

Configurazione e utilizzo del client VPN IPsec GreenBow per la connessione con i router RV160 e RV260

Obiettivo

L'obiettivo di questo documento è configurare e usare il client VPN IPsec GreenBow per il collegamento ai router RV160 e RV260.

Introduzione

Una connessione VPN (Virtual Private Network) consente agli utenti di accedere, inviare e ricevere dati da e verso una rete privata tramite una rete pubblica o condivisa, ad esempio Internet, ma garantisce comunque una connessione sicura a un'infrastruttura di rete sottostante per proteggere la rete privata e le relative risorse.

Un tunnel VPN stabilisce una rete privata in grado di inviare i dati in modo sicuro utilizzando la crittografia e l'autenticazione. Le filiali utilizzano spesso una connessione VPN, in quanto è utile e necessario per consentire ai dipendenti di accedere alla rete privata anche quando si trovano all'esterno dell'ufficio.

La VPN consente a un host remoto, o client, di agire come se si trovasse sulla stessa rete locale. Il router RV160 supporta fino a 10 tunnel VPN e il router RV260 ne supporta fino a 20. È possibile configurare una connessione VPN tra il router e un endpoint dopo aver configurato il router per la connessione Internet. Il client VPN dipende interamente dalle impostazioni del router VPN per poter stabilire una connessione. Le impostazioni devono corrispondere esattamente o non possono comunicare.

Il client VPN GreenBow è un'applicazione client VPN di terze parti che consente a un dispositivo host di configurare una connessione sicura per il tunnel IPsec da client a sito con i router serie RV160 e RV260.

Vantaggi dell'utilizzo di una connessione VPN

L'utilizzo di una connessione VPN consente di proteggere i dati e le risorse di rete riservati.

Offre convenienza e accessibilità per i dipendenti remoti o aziendali, in quanto possono accedere facilmente all'ufficio principale senza dover essere fisicamente presenti e mantenere la sicurezza della rete privata e delle sue risorse.

La comunicazione tramite una connessione VPN offre un livello di protezione più elevato rispetto ad altri metodi di comunicazione remota. Un algoritmo di crittografia avanzato rende possibile questa operazione, proteggendo la rete privata da accessi non autorizzati.

Le posizioni geografiche effettive degli utenti sono protette e non esposte al pubblico o a reti condivise come Internet.

Una VPN consente di aggiungere nuovi utenti o un gruppo di utenti senza la necessità di componenti aggiuntivi o una configurazione complessa.

Rischi dell'utilizzo di una connessione VPN

Potrebbero esistere rischi per la sicurezza dovuti a una configurazione errata. Poiché la progettazione e l'implementazione di una VPN può essere complicata, è necessario affidare il compito di configurare la connessione a un professionista altamente qualificato ed esperto per assicurarsi che la sicurezza della rete privata non venga compromessa.

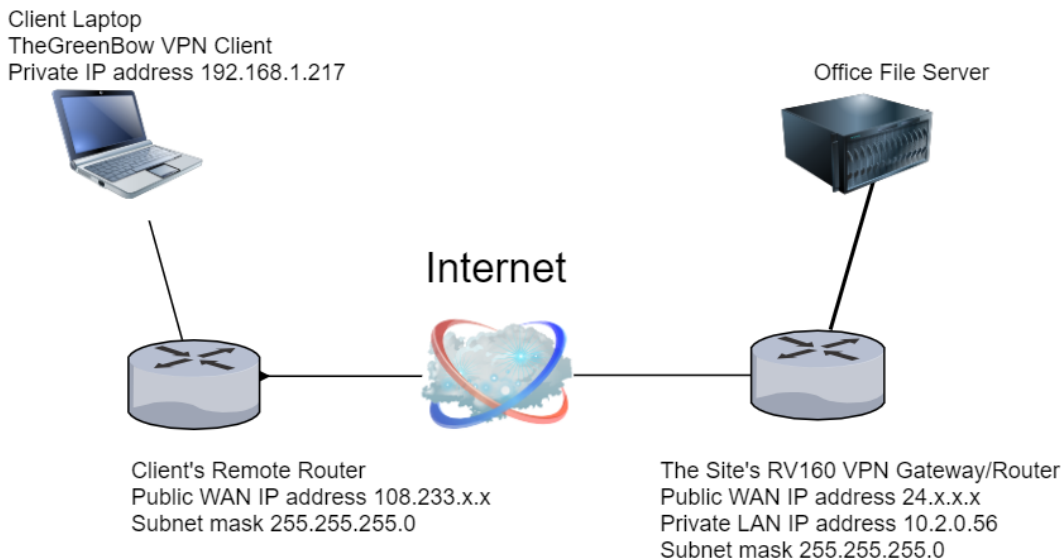
Può essere meno affidabile. Poiché una connessione VPN richiede una connessione a Internet, è importante disporre di un provider con una reputazione collaudata e testata per fornire un servizio Internet eccellente e garantire tempi di inattività minimi o nulli.

Se si verifica una situazione in cui è necessario aggiungere una nuova infrastruttura o una nuova serie di configurazioni, possono verificarsi problemi tecnici dovuti all'incompatibilità, in particolare se si tratta di prodotti o fornitori diversi da quelli già in uso.

Si possono verificare velocità di connessione lente. Se si utilizza un client VPN che offre un servizio VPN gratuito, è probabile che anche la connessione risulti lenta poiché questi provider non assegnano la priorità alle velocità di connessione. In questo articolo, utilizzeremo una terza parte a pagamento che dovrebbe eliminare il problema.

Topologia di base della rete da client a sito

Si tratta del layout di base della rete per la configurazione. Gli indirizzi IP della rete WAN pubblica sono parzialmente offuscati o stanno mostrando una x al posto dei numeri effettivi per proteggere la rete dagli attacchi.



In questo documento vengono illustrati i passaggi necessari per configurare il router RV160 o RV260 sul sito per:

- Un gruppo di utenti — **VPNUsers**
- Account utente (uno o più utenti) a cui sarà consentito l'accesso come client
- Profilo IPsec - **TheGreenBow**
- Profilo da client a sito - **Client**
- Verrà inoltre illustrato come visualizzare lo stato della VPN sul sito una volta connesso il client

Nota: È possibile utilizzare qualsiasi nome per il gruppo di utenti, il profilo IPsec e il profilo da client a sito. I nomi elencati sono solo esempi.

Questo articolo spiega anche la procedura che ogni client deve seguire per configurare la VPN di TheGreenBow sul proprio computer:

- Scarica e configura il software client VPN GreenBow
- Configurare le impostazioni delle fasi 1 e 2 per il client
- Avvia e verifica una connessione VPN come client

È essenziale che tutte le impostazioni del router sul sito corrispondano alle impostazioni del client. Se la configurazione non consente di stabilire una connessione VPN, controllare tutte le impostazioni per verificare che corrispondano. L'esempio illustrato in questo articolo è solo un modo per impostare la connessione.

Sommario

Configurazione sul router RV160 o RV260 sul sito

[Crea un gruppo di utenti](#)

[Crea un account utente](#)

[Configura profilo IPsec](#)

[Configurazione delle impostazioni di Fase 1 e Fase 2](#)

[Creazione di un profilo da client a sito](#)

Configurazione nella posizione client

[Configurazione delle impostazioni della fase 1](#)

[Configura impostazioni tunnel](#)

[Avvia una connessione VPN come client](#)

Controllare la connettività su RV160 o RV260

[Verifica dello stato della VPN sul sito](#)

