

Configurazione guidata VPN Setup su RV160 e RV260

Obiettivo

In questo documento viene spiegato come configurare la Configurazione guidata VPN su RV160 e RV260.

Introduzione

La tecnologia si è evoluta e le attività aziendali vengono spesso condotte all'esterno dell'ufficio. I dispositivi sono più mobili e i dipendenti spesso lavorano da casa o in viaggio. Ciò può causare alcune vulnerabilità della sicurezza. 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.

Una VPN stabilisce una connessione crittografata su una rete meno sicura come Internet. Assicura il livello di sicurezza appropriato per i sistemi collegati. Un tunnel è definito come una rete privata in grado di inviare i dati in modo sicuro utilizzando tecniche di crittografia e autenticazione standard per proteggere i dati inviati. Per proteggere la connessione, una VPN ad accesso remoto si basa in genere su IPsec (Internet Protocol Security) o SSL (Secure Sockets Layer).

Le VPN forniscono accesso di livello 2 alla rete di destinazione; che richiedono l'esecuzione di un protocollo di tunneling, ad esempio PPTP (Point-to-Point Tunneling Protocol) o L2TP (Layer 2 Tunneling Protocol), sulla connessione IPsec di base. La VPN IPsec supporta la VPN da sito a sito per un tunnel gateway-to-gateway. Ad esempio, un utente può configurare il tunnel VPN di una succursale per connettersi al router della sede aziendale, in modo che quest'ultima possa accedere in modo sicuro alla rete aziendale. La VPN IPsec supporta anche la VPN da client a server per il tunnel da host a gateway. La VPN da client a server è utile per la connessione da laptop/PC da casa a una rete aziendale tramite server VPN.

La serie RV160 supporta 10 tunnel e la serie RV260 20 tunnel. L'Installazione guidata VPN assiste l'utente durante la configurazione di una connessione protetta per un tunnel IPsec da sito a sito. Ciò semplifica la configurazione evitando parametri complessi e facoltativi, in modo che qualsiasi utente possa configurare il tunnel IPsec in modo rapido ed efficiente.

Dispositivi interessati

- RV160
- RV260

Versione del software

- 1.0.0.13

Configurazione guidata VPN su router locale

Passaggio 1. Accedere alla pagina di configurazione Web sul router locale.

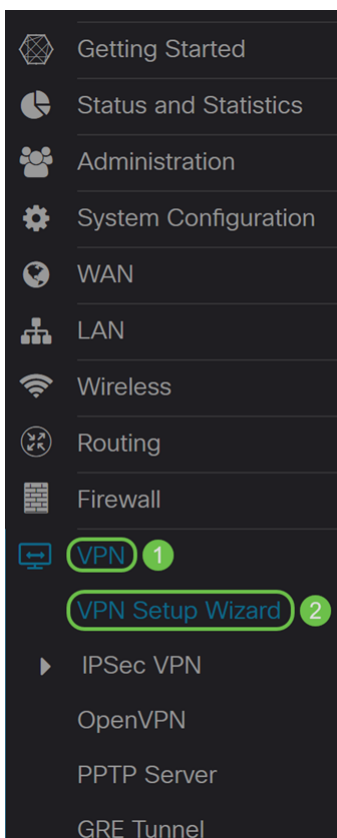
Nota: Il router locale verrà indicato come router A e il router remoto come router B. In questo documento, utilizzeremo due RV160 per illustrare la Configurazione guidata VPN.



©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 > Impostazione guidata VPN.



Passaggio 3. Nella sezione *Riquadro attività iniziale*, immettere un nome di connessione nel

campo **Immettere un nome di connessione**. Abbiamo inserito **HomeOffice** come nome della connessione.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name: 

4. Profile

Interface: WAN

5. Summary

[Next](#)

[Cancel](#)

Passaggio 4. Nel campo *Interface* (Interfaccia), selezionare un'interfaccia dall'elenco a discesa se si utilizza un RV260. L'RV160 dispone solo di un collegamento WAN, quindi non sarà possibile selezionare un'interfaccia dall'elenco a discesa. Fare clic su **Avanti** per passare alla sezione *Impostazioni router remoto*.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name:  HomeOffice

4. Profile

Interface: WAN

5. Summary

Next

Cancel

Passaggio 5. Selezionare un *tipo di connessione remota* dall'elenco a discesa. Selezionare **Static IP** o **FQDN** (Fully Qualified Domain Name), quindi immettere l'indirizzo IP WAN o il FQDN del gateway che si desidera connettere nel campo *Remote Address* (Indirizzo remoto). Nell'esempio, è stato selezionato **Static IP** (IP statico) ed è stato immesso l'indirizzo IP WAN del router remoto (router B). Fare quindi clic su **Avanti** per passare alla sezione successiva.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Remote Connection Type :

Static IP

1

2. Remote Router Settings

Remote Address : ?

