

# Controllare lo stato della VPN su RV016 RV042 RV042G e RV082 VPN Router

## Obiettivo

Una rete VPN (Virtual Private Network) è una connessione protetta tra due endpoint. La VPN crea un tunnel sicuro tra questi due endpoint e fornisce sicurezza al traffico di dati lungo il tunnel. Una VPN (Virtual Private Network) è una connessione protetta stabilita all'interno di una rete o tra reti. Per il corretto funzionamento di questo tunnel, la configurazione VPN su entrambi i lati della connessione deve essere eseguita con attenzione e alcune informazioni devono corrispondere. L'obiettivo di questo documento è spiegare come controllare lo stato della VPN su RV016, RV042, RV042G e RV082 VPN Router. Le VPN consentono di isolare il traffico tra host e reti specificati dal traffico di host e reti non autorizzati.

## Dispositivi interessati

- RV016
- RV042
- RV042G
- RV082

## Versione del software

4.2.1.02

## Parametri VPN comuni da controllare

Per il corretto funzionamento di una connessione VPN, le due estremità della connessione devono soddisfare gli stessi requisiti. In caso di errore nella connessione VPN, è possibile verificare due fattori che possono fare la differenza. (ossia SmartNIC):

- L'indirizzo IP locale è in conflitto tra i due endpoint VPN.
- Esistono differenze nelle impostazioni di crittografia e autenticazione dei due endpoint.

La sezione successiva spiegherà come controllare lo schema di indirizzi IP di una VPN e come apportare le modifiche corrette.

### Modificare l'indirizzo IP LAN del router

L'interfaccia LAN di entrambe le estremità della connessione VPN deve far parte di un indirizzo di rete diverso. Se entrambe le parti appartengono allo stesso indirizzo di rete, la connessione VPN non funzionerà. Nei passaggi seguenti viene illustrato come apportare modifiche all'indirizzo IP LAN sui router VPN RV042, RV042G e RV082.

Passaggio 1. Accedere all'utilità di configurazione basata sul Web e scegliere **Impostazione > Rete**. Viene visualizzata la pagina *Rete*:

## Network

Host Name :  (Required by some ISPs)

Domain Name :  (Required by some ISPs)

### IP Mode

Mode	WAN	LAN
<input checked="" type="radio"/> IPv4 Only	IPv4	IPv4
<input type="radio"/> Dual-Stack IP	IPv4 and IPv6	IPv4 and IPv6

IPv4

IPv6

### LAN Setting

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask :

Multiple Subnet :  Enable

### WAN Setting

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

### DMZ Setting

Enable DMZ

Passaggio 2. In Impostazioni LAN, nel campo Indirizzo IP dispositivo, immettere un indirizzo IP che appartenga a un indirizzo di rete diverso dell'altra estremità della connessione VPN.

**LAN Setting**

MAC Address : 64:9E:F3:88:C6:A4

Device IP Address :

Subnet Mask :  ▼

Multiple Subnet :

---

**WAN Setting**

Interface	Connection Type	Configuration
WAN1	Obtain an IP automatically	
WAN2	Obtain an IP automatically	

Passaggio 3. Nell'elenco a discesa Subnet mask scegliere la subnet mask appropriata per la connessione VPN.

Passaggio 4. (Facoltativo) Per abilitare l'utilizzo di più subnet, nel campo Subnet multipla selezionare la casella di controllo Abilita.

Passaggio 5. Fare clic su **Salva** per applicare le nuove impostazioni.

## Controllare i parametri di sicurezza della connessione VPN

La configurazione di protezione della connessione VPN deve essere la stessa su entrambe le estremità della connessione. Nella procedura seguente viene illustrato come controllare questi parametri sui router VPN RV042, RV042G e RV082.

Passaggio 1. Accedere all'utility di configurazione basata sul Web e scegliere **VPN > Gateway to Gateway**. Viene visualizzata la pagina *Gateway to Gateway*.

## Gateway To Gateway

### Add a New Tunnel

Tunnel No. 1

Tunnel Name : TestTunnel

Interface : WAN1

Enable :

### Local Group Setup

Local Security Gateway Type : IP Only

IP Address : 156.26.31.119

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

### Remote Group Setup

Remote Security Gateway Type : IP Only

IP Address : 192.0.2.2

Remote Security Group Type : Subnet

IP Address : 192.168.2.0

Subnet Mask : 255.255.255.0

### IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key : VPNkey

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Save

Cancel

Passaggio 2. Controllare i seguenti parametri. Accertarsi che entrambe le estremità della connessione VPN abbiano le stesse impostazioni:

- Il tipo di gruppo di sicurezza locale è lo stesso segmento LAN del router locale.
- Il tipo di gruppo di sicurezza remoto è lo stesso segmento LAN del router remoto.
- Tipo di gateway di sicurezza remoto è l'indirizzo IP WAN/Internet del router remoto.
- I campi di configurazione IPSec devono corrispondere su entrambi i lati del tunnel VPN.
- La chiave precondivisa deve essere la stessa su entrambi i lati del tunnel VPN.

Passaggio 3. (Facoltativo) Fare clic su **Avanzate+** per ulteriori proprietà di sicurezza. Come in precedenza, queste impostazioni devono essere le stesse su entrambi i lati della connessione.

Passaggio 4. Fare clic su **Save** (Salva) per applicare le nuove impostazioni se sono state apportate modifiche.

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).