Dispositivi interessati

- RV160
- RV260

Versione del software

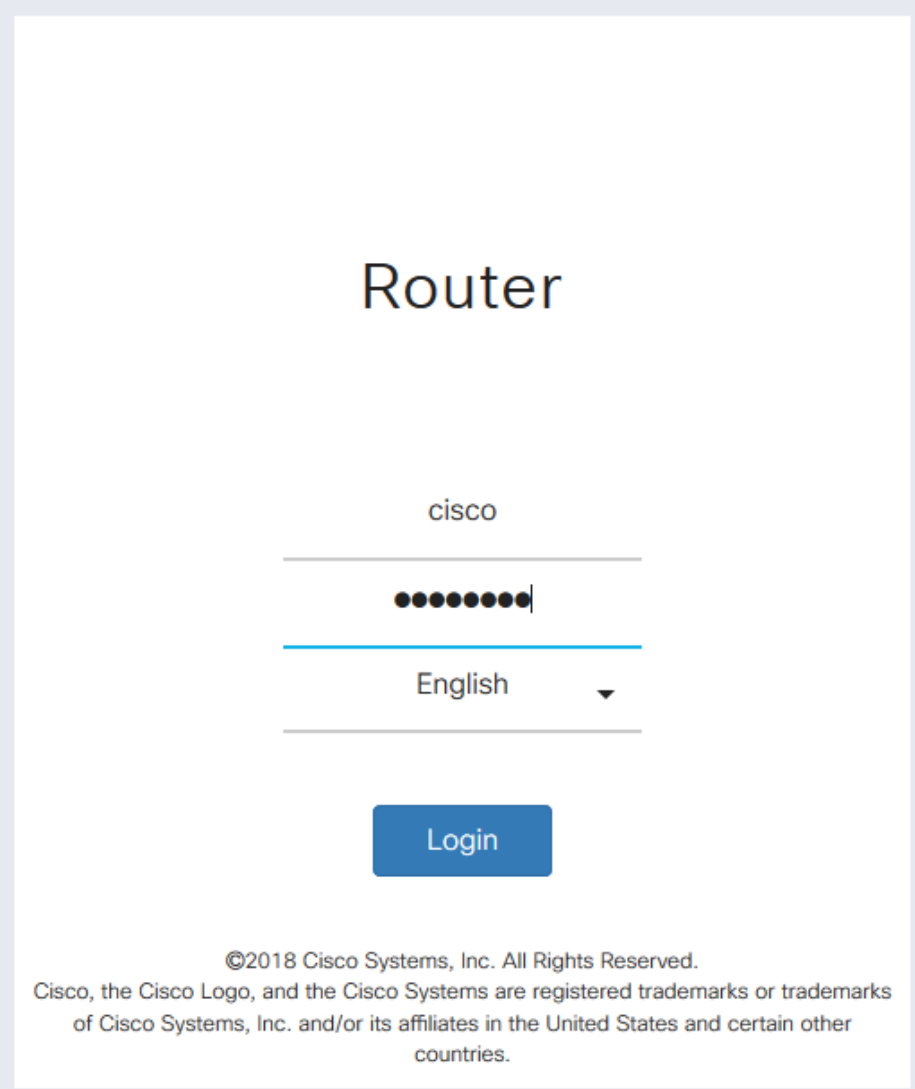
- 1.0.00.15

Configurazione del client VPN sul sito sul router RV160 o RV260

Crea un gruppo di utenti

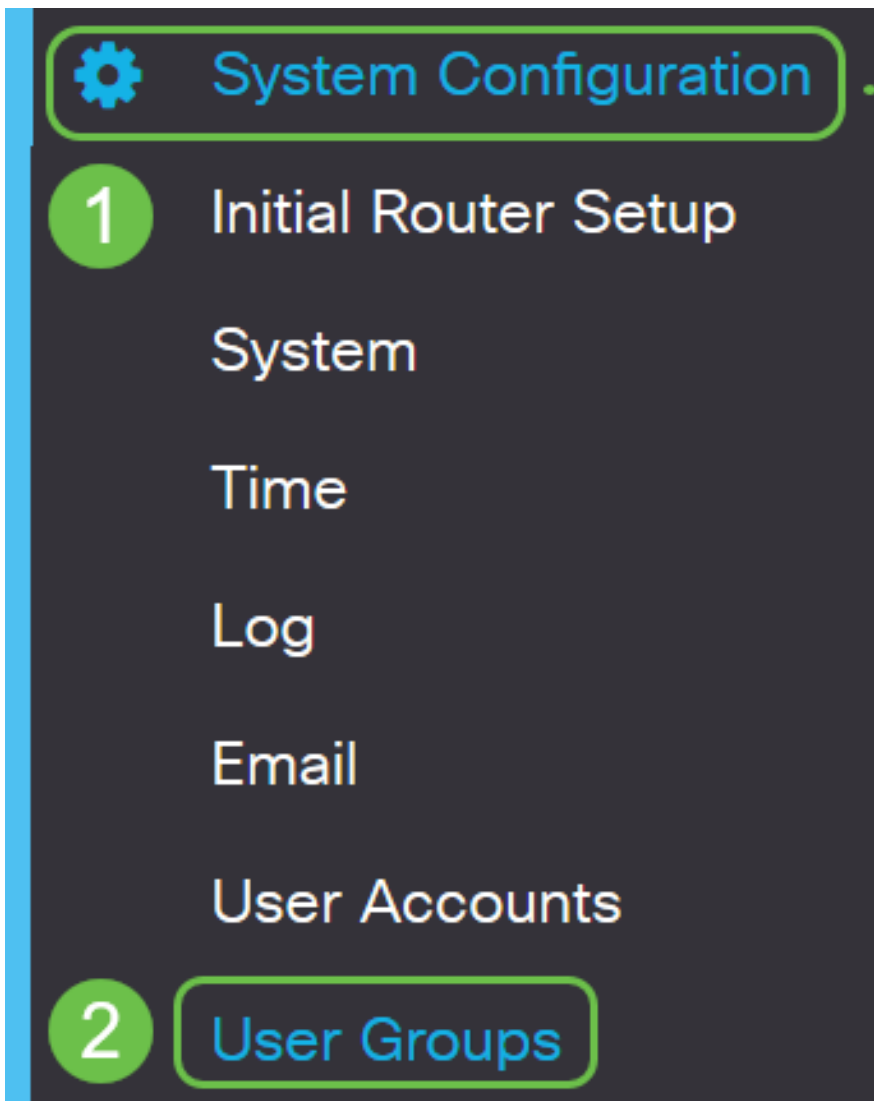
Nota importante: Lasciare l'account amministratore predefinito nel gruppo di amministratori e creare un nuovo account utente e un nuovo gruppo di utenti per TheGreenBow. Se si sposta l'account amministratore in un gruppo diverso, non sarà possibile accedere al router.

Passaggio 1. Accedere all'utility basata sul Web del router.

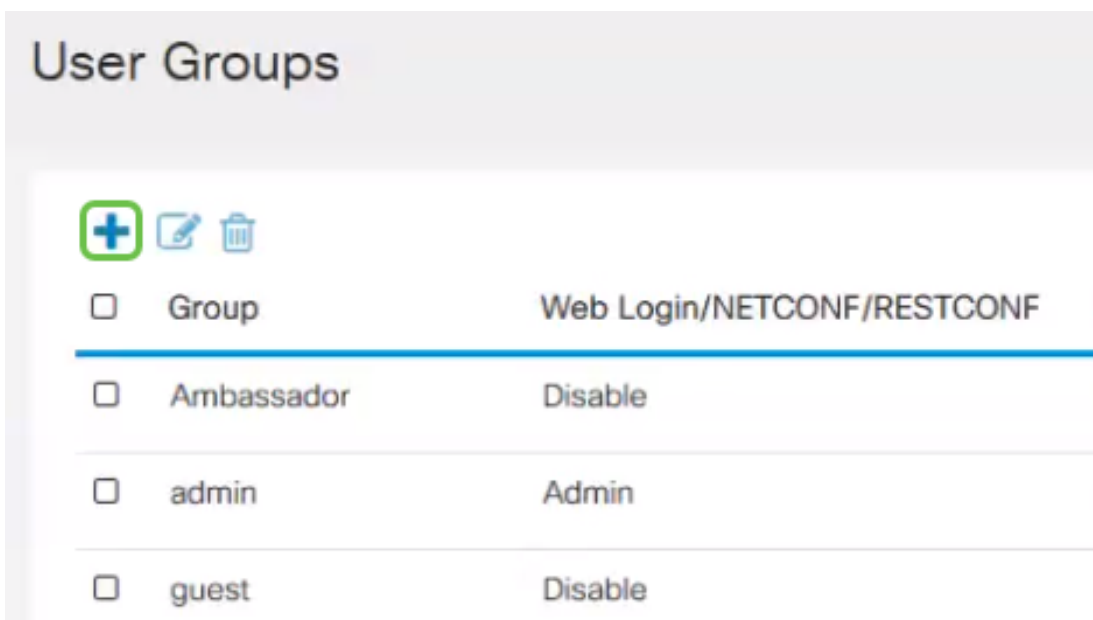


The image shows the login page of a Cisco Router. At the top, the word "Router" is displayed in a large, black, sans-serif font. Below this, the word "cisco" is centered. A horizontal line separates the text from a password field, which contains ten black dots and a vertical cursor. Another horizontal line is below the password field. Below that, the word "English" is centered, followed by a small downward-pointing triangle indicating a dropdown menu. A third horizontal line is below the language selection. At the bottom of the form area is a blue rectangular button with the word "Login" in white text. At the very bottom of the page, there is a copyright notice: "©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. Selezionare **Configurazione di sistema > Gruppi di utenti**.



Passaggio 3. Fare clic sull'icona **più** per aggiungere un gruppo di utenti.



Passaggio 4. Nell'area Panoramica, inserire il nome del gruppo nel campo *Nome gruppo*.

User Groups

Group Name:

VPNUsers



Local User Membership List






Passaggio 5. In *Elenco appartenenza utenti locali*, fare clic sul pulsante **più** e selezionare l'utente dall'elenco a discesa. Per aggiungere altri membri, premere di nuovo l'icona **più** e selezionare un altro membro da aggiungere. I membri possono far parte di un solo gruppo. Se non si dispone già di tutti gli utenti immessi, è possibile aggiungerne altri nella sezione [Creazione di un account utente](#).

Local User Membership List

1

<input type="checkbox"/>	#	User
<input type="checkbox"/>	1	John 
<input type="checkbox"/>	2	Kevin 
<input type="checkbox"/>	3	Teri 

2

Passaggio 6. In *Servizi*, scegliere un'autorizzazione da concedere agli utenti del gruppo. Le opzioni sono:

- Disattivata - Questa opzione indica che ai membri del gruppo non è consentito accedere all'utility basata sul Web tramite un browser.
- Sola lettura - Questa opzione consente ai membri del gruppo di leggere lo stato del sistema solo dopo aver eseguito l'accesso. Non possono modificare nessuna delle impostazioni.
- Admin - Questa opzione fornisce ai membri del gruppo i privilegi di lettura e scrittura ed è in grado di configurare lo stato del sistema.

Services

Web Login/NETCONF/RESTCONF: Disable Readonly Admin

Passaggio 7. Fare clic sul pulsante **più** per aggiungere una VPN da client a sito esistente. Se non è stata configurata questa opzione, è possibile trovare le informazioni in questo articolo nella sezione [Creazione di un profilo da client a sito](#).

Client to Site VPN:



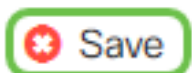
Group Name

1 Client

Passaggio 8. Fare clic su **Applica**.



Passaggio 9. Fare clic su **Salva**.



cisco(admin)

English



Passaggio 10. Fare di nuovo clic su **Applica** per salvare la configurazione in esecuzione nella configurazione di avvio.

Configuration Management

Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source: Running Configuration

Destination: Startup Configuration

Passaggio 11. Quando si riceve la conferma, fare clic su **OK**.

Information



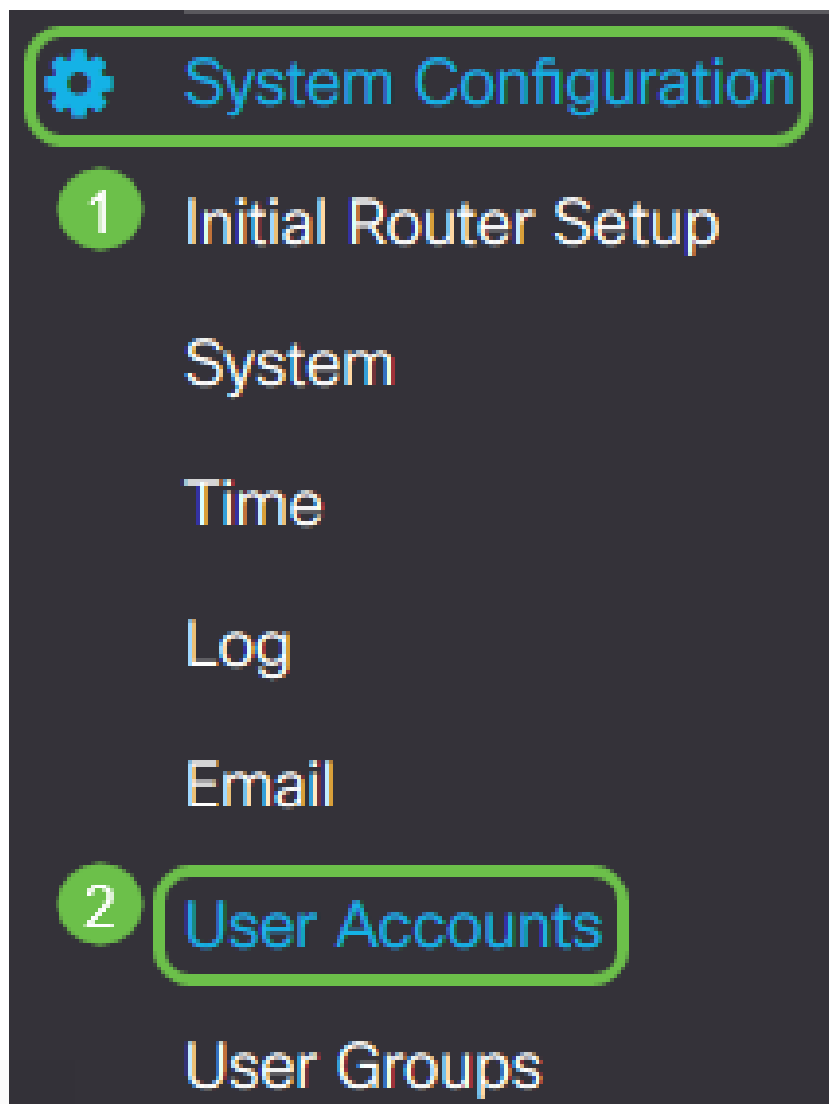
Running configuration saved to startup configuration

OK

A questo punto, è necessario creare un gruppo di utenti sul router serie RV160 o RV260.