145.

2

3. Local and Remote Networks

4. Profile

5. Summary

3

Back

Next

Cancel

Passaggio 6. Nella sezione *Rete locale e remota*, in *Selezione traffico locale*, selezionare l'indirizzo IP locale (**Subnet**, **Single** o **Any**) dall'elenco a discesa. Se si seleziona **Subnet**, immettere l'indirizzo IP della subnet e la subnet mask. Se si seleziona **Singolo**, immettere un indirizzo IP. Se è stato selezionato **Any** (Qualsiasi), andare al passaggio successivo per configurare *Remote Traffic Selection*.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

Subnet Mask:

Back

Next

Cancel

Passaggio 7. In *Remote Traffic Selection*, selezionare *Remote IP* (Subnet, **Single**, o **Any**) dall'elenco a discesa. Se si seleziona **Subnet**, immettere l'indirizzo IP della subnet e la subnet mask del router remoto (router B). Se si seleziona **Singolo**, immettere l'indirizzo IP. Quindi fare clic su **Avanti** per configurare la sezione *Profilo*.

Nota: Se è stato selezionato Qualsiasi per *Selezione traffico locale*, è necessario selezionare **Subnet** o **Single** per la *Selezione traffico remoto*.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

1

IP Address:

10.1.1.0

2

Subnet Mask:

255.255.255.0

3

4

Back

Next

Cancel

Passaggio 8. Nella sezione *Profilo*, selezionare un nome per il profilo IPSec dall'elenco a discesa. Per questa dimostrazione, è stato selezionato **nuovo profilo** come profilo IPSec.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: new-profile

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back

Next

Cancel

Passaggio 9. Scegliere **IKEv1** (Internet Key Exchange versione 1) o **IKEv2** (Internet Key Exchange versione 2) come *versione IKE*. IKE è un protocollo ibrido che implementa lo scambio di chiavi Oakley e Skeme all'interno della struttura ISAKMP (Internet Security Association and Key Management Protocol). IKE fornisce l'autenticazione dei peer IPsec, negozia le chiavi IPsec e le associazioni di protezione IPsec. IKEv2 è più efficiente perché richiede meno pacchetti per lo scambio di chiavi e supporta più opzioni di autenticazione, mentre IKEv1 esegue solo l'autenticazione basata su chiave condivisa e certificati. Nell'esempio, **IKEv1** è stato selezionato come versione IKE.

Nota: Se il dispositivo supporta IKEv2, è consigliabile utilizzare IKEv2. Se il dispositivo non supporta IKEv2, utilizzare IKEv1. Entrambi i router (locale e remoto) devono utilizzare la stessa versione di IKE e le stesse impostazioni di protezione.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Passaggio 10. Nella sezione *Opzioni fase 1*, selezionare un gruppo DH (Diffie-Hellman) (**gruppo 2 - 1024 bit** o **gruppo 5 - 1536 bit**) dall'elenco a discesa. DH è un protocollo di scambio delle chiavi, con due gruppi di diverse lunghezze di chiavi primarie: Il gruppo 2 può contenere fino a 1.024 bit e il gruppo 5 fino a 1.536 bit. Per questa dimostrazione verrà utilizzato il **gruppo 2 - 1024 bit**.

Nota: Per velocizzare le operazioni e ridurre la protezione, scegliere Gruppo 2. Per velocità più lente e maggiore protezione, scegliere Gruppo 5. Gruppo 2 è selezionato per impostazione predefinita.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Passaggio 11. Selezionare un'opzione di crittografia (**3DES, AES-128, AES-192 o AES-256**) dall'elenco a discesa. Questo metodo determina l'algoritmo utilizzato per crittografare o decrittografare i pacchetti Encapsulating Security Payload (ESP)/Internet Security Association and Key Management Protocol (ISAKMP). Triple Data Encryption Standard (3DES) utilizza la crittografia DES tre volte, ma è ora un algoritmo legacy. Ciò significa che dovrebbe essere utilizzato solo quando non ci sono alternative migliori, in quanto fornisce ancora un livello di sicurezza marginale ma accettabile. Gli utenti dovrebbero utilizzarlo solo se necessario per la compatibilità con le versioni precedenti, in quanto è vulnerabile ad attacchi di tipo "collisione di blocco". Advanced Encryption Standard (AES) è un algoritmo di crittografia progettato per essere più sicuro di DES. AES utilizza una chiave di dimensioni maggiori che garantisce che l'unico approccio noto per decrittografare un messaggio sia che un intruso possa provare tutte le chiavi possibili. Si consiglia di utilizzare AES anziché 3DES. Nell'esempio, utilizzeremo **AES-192** come opzione di crittografia.

