati da alcune applicazioni software e funzionalità di Windows, ad esempio Risorse di rete. Il traffico di broadcast LAN in genere non viene inoltrato su un tunnel VPN. Tuttavia, è possibile selezionare questa casella per consentire il riavvio delle trasmissioni NetBIOS da un'estremità del tunnel all'altra estremità. Selezionare la casella di controllo **Trasmissione NetBIOS** per attivare la funzione.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Passaggio 7. Selezionare la casella di controllo **Keep-Alive** per consentire al router di tentare di ristabilire la connessione VPN a intervalli regolari. Immettere il numero di secondi per l'impostazione dell'intervallo di monitoraggio keep-alive nel campo *Intervallo di monitoraggio keep-alive*. L'intervallo è compreso tra 10 e 999 secondi.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive **1**

Keep-Alive Monitoring Interval: **2** sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

Passaggio 8. Selezionare **Dead Peer Detection (DPD) Enabled** per abilitare DPD. Invia messaggi HELLO/ACK periodici per controllare lo stato del tunnel VPN. L'opzione DPD deve essere abilitata su entrambe le estremità del tunnel VPN. Specificare l'intervallo tra i messaggi HELLO/ACK nel campo Intervallo immettendo quanto segue:

- Ritardo: immettere il ritardo in secondi tra ogni messaggio Hello. L'intervallo è compreso tra 10 e 300 secondi e il valore predefinito è 10.
- Timeout di rilevamento: immettere il timeout in secondi per dichiarare che il peer è inattivo. L'intervallo è compreso tra 30 e 1800 secondi.
- Azione DPD - Azione da intraprendere dopo il timeout DPD. Selezionare **Cancella** o **Riavvia** dall'elenco a discesa.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled **1**

Delay Time: **2** sec. (Range: 10 - 300)

Detection Timeout: **3** sec. (Range: 30 - 1800)

DPD Action: **4**

Extended Authentication

User

User Name

Passaggio 9. Selezionare **Autenticazione estesa** per abilitare l'autenticazione estesa. Ciò fornirà un ulteriore livello di autenticazione che richiederà agli utenti remoti di inserire le proprie credenziali prima di ottenere l'accesso alla VPN. Per il corretto funzionamento dell'autenticazione estesa, il sito principale deve utilizzare l'autenticazione di gruppo e il sito remoto deve utilizzare l'autenticazione utente. Nei passaggi successivi verrà eseguita la configurazione del sito principale per l'utilizzo dell'autenticazione di gruppo.

Nota: È consigliabile configurare l'autenticazione da client a sito per l'autenticazione utente anziché estesa.

Se non è ancora stato creato un gruppo di utenti per il sito principale, fare clic sul collegamento per informazioni sulla creazione di un gruppo di utenti in questo articolo: [Creazione del gruppo di utenti per l'autenticazione estesa](#).

Per informazioni su come creare gli account utente, fare clic sul collegamento da reindirizzare alla sezione: [Creazione dell'account utente per l'autenticazione estesa](#).

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:



Group Name

Passaggio 10. Selezionare **Gruppo** come autenticazione estesa e premere l'icona **più** per aggiungere un nuovo gruppo. Dall'elenco a discesa scegliere il gruppo che si desidera utilizzare per l'autenticazione. Verificare che gli utenti desiderati siano inclusi nel gruppo.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

1 Group: 2 3

Passaggio 11. Nei passaggi successivi, verrà eseguita la configurazione del router remoto per l'utilizzo dell'autenticazione utente. Nel router remoto, selezionare la casella di controllo **Autenticazione estesa** per abilitare l'autenticazione estesa.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:

Passaggio 12. Selezionare **Utente** come autenticazione estesa. Immettere il **Nome utente** e la **Password** dell'utente nel gruppo selezionato nel router principale. Nell'esempio, VPNuser e CiscoTest123! è stato immesso.

Extended Authentication

1 User

User Name

2 VPNuser

Password

3

Show Password:

Enable

Group:



Group Name

Passaggio 13. Selezionare **Dividi DNS** per abilitare. In questo modo il server DNS (Domain Name System) e altre richieste DNS vengono suddivisi in un altro server DNS in base ai nomi di dominio specificati. Quando il router riceve una richiesta di risoluzione degli indirizzi, controlla il nome di dominio. Se il nome di dominio corrisponde a un nome di dominio nelle impostazioni DNS divise, passa la richiesta al server DNS specificato all'interno della rete del server VPN. In caso contrario, la richiesta viene passata al server DNS specificato nelle impostazioni dell'interfaccia WAN, ad esempio il server DNS dell'ISP.