Crea un account utente

Passaggio 1. Accedere all'utility basata sul Web del router e scegliere **Configurazione del sistema** > **Account utente**.



Passaggio 2. Nell'area *Utenti locali*, fare clic sull'icona **Aggiungi**.

Local Users



Username

John


Kevin

Teri

cisco

Passaggio 3. Immettere un nome per l'utente nel campo *Nome utente*, la password e il gruppo a cui si desidera aggiungere l'utente dal menu a discesa. Fare clic su **Apply** (Applica).

Add user account

 The current minimum requirements are as follows

* Minimal Password Length: 8

* Minimal Number of Character Classes: 3

Username:

1

Dave

New Password:

2

●●●●●●●●

Confirm Password:

3

●●●●●●●●

Password Strength meter:



Group:

4

VPNUsers

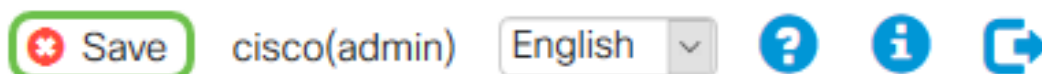
5

Apply

Cancel

Nota: Quando il client configura il client GreenBow sul proprio computer, accederà con lo stesso nome utente e password.

Passaggio 4. Fare clic su **Salva**.



Passaggio 5. Fare di nuovo clic su **Applica** per salvare la configurazione in esecuzione nella configurazione di avvio.

Configuration Management Apply

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC
Startup configuration: 2019-Jan-29, 17:52:43 UTC
Mirror Configuration: 2019-Jan-27, 23:00:07 UTC
Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.
To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Passaggio 6. Quando si riceve la conferma, fare clic su **OK**.

Information ×

 Running configuration saved to startup configuration

OK

A questo punto è necessario creare un account utente sul router RV160 o RV260.

Configura profilo IPsec

Passaggio 1. Accedere all'utility basata sul Web del router RV160 o RV260 e scegliere **VPN > IPsec VPN > Profili IPsec**.



Passaggio 2. Nella tabella Profili IPsec vengono visualizzati i profili esistenti. Fare clic sul pulsante **più** per creare un nuovo profilo.

IPSec Profiles



Name

Default

Amazon_Web_Services

Microsoft_Azure

VPNTTest

Nota: Amazon_Web_Services, Default e Microsoft_Azure sono profili predefiniti.

Passaggio 3. Creare un nome per il profilo nel campo *Nome profilo*. Il nome del profilo deve contenere solo caratteri alfanumerici e un carattere di sottolineatura (_) per i caratteri speciali.

Add/Edit a New IPSec Profile

Profile Name:

TheGreenBow

Keying Mode:

Auto Manual

IKE Version:

IKEv1 IKEv2

Passaggio 4. Fare clic su un pulsante di opzione per determinare il metodo di scambio delle chiavi che verrà utilizzato dal profilo per l'autenticazione. Le opzioni sono:

- Auto — i parametri dei criteri vengono impostati automaticamente. Questa opzione utilizza un criterio IKE (Internet Key Exchange) per l'integrità dei dati e gli scambi di chiavi di crittografia. Se questa opzione è selezionata, le impostazioni di configurazione

nell'area Parametri criteri automatici sono attivate.

- Manuale: questa opzione consente di configurare manualmente le chiavi per la crittografia dei dati e l'integrità del tunnel VPN. Se questa opzione è selezionata, le impostazioni di configurazione nell'area Parametri criteri manuali sono attivate. Non è molto usato.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Nota: Per questo esempio è stato scelto **Auto**.

Passaggio 5. Selezionare la versione IKE. Quando si imposta TheGreenBow sul lato client, è selezionata la stessa versione.

Add/Edit a New IPSec Profile

Profile Name:

Keying Mode: Auto Manual

IKE Version: IKEv1 IKEv2

Configurazione delle impostazioni di Fase 1 e Fase 2

Passaggio 1. Nell'area Opzioni fase 1, scegliere il gruppo Diffie-Hellman (DH) appropriato da utilizzare con la chiave nella fase 1 dall'elenco a discesa *Gruppo DH*. Diffie-Hellman è un protocollo di scambio chiave crittografica utilizzato nella connessione per lo scambio di set di chiavi già condivisi. La forza dell'algoritmo è determinata dai bit. Le opzioni sono:

- Group2-1024 bit: questa opzione calcola la chiave più lentamente, ma è più sicura di Group 1.
- Gruppo5-1536 bit — questa opzione calcola la chiave più lentamente, ma è la più sicura.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

28800

Passaggio 2. Dall'elenco a discesa *Encryption*, scegliere un metodo di crittografia per crittografare e decrittografare il payload di protezione (ESP) e il protocollo ISAKMP (Internet Security Association and Key Management Protocol). Le opzioni sono:

- 3DES: standard per la crittografia tripla dei dati. Non consigliato. Utilizzarlo solo se è necessario per la compatibilità con le versioni precedenti, in quanto è vulnerabile ad attacchi di "collisione di blocchi".
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit. 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.
- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.
- AES-256 — Advanced Encryption Standard utilizza una chiave a 256 bit. Si tratta dell'opzione di crittografia più sicura.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

MD5

SA Lifetime:

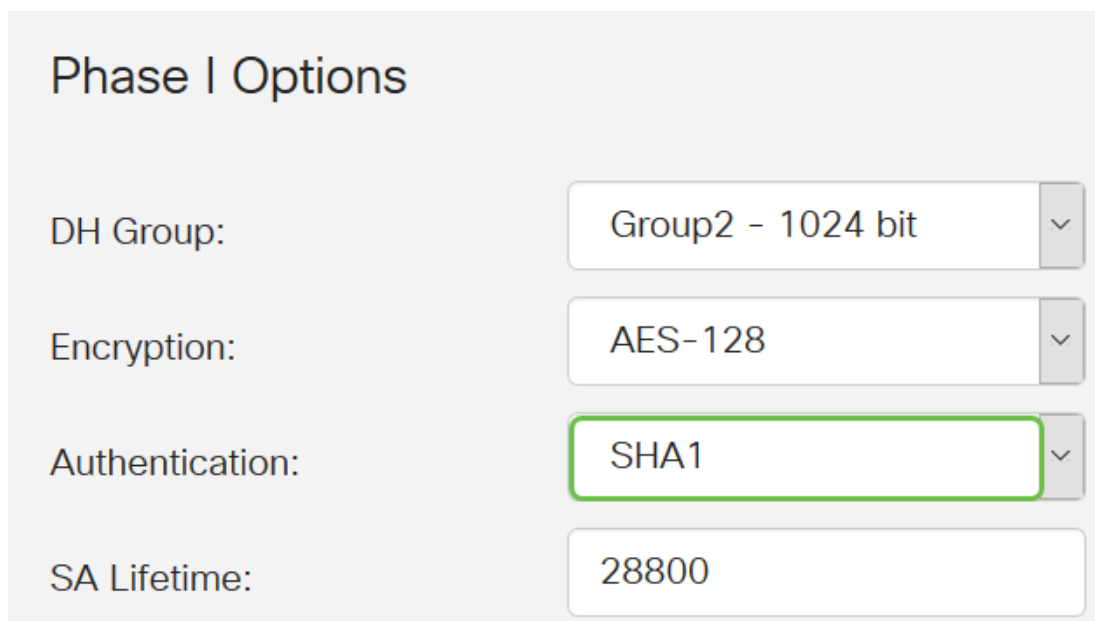
28800

Nota: AES è il metodo standard di crittografia su DES e 3DES per prestazioni e sicurezza più elevate. L'aumento della lunghezza della chiave AES aumenta la sicurezza con un calo delle prestazioni.

Passaggio 3. Dall'elenco a discesa *Authentication* (Autenticazione), scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- MD5 — Message-Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit. Si tratta dell'algoritmo più sicuro e consigliato.

Nota: Verificare che entrambe le estremità del tunnel VPN utilizzino lo stesso metodo di autenticazione.



The image shows a configuration window titled "Phase I Options". It contains four settings:

- DH Group:** Group2 - 1024 bit
- Encryption:** AES-128
- Authentication:** SHA1 (highlighted with a green border)
- SA Lifetime:** 28800

Nota: MD5 e SHA sono entrambe funzioni hash crittografiche. Prendono un dato, lo compattano e creano un output esadecimale unico che in genere non può essere riprodotto. Nell'esempio viene scelto SHA1.

Passaggio 4. Nel campo *Durata SA* immettere un valore compreso tra 120 e 86400. Il valore predefinito è 28800. *Durata SA (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 2800 e l'intervallo è compreso tra 120 e 86400. Per la fase I verranno utilizzati 28800 secondi come durata dell'ASA.

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.

Phase I Options

DH Group:

Group2 - 1024 bit

Encryption:

AES-128

Authentication:

SHA1

SA Lifetime:

28800

Passaggio 5. Dall'elenco a discesa *Selezione protocollo* nell'area Opzioni fase II, scegliere un tipo di protocollo da applicare alla seconda fase della negoziazione. Le opzioni sono:

- ESP: questa opzione è nota anche come payload di sicurezza incapsulante. Questa opzione incapsula i dati da proteggere. Se si sceglie questa opzione, andare al passo 6 per scegliere un metodo di crittografia.
- AH — questa opzione è nota anche come AH (Authentication Header). Si tratta di un protocollo di sicurezza che fornisce l'autenticazione dei dati e il servizio anti-replay opzionale. AH è incorporato nel datagramma IP da proteggere. Se si sceglie questa opzione, andare al passaggio 7.

Phase II Options

Protocol Selection:

ESP

Encryption:

3DES

Authentication:

MD5

SA Lifetime:

3600

Perfect Forward Secrecy:

Enable

DH Group:

Group2 - 1024 bit

Passaggio 6. Se nel passaggio 6 è stato scelto ESP, scegliere una *cifratura*. Le opzioni sono:

- 3DES: standard Triple Data Encryption
- AES-128 — Advanced Encryption Standard utilizza una chiave a 128 bit.

- AES-192 — Advanced Encryption Standard utilizza una chiave a 192 bit.
- AES-256 — Advanced Encryption Standard utilizza una chiave a 256 bit.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	MD5
SA Lifetime:	3600
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Passaggio 7. Dall'elenco a discesa *Authentication* (Autenticazione), scegliere un metodo di autenticazione che determinerà la modalità di autenticazione di ESP e ISAKMP. Le opzioni sono:

- MD5 — Message-Digest Algorithm ha un valore hash a 128 bit.
- SHA-1: l'algoritmo hash sicuro ha un valore hash a 160 bit.
- SHA2-256 — algoritmo hash sicuro con un valore hash a 256 bit.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	SHA1
SA Lifetime:	3600
Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Passaggio 8. Nel campo *Durata associazione di protezione* immettere un valore compreso tra 120 e 2800. Questo valore indica il periodo di tempo durante il quale l'associazione di protezione IKE rimarrà attiva in questa fase. Il valore predefinito è 3600.