Nota: Di seguito sono riportate alcune risorse aggiuntive che possono essere utili:
[Configurazione della sicurezza per le VPN con IPsec](#) e [crittografia di nuova generazione](#).

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Passaggio 12. Il metodo di autenticazione determina la modalità di convalida dei pacchetti di intestazione Encapsulating Security Payload Protocol (ESP). MD5 è un algoritmo di hash unidirezionale che produce un digest a 128 bit. SHA1 è un algoritmo di hash unidirezionale che produce un digest a 160 bit, mentre SHA2-256 produce un digest a 256 bit. SHA2-256 è consigliato perché più sicuro. Verificare che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione. Selezionare un'autenticazione (**MD5, SHA1 o SHA2-256**). Per questo esempio è stato selezionato **SHA2-256**.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile:

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group:

Encryption:

Authentication:

SA Lifetime (sec.): ?

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Passaggio 13. La *durata dell'associazione di protezione (sec)* indica la quantità di tempo in secondi durante la quale un'associazione di protezione IKE è attiva. Una nuova associazione di sicurezza (SA) viene negoziata prima della scadenza della durata per garantire che una nuova SA sia pronta per essere utilizzata alla scadenza della precedente. Il valore predefinito è 28800 e l'intervallo è compreso tra 120 e 86400. Verrà utilizzato il valore predefinito di **28800** secondi come durata SA per la fase I.

Nota: Si consiglia che la durata dell'ASA nella Fase I sia maggiore della durata dell'ASA nella Fase II. Se si rende la Fase I più breve della Fase II, sarà necessario rinegoziare il tunnel frequentemente in senso inverso rispetto al tunnel di dati. Il tunnel dei dati è ciò che richiede maggiore sicurezza, quindi è meglio avere una durata di vita inferiore nella Fase II rispetto alla Fase I.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.):

Pre-shared Key:

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Passaggio 14. Immettere la **chiave già condivisa** da utilizzare per autenticare il peer IKE remoto. È possibile immettere fino a 30 caratteri della tastiera o valori esadecimali, ad esempio My_@123 o 4d795f40313233. Entrambe le estremità del tunnel VPN devono utilizzare la stessa chiave precondivisa.

Nota: È consigliabile modificare periodicamente la chiave precondivisa per ottimizzare la sicurezza della VPN.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile: new-profile

IKE Version: IKEv1 IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 28800

Pre-shared Key: ●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Back Next Cancel

Passaggio 15. Nella sezione *Opzioni fase II*, selezionare un protocollo dall'elenco a discesa.

- **ESP** - Selezionare ESP per la crittografia dei dati e immettere la crittografia.
- **AH** - Selezionare questa opzione per garantire l'integrità dei dati quando i dati non sono segreti ma devono essere autenticati.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Passaggio 16. Selezionare un'opzione di crittografia (**3DES, AES-128, AES-192 o AES-256**) dall'elenco a discesa. Questo metodo determina l'algoritmo utilizzato per crittografare o decrittografare i pacchetti Encapsulating Security Payload (ESP)/Internet Security Association and Key Management Protocol (ISAKMP). Triple Data Encryption Standard (3DES) utilizza la crittografia DES tre volte, ma è ora un algoritmo legacy. Ciò significa che dovrebbe essere utilizzato solo quando non ci sono alternative migliori, in quanto fornisce ancora un livello di sicurezza marginale ma accettabile. Gli utenti dovrebbero utilizzarlo solo se necessario per la compatibilità con le versioni precedenti, in quanto è vulnerabile ad attacchi di tipo "collisione di blocco". Advanced Encryption Standard (AES) è un algoritmo di crittografia progettato per essere più sicuro di DES. AES utilizza una chiave di dimensioni maggiori che garantisce che l'unico approccio noto per decrittografare un messaggio sia che un intruso possa provare tutte le chiavi possibili. Si consiglia di utilizzare AES anziché 3DES. Nell'esempio, utilizzeremo **AES-192** come opzione di crittografia.

Nota: Di seguito sono riportate alcune risorse aggiuntive che possono essere utili:
[Configurazione della sicurezza per le VPN con IPsec](#) e [crittografia di nuova generazione](#).