Il DNS diviso è separato in due zone per lo stesso dominio. Uno deve essere utilizzato dalla rete interna e l'altro dalla rete esterna. Il DNS diviso indirizza gli host interni a un DNS interno per la risoluzione dei nomi e gli host esterni vengono indirizzati a un DNS esterno per la risoluzione dei nomi.

Se è stata abilitata l'opzione *Suddividi DNS*, immettere l'indirizzo IP del server DNS da utilizzare per i domini specificati. Facoltativamente, specificare un server DNS secondario nel campo *Server DNS 2*. In *Nome dominio 1-6* immettere i nomi di dominio per i server DNS. Le richieste per i domini vengono passate al server DNS specificato.

Split DNS 1

DNS Server 1:

2 192.168.1.80

DNS Server 2:

(Optional)

Domain Name 1:

3 www.cisco.com

Domain Name 2:

(Optional)

Domain Name 3:

(Optional)

Domain Name 4:

(Optional)

Domain Name 5:

(Optional)

Domain Name 6:

(Optional)

Passaggio 14. Fare clic su **Applica**.

Add/Edit a New Connection

Apply

Cancel

Group Name

Split DNS

DNS Server 1:

DNS Server 2: (Optional)

Domain Name 1:

Domain Name 2: (Optional)

Domain Name 3: (Optional)

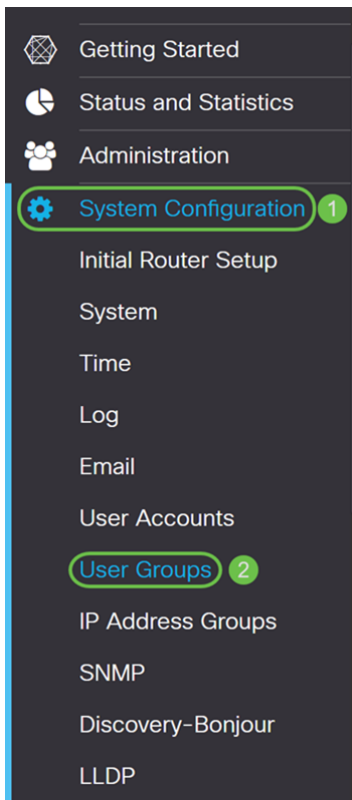
Domain Name 4: (Optional)

Domain Name 5: (Optional)

Domain Name 6: (Optional)

[Creazione del gruppo di utenti per l'autenticazione estesa](#)

Passaggio 1. Passare a **Configurazione di sistema > Gruppi di utenti**.



Passaggio 2. Fare clic sul pulsante **più** per aggiungere un nuovo gruppo di utenti.

User Groups

Apply

Cancel



<input type="checkbox"/>	Group	Web Login /NETCONF /RESTCONF	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Disable	Disable

Passaggio 3. Immettere un nome nel campo *Nome gruppo* e quindi premere **Applica**. In questo esempio è stato immesso SiteGroupTest come nome del gruppo.

User Groups

2

Apply

Cancel

Group Name:

1

Local User Membership List



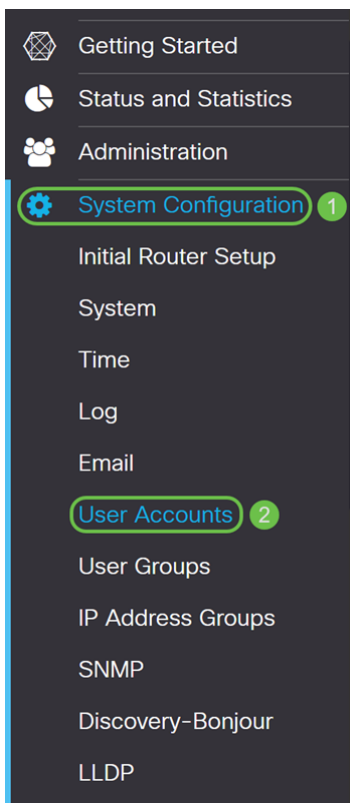
User

* Should have at least one account in the 'admin' group.