Phase II Options

Protocol Selection:	ESP
Encryption:	AES-128
Authentication:	SHA1
SA Lifetime:	3600

Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Abilita** Perfect Forward Secrecy per generare una nuova 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.

Perfect Forward Secrecy:	<input checked="" type="checkbox"/> Enable
DH Group:	Group2 - 1024 bit

Passaggio 10. Dall'elenco a discesa *Gruppo DH*, scegliere un gruppo DH da utilizzare con la chiave nella fase 2. Le opzioni sono:

- Group2-1024 bit: questa opzione consente di calcolare la chiave più rapidamente, ma è meno sicura.
- Gruppo5-1536 bit — questa opzione calcola la chiave più lentamente, ma è la più sicura.

Phase II Options

Protocol Selection:

Encryption:

Authentication:

SA Lifetime:

Perfect Forward Secrecy: Enable


DH Group:

Passaggio 11. Fare clic su **Applica**.

Passaggio 12. Fare clic su **Save** per salvare la configurazione in modo permanente.

cisco(admin) English

Passaggio 13. Fare di nuovo clic su **Applica** per salvare la configurazione in esecuzione nella configurazione di avvio.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration


All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Passaggio 14. Quando si riceve la conferma, fare clic su **OK**.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

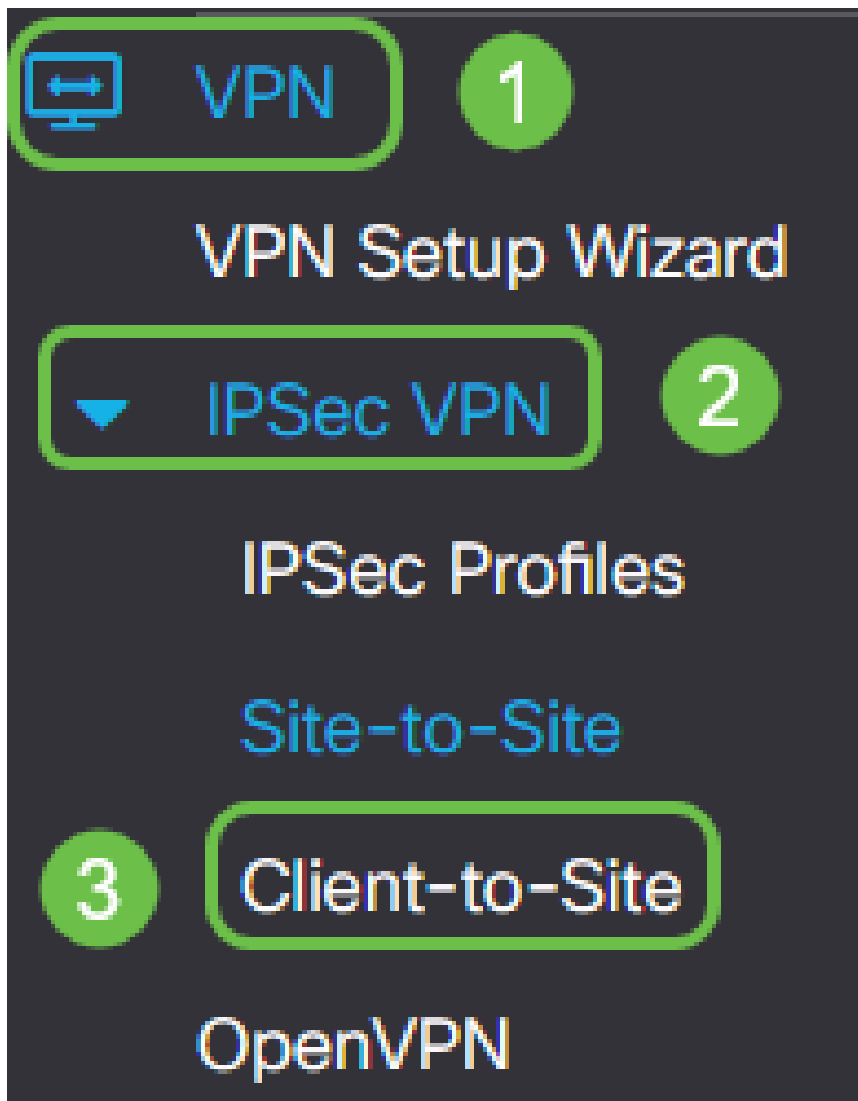
Source:

Destination:

È ora necessario configurare correttamente un profilo IPsec sul router RV160 o RV260.

Creazione di un profilo da client a sito

Passaggio 1. Scegliere **VPN > VPN IPSec > Da client a sito**.



Passaggio 2. Fare clic sull'icona **più**.

IPSec Profiles

<input type="checkbox"/>	Name	Policy	IKE Version
<input type="checkbox"/>	Default	Auto	IKEv1
<input type="checkbox"/>	Amazon_Web_Services	Auto	IKEv1
<input type="checkbox"/>	Microsoft_Azure	Auto	IKEv1

Passaggio 3. Nella scheda Basic Settings, selezionare la casella di controllo **Enable** per assicurarsi che il profilo VPN sia attivo.

Add/Edit a New Tunnel

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

Passaggio 4. Immettere un nome per la connessione VPN nel campo *Nome tunnel*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

IPSec Profile:

Default

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Passaggio 5. Selezionare il profilo IPSec da utilizzare dall'elenco a discesa *IPSec*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

Client

IPSec Profile:

TheGreenBow

(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Passaggio 6. Scegliere l'interfaccia dall'elenco a discesa *Interfaccia*.

Basic Settings

Advanced Settings

Enable:



Tunnel Name:

Client

IPSec Profile:

TheGreenBow



(Auto Profile (IKEv1) is chosen.)

⚠ Configure higher lifetimes if this profile is used for Windows Clients.

Interface:

WAN

Nota: Le opzioni dipendono dal modello di router in uso. Nell'esempio, viene scelta WAN.

Passaggio 7. Scegliere un metodo di autenticazione IKE. Le opzioni sono:

- Chiave già condivisa — Questa opzione consente di utilizzare una password condivisa per la connessione VPN.

- **Certificato** - questa opzione utilizza un certificato digitale che contiene informazioni quali il nome, l'indirizzo IP, il numero di serie, la data di scadenza del certificato e una copia della chiave pubblica del titolare del certificato.

IKE Authentication Method

Pre-shared Key:

Please enter a valid Preshared Key.

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Nota: Una chiave già condivisa può essere ciò che si desidera, ma deve semplicemente corrispondere sul sito e con il client quando impostano il client GreenBow sul loro computer.

Passaggio 8. Immettere la password di connessione nel campo *Chiave già condivisa*.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Passaggio 9. (Facoltativo) Deselezionare la casella di controllo **Abilita complessità chiave precondivisa minima** per poter utilizzare una password semplice.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key: Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Nota: In questo esempio, la complessità minima delle chiavi già condivise rimane abilitata.

Passaggio 10. (Facoltativo) Selezionare la casella di controllo **Mostra abilitazione chiave già condivisa** per visualizzare la password in testo normale.

IKE Authentication Method

Pre-shared Key:

Show Pre-shared Key:

 Enable

Preshared Key Strength Meter:

Minimum Preshared Key Complexity: Enable

Certificate:

Nota: In questo esempio, Show Pre-shared key è disattivato.

Passaggio 11. Scegliere un identificatore locale dall'elenco a discesa *Identificatore locale*. Le opzioni sono:

- Local WAN IP: questa opzione utilizza l'indirizzo IP dell'interfaccia WAN (Wide Area Network) del gateway VPN.
- Indirizzo IP - Questa opzione consente di immettere manualmente un indirizzo IP per la connessione VPN. Questo è l'indirizzo IP WAN del router sul sito (ufficio).
- FQDN: questa opzione è nota anche come nome di dominio completo (FQDN). Consente di utilizzare un nome di dominio completo per un computer specifico su Internet.
- FQDN utente — questa opzione consente di utilizzare un nome di dominio completo per un utente specifico su Internet.

Local Identifier:

1

2

Remote Identifier:

Nota: Nell'esempio, viene scelto IP Address (Indirizzo IP) e viene immesso l'indirizzo IP WAN del router sul sito. Nell'esempio, è stato immesso 24.x.x.x. L'indirizzo completo è stato offuscato per motivi di privacy.

Passaggio 12. Scegliere un identificatore per l'host remoto. Le opzioni sono:

- Indirizzo IP - Questa opzione utilizza l'indirizzo IP WAN del client VPN. Per trovare l'indirizzo IP WAN, immettere "what is my IP" (qual è il mio IP) nel browser Web. Indirizzo IP del client.
- FQDN: nome di dominio completo. Questa opzione consente di utilizzare un nome di dominio completo per un computer specifico su Internet.
- FQDN utente — questa opzione consente di utilizzare un nome di dominio completo per un utente specifico su Internet.

Nota: Nell'esempio, viene scelto IP Address (Indirizzo IP) e viene immesso l'indirizzo IPv4 corrente del router nella posizione del client. Questo può essere determinato effettuando una ricerca per "Qual è il mio indirizzo IP" nel vostro browser web. L'indirizzo può cambiare, quindi se

si verificano problemi di connessione dopo una configurazione corretta, può essere un'area da controllare e modificare sia sul client che sul sito.

Local Identifier:

Remote Identifier: **1** **2**

Passaggio 13. (Facoltativo) Selezionare la casella di controllo **Autenticazione estesa** per attivare la funzionalità. Se attivata, questa opzione fornirà un ulteriore livello di autenticazione che richiederà agli utenti remoti di inserire le proprie credenziali prima di ottenere l'accesso alla VPN.

Extended Authentication +

Group Name

Passaggio 14. (Facoltativo) Scegliere il gruppo che utilizzerà l'autenticazione estesa facendo clic sull'icona **più** e selezionando l'utente dall'elenco a discesa.

Extended Authentication **1** +

Group Name

CiscoTest123

KevGroupTest

VPNUsers **2**

Nota: Nell'esempio, viene scelto **VPNUsers**.

Passaggio 15. In *Intervallo pool per LAN client*, immettere il primo indirizzo IP e l'indirizzo IP finale che possono essere assegnati a un client VPN. Deve trattarsi di un pool di indirizzi che non si sovrappone agli indirizzi del sito. Queste interfacce possono essere definite interfacce virtuali. Se viene visualizzato un messaggio che indica la necessità di modificare un'interfaccia virtuale, è possibile risolvere il problema.

Pool Range for Client LAN:

Start IP: **1**

End IP: **2**

Passaggio 16. Selezionare la scheda **Impostazioni avanzate**.

Basic Settings

Advanced Settings

Passaggio 17. (Facoltativo) Scorrere fino alla fine della pagina e selezionare **Modalità aggressiva**. La funzionalità della modalità aggressiva consente di specificare gli attributi del tunnel RADIUS per un peer IPsec e di avviare una negoziazione in modalità aggressiva IKE (Internet Key Exchange) con il tunnel. Per ulteriori informazioni su Modalità aggressiva e Modalità principale, fare clic [qui](#).