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Passaggio 17. Il metodo di autenticazione determina la modalità di convalida dei pacchetti di intestazione Encapsulating Security Payload Protocol (ESP). MD5 è un algoritmo di hash unidirezionale che produce un digest a 128 bit. SHA1 è un algoritmo di hash unidirezionale che produce un digest a 160 bit, mentre SHA2-256 produce un digest a 256 bit. SHA2-256 è consigliato perché più sicuro. Verificare che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione. Selezionare un'autenticazione (MD5, SHA1 o SHA2-256). Per questo esempio è stato selezionato **SHA2-256**.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.):

3600

Pre-shared Key:

●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.):

3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back

Next

Cancel

Passaggio 18. Immettere il valore per *Durata SA (sec)*, che indica il periodo di tempo, in secondi, durante il quale un tunnel VPN (SA IPsec) è attivo. Il valore predefinito per la Fase 2 è 3600 secondi.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.): 2000

Pre-shared Key: ●●●●●●

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): ? 3600

Perfect Forward Secrecy: Enable

Save as a new profile

Back Next Cancel

Passaggio 19. Quando PFS (Perfect Forward Secrecy) è abilitato, la negoziazione IKE fase 2 genera nuovo materiale della chiave per la crittografia e l'autenticazione del traffico IPsec. Perfect Forward Secrecy viene utilizzato per migliorare la sicurezza delle comunicazioni trasmesse attraverso Internet utilizzando la crittografia a chiave pubblica. Selezionare o deselezionare la casella per attivare questa funzione. Questa funzione è consigliata. Se selezionata, selezionare un *gruppo DH*. Nell'esempio viene usato **Group2 - 1024 bit**.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

Show Pre-shared Key:


 Enable

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime (sec.): 

Perfect Forward Secrecy: Enable 1

DH Group: 2

Save as a new profile

Back

Next

Cancel

Passaggio 20. In *Salva come nuovo profilo*, immettere un nome per il nuovo profilo appena creato. Fare clic su **Avanti** per visualizzare il riepilogo della configurazione VPN.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

••••••

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.): ?

3600

Perfect Forward Secrecy: Enable

DH Group:

Group2 - 1024 bit

Save as a new profile 1

HomeOffice

Back

2
Next

Cancel

Passaggio 21. Verificare le informazioni e fare clic su **Invia**.

VPN Setup Wizard (Site-to-Site)

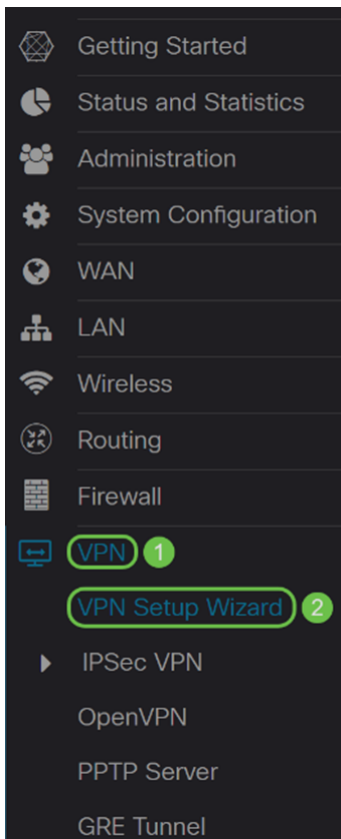
✓ 1. Getting Started	(sec.):	-----	
✓ 2. Remote Router Settings	Pre-shared Key:	Test123	
✓ 3. Local and Remote Networks	Phase II Options		Remote Group
✓ 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
5. Summary	Encryption:	AES-192	IP Address: 10.1.1.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

Back Submit Cancel

Configurazione guidata VPN su router remoto

Sul router remoto, è necessario configurare le stesse impostazioni di sicurezza del router locale, ma utilizzare l'indirizzo IP del router locale come traffico remoto.

Passaggio 1. Accedere alla pagina di configurazione Web sul router remoto (Router B) e selezionare **VPN > VPN Setup Wizard** (Configurazione guidata VPN).



Passaggio 2. Immettere un nome di connessione e scegliere l'interfaccia che verrà utilizzata per la VPN se si utilizza un RV260. L'RV160 dispone solo di un collegamento WAN, quindi non sarà possibile selezionare un'interfaccia dall'elenco a discesa. Quindi fare clic su **Next** (Avanti) per continuare.

VPN Setup Wizard (Site-to-Site)

1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPSec VPN tunnel.