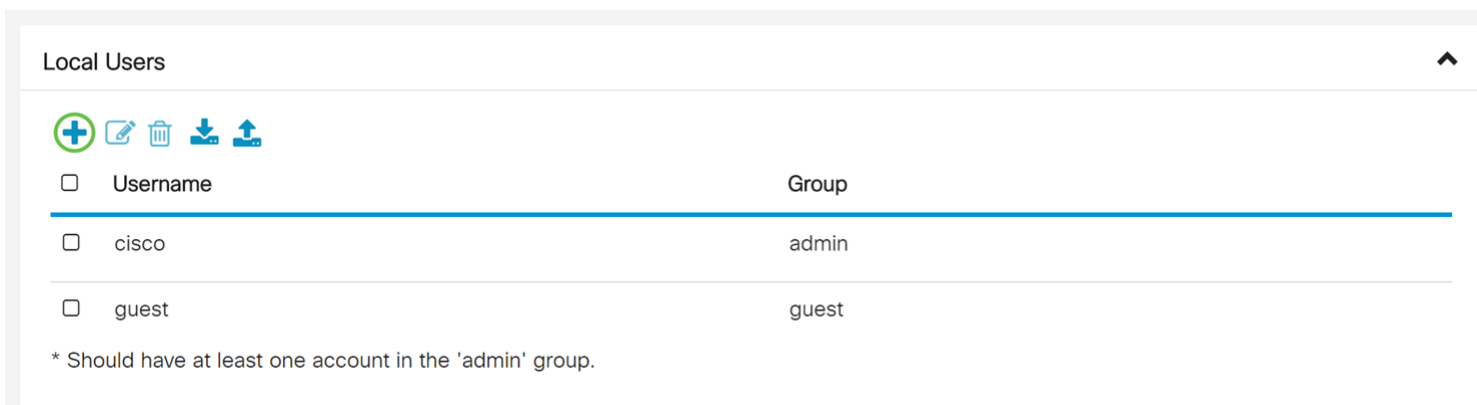
[Configurazione degli account utente per l'autenticazione estesa](#)

Nota importante: Lasciare l'account amministratore predefinito nel gruppo di amministratori e creare un nuovo account utente e un nuovo gruppo di utenti per Shrew Soft. Se si sposta l'account amministratore in un gruppo diverso, non sarà possibile accedere al router.

Passaggio 1. Passare a **Configurazione di sistema > Account utente**.




Passaggio 2. Scorrere la pagina fino a *Utenti locali*. Fare clic sul pulsante **più** per aggiungere un nuovo utente locale.



Passaggio 3. Viene visualizzata la pagina *Aggiungi account utente*. Immettere un nome utente nel campo *Nome utente*. Nell'esempio, VPNuser è stato immesso come nome utente.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter:

Group:

 ▼


Apply

Cancel

Passaggio 4. Immettere una password nei campi *Nuova password* e *Conferma password*. Nell'esempio, CiscoTest123! è stato immesso.

Nota: Questa password è stata utilizzata come esempio, tuttavia è consigliabile utilizzare una password più complessa.

Add user account


 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password: 1

Confirm Password: 2

Password Strength meter: 


Group:

Apply

Cancel

Passaggio 5. Selezionare un gruppo, quindi premere **Applica** per creare il nuovo account utente. In questo esempio è stato selezionato SiteGroupTest come gruppo.

Add user account


 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter: 

Group: 1

2

Configurazione del failover

Per attivare il failover da sito a sito, è necessario attivare la funzione keep-alive nella scheda *Impostazioni avanzate*.

Passaggio 1. Fare clic sulla scheda **Failover** per configurare il failover.

Add/Edit a New Connection

Basic Settings | Advanced Settings | **Failover**

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

Passaggio 2. Selezionare **Tunnel Backup** per abilitare. Quando il tunnel primario non è attivo, questa funzionalità consente al router di ristabilire il tunnel VPN utilizzando un indirizzo IP alternativo per il peer remoto o una WAN locale alternativa. Questa funzione è disponibile solo se DPD è attivato.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

Passaggio 3. Nel campo *Indirizzo IP backup remoto*, immettere l'indirizzo IP del peer remoto o immettere nuovamente l'indirizzo IP WAN già impostato per il gateway remoto. Selezionare quindi l'interfaccia locale (**WAN1**, **WAN2**, **USB1** o **USB2**) dall'elenco a discesa.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address) **1**

Local Interface: **2**

Passaggio 4. Fare clic su **Applica**.

The screenshot shows the 'Add/Edit a New Connection' configuration page with the 'Failover' tab selected. The 'Tunnel Backup' checkbox is checked. The 'Remote Backup IP Address' field contains '145.' followed by a redacted IP address. The 'Local Interface' dropdown menu is set to 'WAN'. There are 'Apply' and 'Cancel' buttons at the top right of the configuration area.

Conclusioni

È ora necessario configurare correttamente le impostazioni avanzate e il failover per la VPN da sito a sito sugli switch RV160 e RV260. La VPN da sito a sito deve essere ancora connessa.

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

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)