Additional Settings

Aggressive Mode

Compress (Support IP Payload Compression Protocol (IPComp))

Nota: La casella di controllo *Comprimi* consente 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). In questo esempio, l'opzione *Comprimi* non è selezionata.

Passaggio 18. Fare clic su **Applica**.

Apply

Cancel

Passaggio 19. Fare clic su **Salva**.

 Save

cisco(admin)

English



Passaggio 20. Fare di nuovo clic su **Applica** per salvare la configurazione in esecuzione nella configurazione di avvio.

Configuration Management 

Configuration File Name

Last Change Time

Running Configuration: 2019-Jan-29, 17:51:56 UTC

Startup configuration: 2019-Jan-29, 17:52:43 UTC

Mirror Configuration: 2019-Jan-27, 23:00:07 UTC

Backup Configuration: --

Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots.

To retain the configuration between reboots, make sure you copy the Running Configuration file to the Startup Configuration file after you have completed all your changes.

Source:

Destination:

Passaggio 21. Quando si riceve la conferma, fare clic su **OK**.

Information

 Running configuration saved to startup configuration



A questo punto, è necessario configurare il tunnel da client a sito sul router per il client VPN GreenBow.

Configurare il client VPN GreenBow nel computer del processo di lavoro remoto

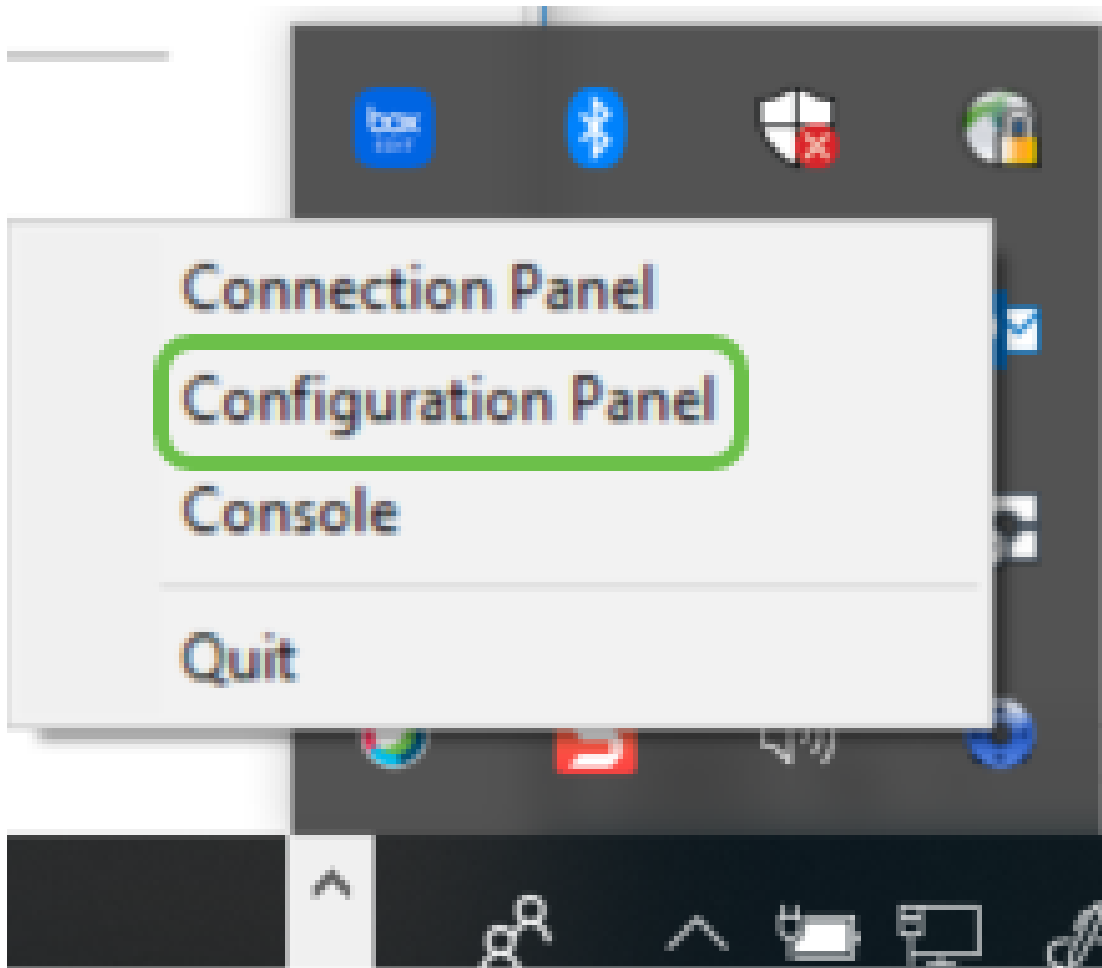
Configurazione delle impostazioni della fase 1

Per scaricare l'ultima versione del software Client VPN IPsec di GreenBow, fare clic [qui](#).

Passaggio 1. Fare clic con il pulsante destro del mouse sull'icona di GreenBow VPN Client. Si trova nell'angolo inferiore destro della barra delle applicazioni.

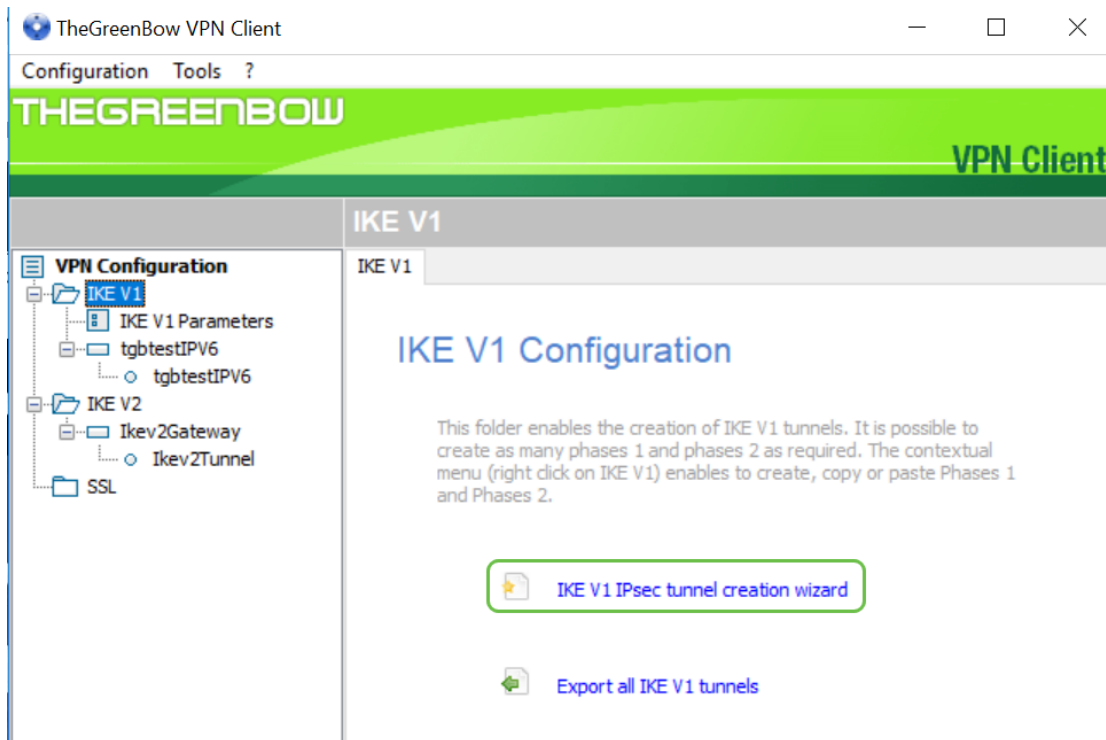


Passaggio 2. Selezionare il pannello di configurazione.



Nota: Questo è un esempio in un computer Windows. Questa impostazione può variare a seconda del software in uso.

Passaggio 3. Selezionare **Creazione guidata tunnel IPsec IKE V1**.



Nota: Nell'esempio, è in corso la configurazione di IKE versione 1. Per configurare IKE versione 2, seguire la stessa procedura facendo clic con il pulsante destro del mouse sulla cartella IKE V2. Inoltre, è necessario selezionare IKEv2 per il profilo IPsec sul router del sito.

Passaggio 4. Inserire l'indirizzo IP WAN pubblico del router presso il sito (ufficio) in cui si trova il file server, la chiave già condivisa e l'indirizzo interno privato della rete remota sul sito. Fare clic su **Next** (Avanti). In questo esempio, il sito è 24.x.x.x. Gli ultimi tre ottetti (gruppi di numeri in questo indirizzo IP) sono stati sostituiti da una x per proteggere questa rete. Immettere l'indirizzo IP completo.

VPN Configuration Wizard



VPN tunnel parameters

2/3

Enter the following parameters for the VPN tunnel:

IP or DNS public (external) address: of the remote gateway	<input type="text" value="24. . ."/>	1
Preshared key:	<input type="text" value="....."/>	2
IP private (internal) address: of the remote network	<input type="text" value="10 . 2 . 0 . 0"/>	3