2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

3. Local and Remote Networks

Enter a connection name:

4. Profile

Interface: WAN

5. Summary

Passaggio 3. In *Impostazioni router remoto*, selezionare il *Tipo di connessione remota*,

quindi immettere l'indirizzo IP WAN del router A. Quindi fare clic su **Next** (Avanti) per passare alla sezione successiva.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Remote Connection Type :

Static IP

1

2. Remote Router Settings

Remote Address : ?

140.

2

3. Local and Remote Networks

4. Profile

5. Summary

3

Back

Next

Cancel

Passaggio 4. Selezionare il traffico locale e remoto. Se è stata selezionata l'opzione **Subnet** nel campo *Selezione traffico remoto*, immettere nella subnet dell'indirizzo IP privato del router A. Quindi fare clic su **Avanti** per configurare la sezione *Profilo*.

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

Local Traffic Selection:

Any

1

✓ 2. Remote Router Settings

Remote Traffic Selection:

Subnet

2

3. Local and Remote Networks

IP Address:

192.168.2.0

3

Subnet Mask:

255.255.255.0

4

4. Profile

5. Summary

5

Back

Next

Cancel

Passaggio 5. Nella sezione *Profile*, selezionare le stesse impostazioni di sicurezza del router A. È stata inoltre immessa la stessa chiave già condivisa del router A. Quindi fare clic su **Avanti** per andare alla pagina *Riepilogo*.

Opzioni fase I:

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

IPSec Profile:

1 new-profile

IKE Version:

2 IKEv1 IKEv2

Phase I Options

DH Group:

3 Group2 - 1024 bit

Encryption:

4 AES-192

Authentication:

5 SHA2-256

SA Lifetime (sec.):

? 6 28800

Pre-shared Key:

7 ●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Back

Next

Cancel

Opzioni fase II:

VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared key:

Show Pre-shared Key: Enable

Phase II Options

Protocol Selection: 1

Encryption: 2

Authentication: 3

SA Lifetime (sec.): ? 4

Perfect Forward Secrecy: Enable 5

DH Group: 6

Save as a new profile 7

8

Back

Next

Cancel

Passaggio 6. Nella pagina *Riepilogo* verificare che le informazioni appena configurate siano corrette. Quindi fare clic su **Submit** (Invia) per creare la VPN da sito a sito.

VPN Setup Wizard (Site-to-Site)

1. Getting Started (sec.): -----

2. Remote Router Settings
Pre-shared Key: Test123

3. Local and Remote Networks
Phase II Options
Protocol Selection: ESP
Encryption: AES-192
Authentication: SHA2-256
SA Lifetime (sec.): 3600
Perfect Forward Secrecy: Enable
DH Group: Group2 - 1024 bit

Remote Group
Remote IP Type: Subnet
IP Address: 192.168.2.0
Subnet: 255.255.255.0

4. Profile

5. Summary

Back Submit Cancel

Nota: Tutte le configurazioni attualmente utilizzate dal router si trovano nel file della configurazione in esecuzione, che è volatile e non viene conservato tra un riavvio e l'altro. Per mantenere la configurazione tra un riavvio e l'altro, accertarsi di copiare il file della configurazione di esecuzione nel file della configurazione di avvio dopo aver completato tutte le modifiche. A tale scopo, fare clic sul pulsante **Salva** nella parte superiore della pagina oppure selezionare **Amministrazione > Gestione configurazione**. Verificare quindi che l'*origine* stia **eseguendo la configurazione** e che la *destinazione* sia la **configurazione di avvio**. Fare clic su **Apply** (Applica).

Conclusioni

È necessario aver configurato correttamente una VPN da sito a sito utilizzando la Configurazione guidata VPN. Per verificare che la VPN da sito a sito sia connessa, eseguire la procedura seguente.

Passaggio 1. Per verificare che la connessione sia stata stabilita, è necessario visualizzare lo stato *Connesso* quando si passa a **VPN > IPSec VPN > Da sito a sito**.

Site-to-Site Apply Cancel

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

Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
<input type="checkbox"/> RemoteOffice	140.140.140.140	WAN	VPNTTest	0.0.0.0/0	192.168.2.0/24	Connected	

Passaggio 2. Passare a **Stato e statistiche > Stato VPN** e verificare che il tunnel da sito a

sito sia *abilitato e attivo*.

VPN Status

Site-to-Site Tunnel Status

1 Tunnel(s) Used 9 Tunnel(s) Available
1 Tunnel(s) Enabled 1 Tunnel(s) Defined

Connection Table



Column Display Selection

<input type="checkbox"/>	No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
<input type="checkbox"/>	1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140. [redacted]	