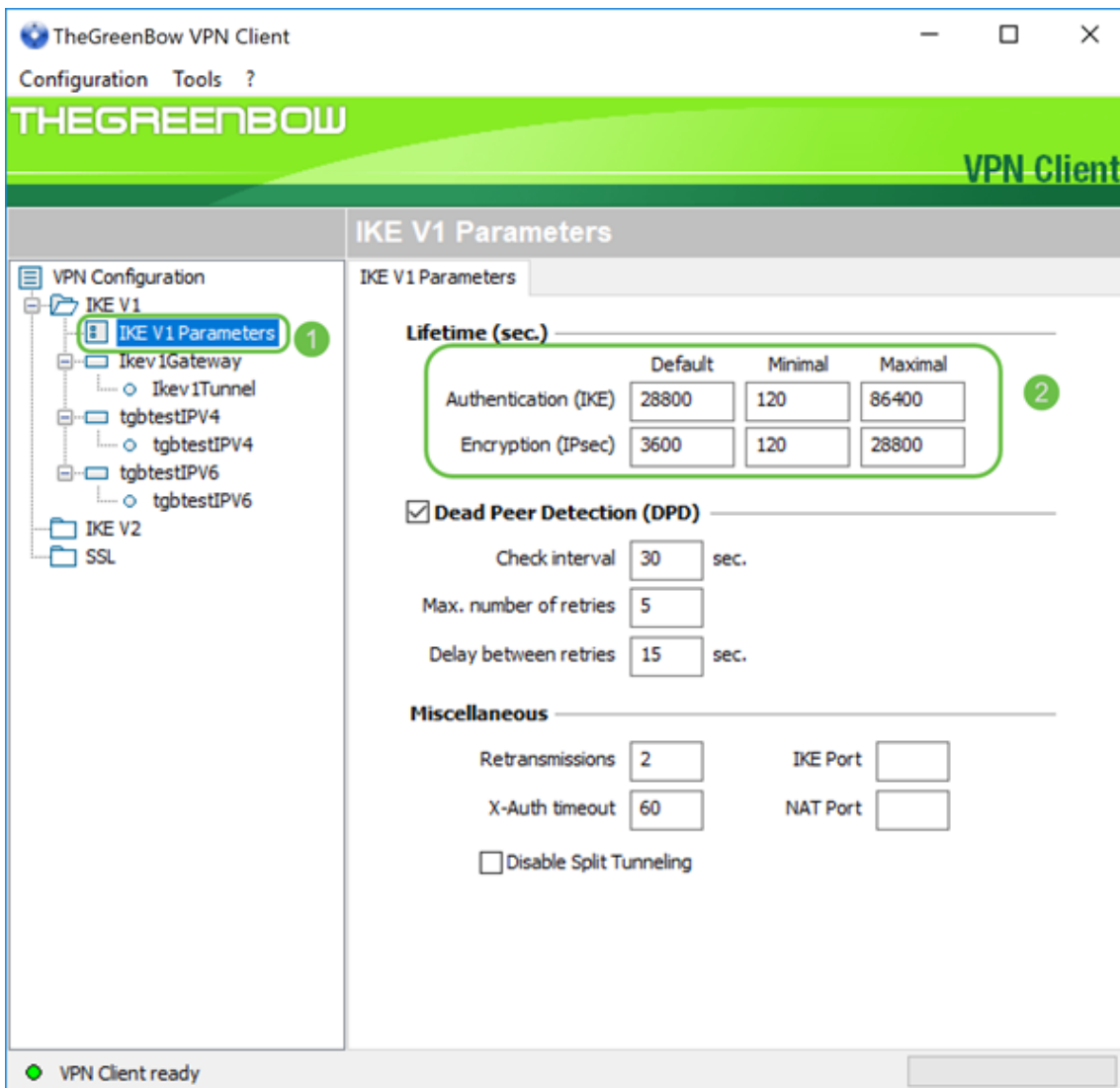
< Previous **Next >** 4 Cancel

Passaggio 5. Fare clic su **Finish**.

You may change these parameters anytime directly with the main interface.

< Previous **Finish** Cancel

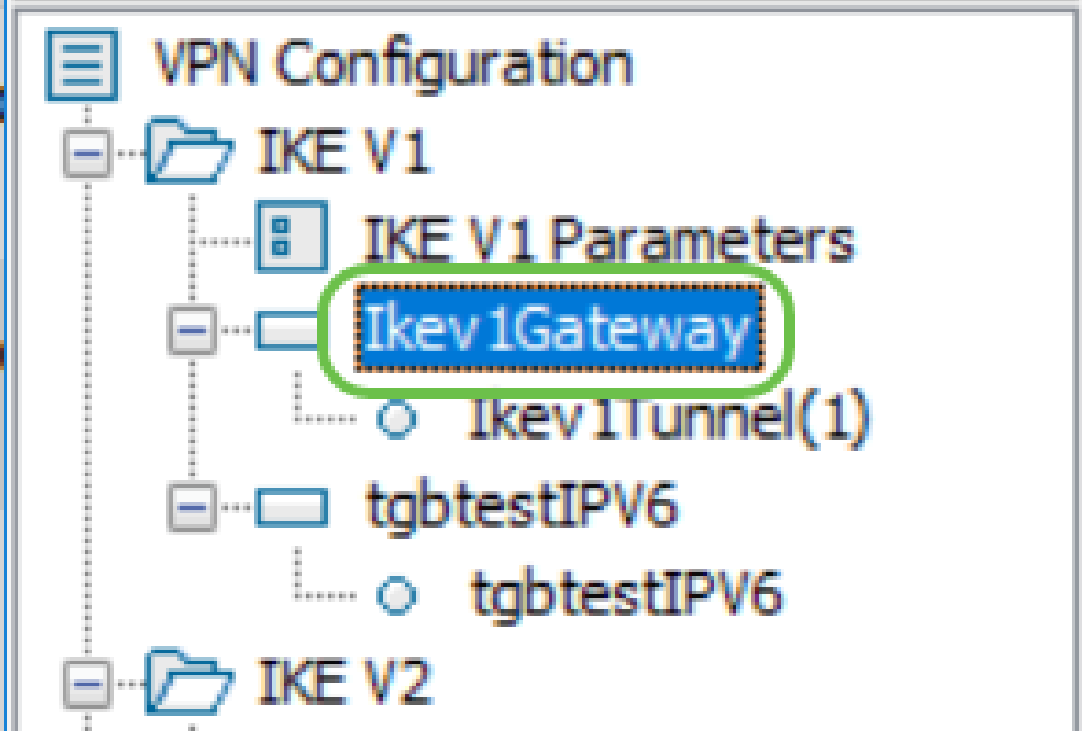
Passaggio 6 (Facoltativo) È possibile modificare i parametri IKE V1. È possibile regolare la durata predefinita, minima e massima di GreenBow. In questa posizione è possibile immettere qualsiasi intervallo della durata accettato dal router.



Passaggio 7. Fare clic sul gateway creato.

Configuration Tools ?

THEGREENBOW



Passaggio 8. Nella scheda *Autenticazione* sotto *Indirizzi* verrà visualizzato un elenco a discesa di indirizzi locali. È possibile sceglierne uno o selezionare **Qualsiasi**, come mostrato di seguito.

Configuration Tools ?

THEGREENBOW

VPN

Ikev1Gateway: Authentication

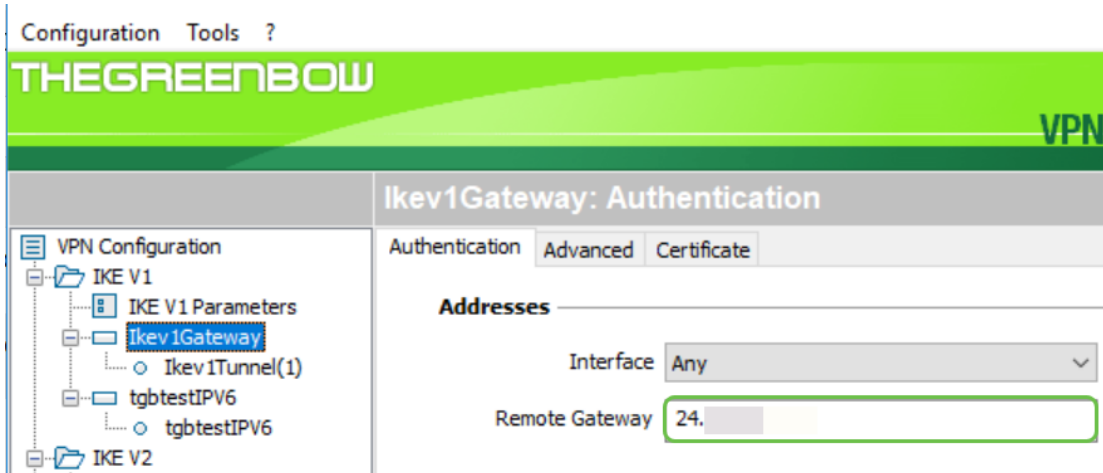
Authentication | Advanced | Certificate

Addresses

Interface: Any

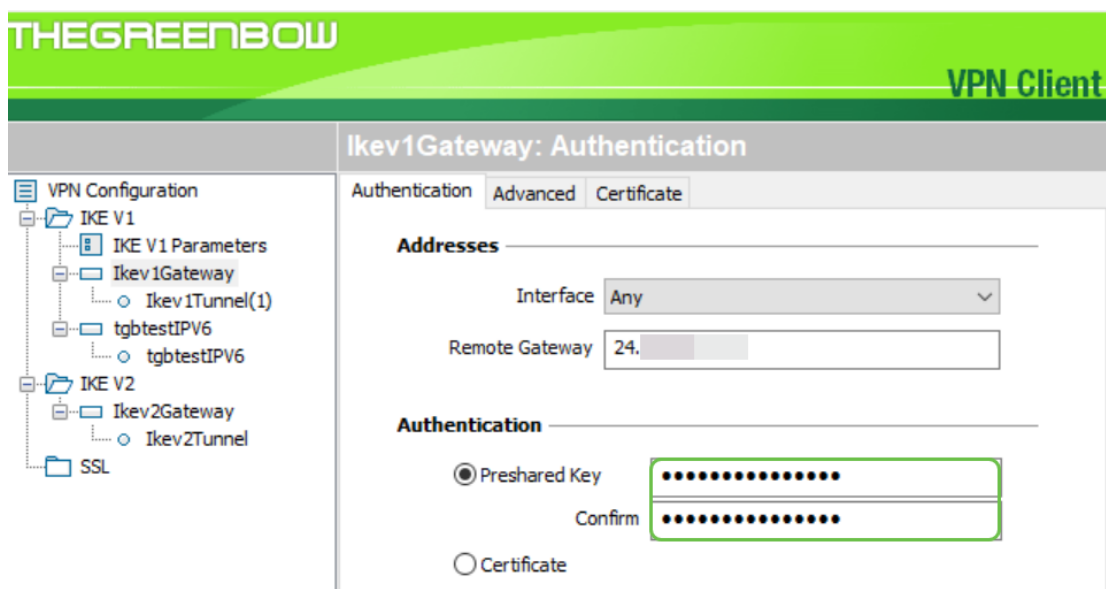
Remote Gateway:

Passaggio 9. Immettere l'indirizzo del gateway remoto nel campo *Gateway remoto*. Può essere un indirizzo IP o un nome DNS. Questo è l'indirizzo IP pubblico del router sul sito (ufficio).



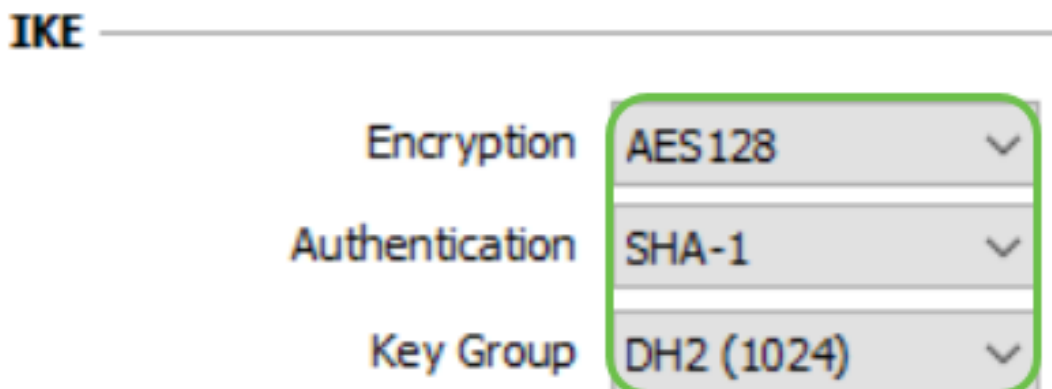
Passaggio 10. In *Autenticazione* scegliere il tipo di autenticazione. Le opzioni sono:

- Chiave già condivisa — questa opzione consente all'utente di utilizzare una password configurata sul gateway VPN. Per poter stabilire un tunnel VPN, l'utente deve associare la password.
- Certificato — questa opzione utilizza un certificato per completare l'handshake tra il client VPN e il gateway VPN.



Nota: Nell'esempio, è stata immessa e confermata la chiave già condivisa configurata sul router.

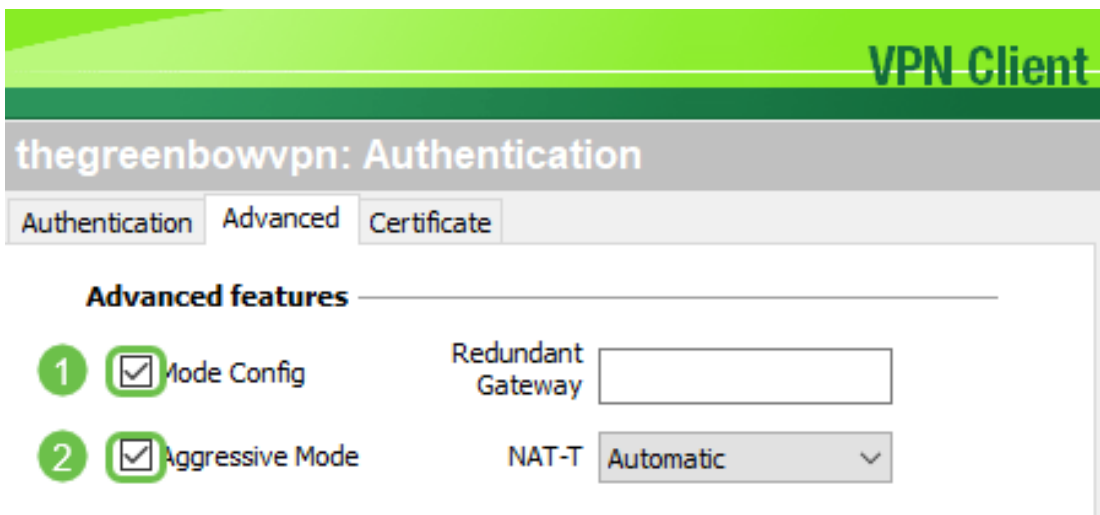
Passaggio 11. In *IKE*, impostare le impostazioni di crittografia, autenticazione e gruppo di chiavi in modo che corrispondano alla configurazione del router.



Passaggio 12. Fare clic sulla scheda **Avanzate**.

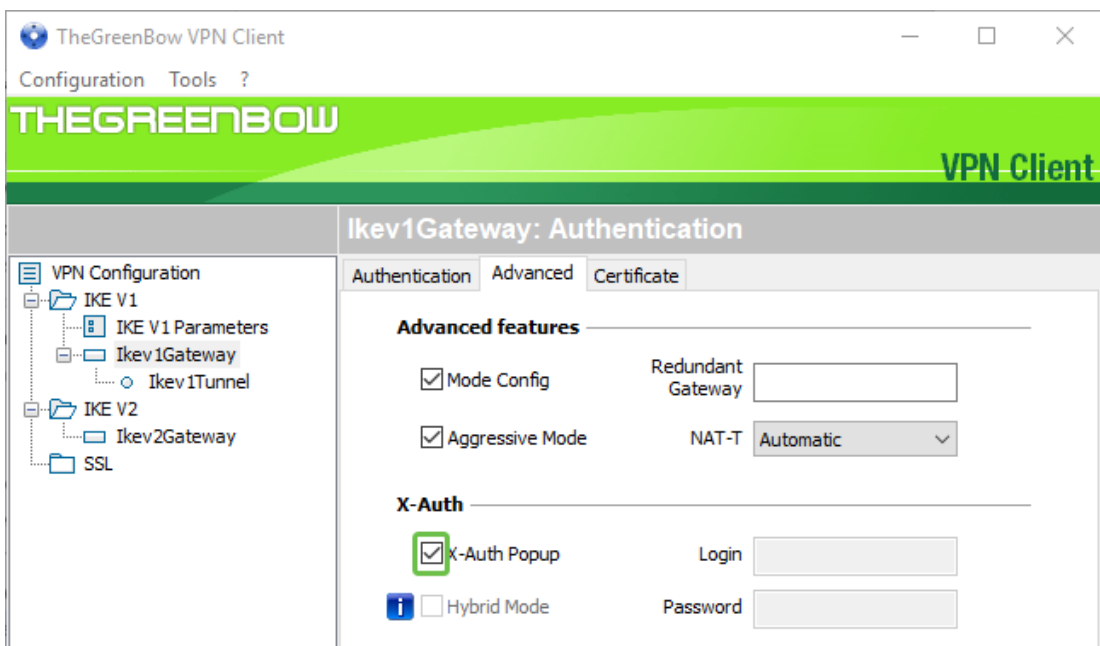


Passaggio 13. In Advanced features, selezionare le caselle di controllo **Mode Config** e **Aggressive Mode**. La modalità aggressiva è stata selezionata sull'RV160 nel profilo da client a sito di questo esempio. Lasciare l'impostazione NAT-T su Automatico.



Nota: Con la configurazione della modalità abilitata, il client VPN GreenBow estrae le impostazioni dal gateway VPN per tentare di stabilire un tunnel. NAT-T consente di stabilire una connessione più rapidamente.

Passaggio 14. (Facoltativo) In *X-Auth*, è possibile selezionare la casella di controllo **X-Auth Popup** per richiamare automaticamente la finestra di login quando si avvia una connessione. Nella finestra di accesso l'utente immette le proprie credenziali per completare il tunnel.



Passaggio 15. (Facoltativo) Se non si seleziona *X-Auth Popup*, immettere il proprio nome utente nel campo *Login*. Il nome utente immesso al momento della creazione di un account utente nel gateway VPN e la password nel sito.

X-Auth

X-Auth Popup

Hybrid Mode

Login

Password

Passaggio 16. In *ID locale e remoto* impostare l'ID locale e l'ID remoto in modo che corrispondano alle impostazioni del gateway VPN.

Local and Remote ID

	Type of ID:	Value for the ID:
Local ID	<input type="text" value="IP Address"/>	<input type="text"/>
Remote ID	<input type="text" value="IP Address"/>	<input type="text"/>

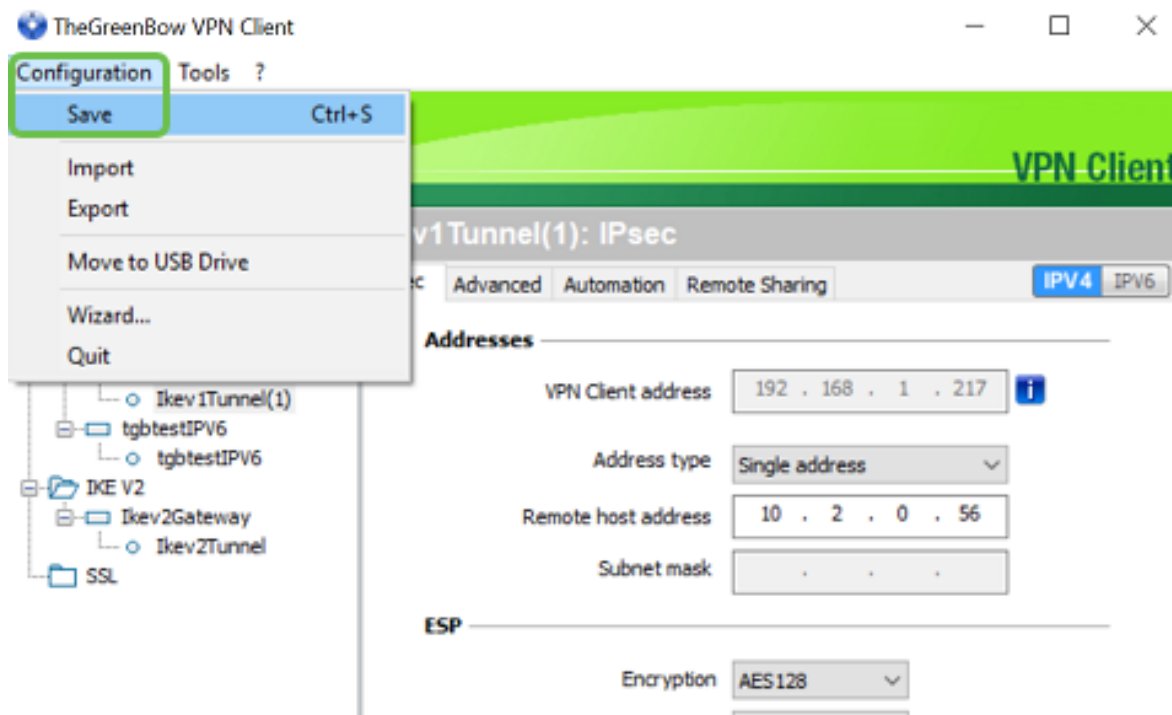
Nota: Nell'esempio, sia l'ID locale che l'ID remoto sono impostati su Indirizzo IP in modo da corrispondere alle impostazioni del gateway VPN RV160 o RV260.

Passaggio 17. In *Valore per l'ID*, immettere l'ID locale e l'ID remoto nei rispettivi campi. L'ID locale è l'indirizzo IP WAN del client. Questo può essere trovato facendo una ricerca web per "What's my IP". L'ID remoto è l'indirizzo IP WAN del router del sito.

Local and Remote ID

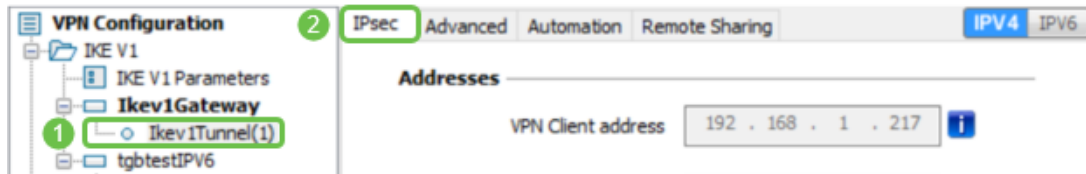
	Type of ID:	Value for the ID:
Local ID	<input type="text" value="IP Address"/>	<input type="text" value="108.233. ."/>
Remote ID	<input type="text" value="IP Address"/>	<input type="text" value="24. ."/>

Passaggio 18. Fare clic su **Configuration** (Configurazione) e scegliere **Save** (Salva).

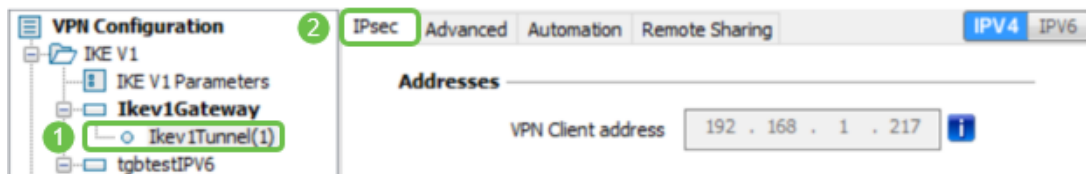


Configura impostazioni tunnel

Passaggio 1. Fare clic su **Ikev1Tunnel(1)** (il nome dell'utente potrebbe essere diverso) e sulla scheda **IPsec**. L'indirizzo del client VPN viene inserito automaticamente se è stata selezionata l'opzione Mode Config nelle impostazioni avanzate di Ikev1Gateway. Visualizza l'indirizzo IP locale del computer/laptop nella posizione remota.

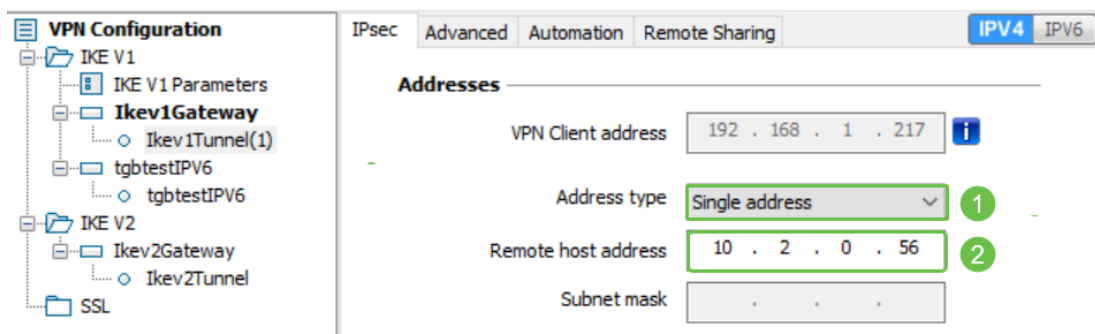


Passaggio 2. Scegliere il tipo di indirizzo a cui il client VPN può accedere dall'elenco a discesa *Tipo di indirizzo*. Può essere un indirizzo singolo, un intervallo di indirizzi o un indirizzo di subnet. L'indirizzo predefinito, Subnet address, include automaticamente l'indirizzo del client VPN (l'indirizzo IP locale del computer), l'indirizzo LAN remoto e la subnet mask. Se si seleziona Indirizzo singolo o Intervallo di indirizzi, questi campi dovranno essere compilati manualmente. Immettere l'indirizzo di rete a cui deve accedere il tunnel VPN nel campo *Indirizzo LAN remoto* e la subnet mask della rete remota nel campo *Subnet mask*.

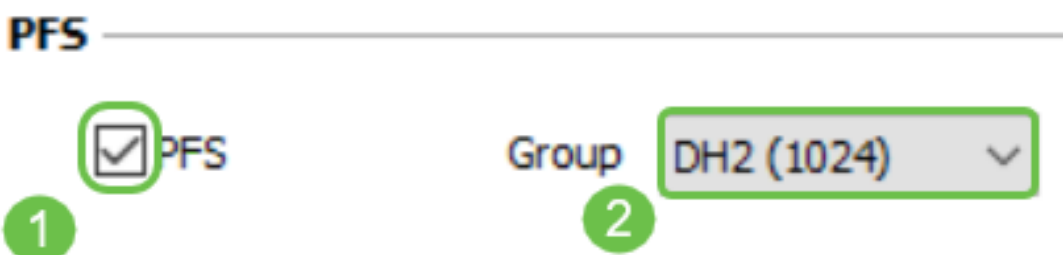


Nota: Nell'esempio, è stato scelto Single address (Indirizzo singolo) e viene immesso l'indirizzo IP locale del router sul sito.

Passaggio 3. In *ESP*, impostare Encryption, Authentication e Mode (Crittografia, autenticazione e modalità) in modo che corrispondano alle impostazioni del gateway VPN nel sito (ufficio).

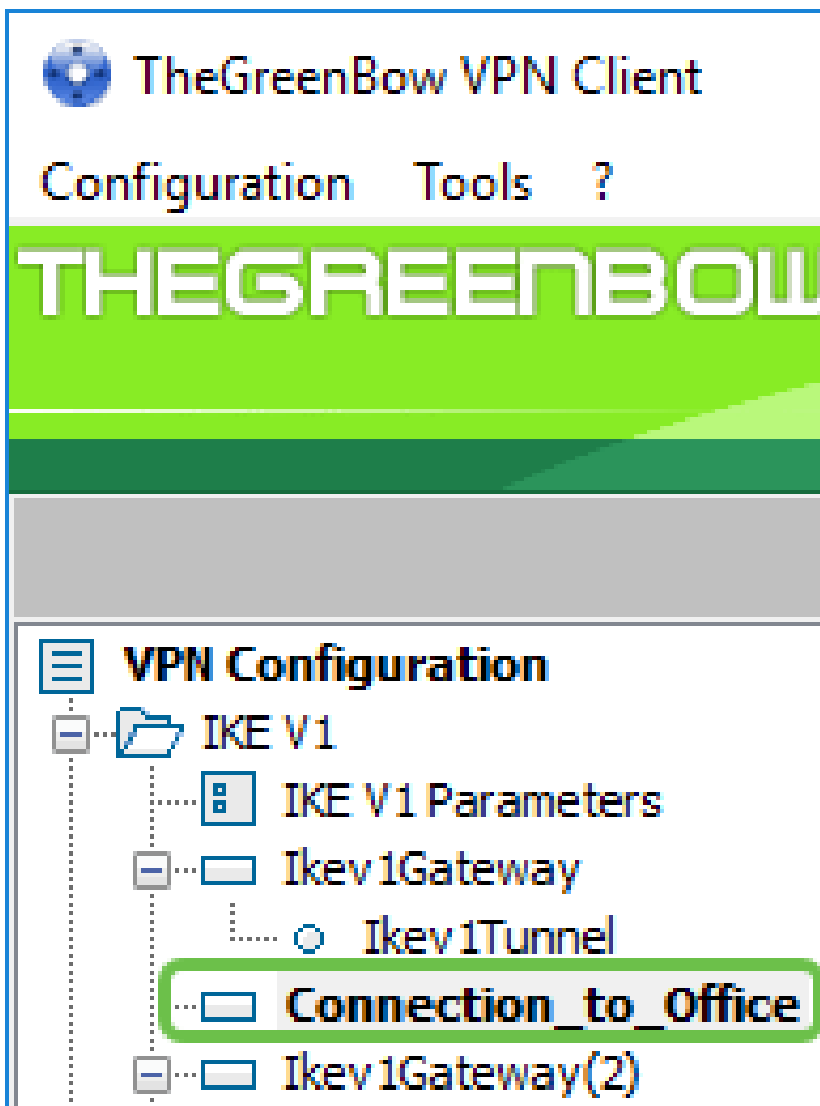


Passaggio 4. (Facoltativo) In *PFS*, selezionare la casella di controllo **PFS** per abilitare PFS (Perfect Forward Secrecy). PFS genera chiavi casuali per la crittografia della sessione. Selezionare un'impostazione di gruppo PFS dall'elenco a discesa *Gruppo*. Se è stato abilitato sul router, anche questo deve essere abilitato qui.

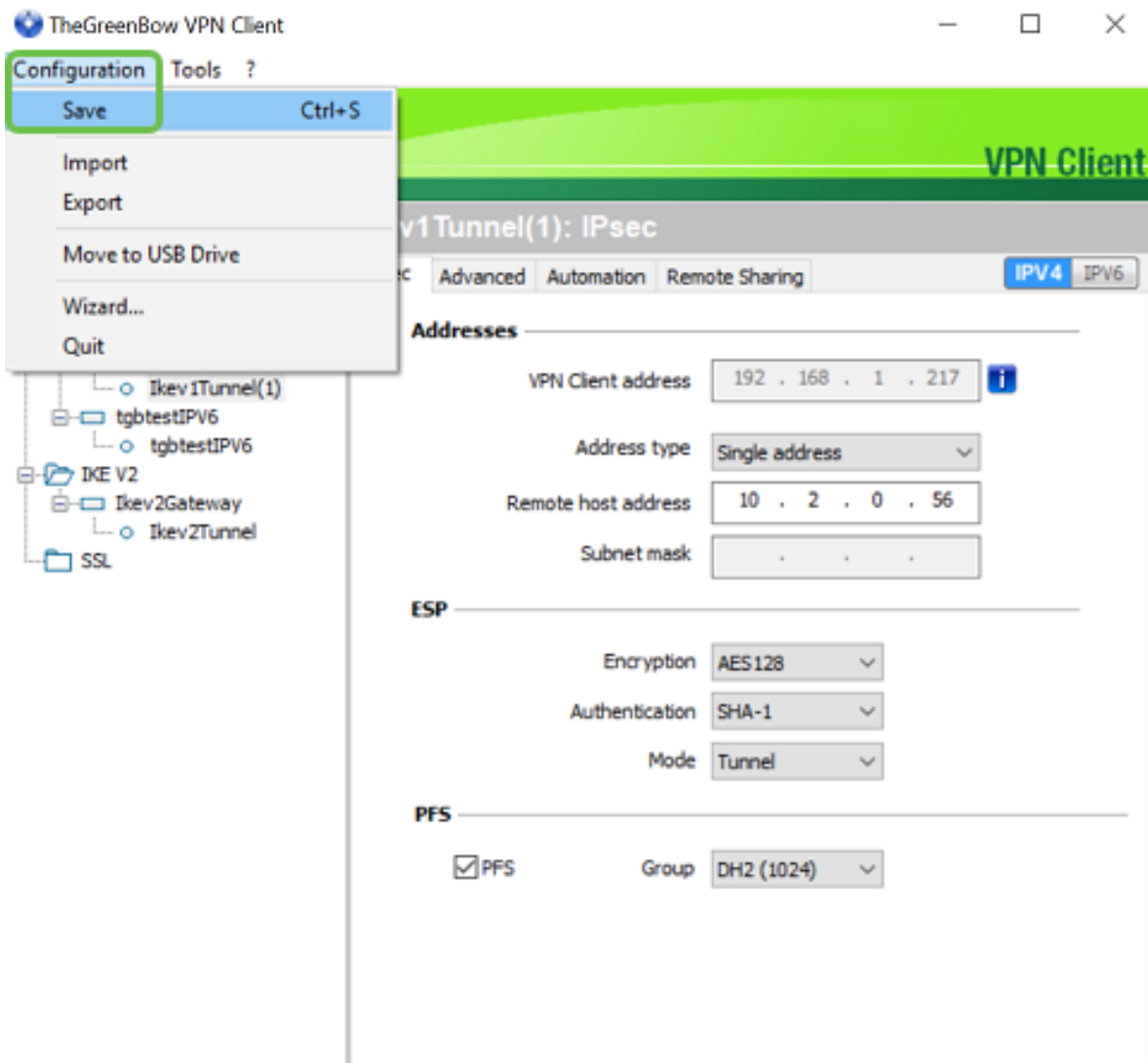


Passaggio 5. (Facoltativo) Fare clic con il pulsante destro del mouse sul nome del gateway Ikev1e

fare clic sulla sezione di ridenominazione per rinominarlo.



Passaggio 6. Fare clic su **Configuration** (Configurazione) e scegliere **Save** (Salva).



A questo punto, è necessario configurare correttamente il client VPN GreenBow per la connessione al router RV160 o RV260 tramite VPN.

Avvia una connessione VPN come client

Passaggio 1. Poiché TheGreenBow è aperto, è possibile fare clic con il pulsante destro del mouse sul tunnel e selezionare **Apri tunnel per avviare una connessione**.

Open tunnel	Ctrl+O
Export	
Copy	Ctrl+C
Rename	F2
Delete	Del

Nota: Per aprire un tunnel, fare doppio clic sul tunnel.

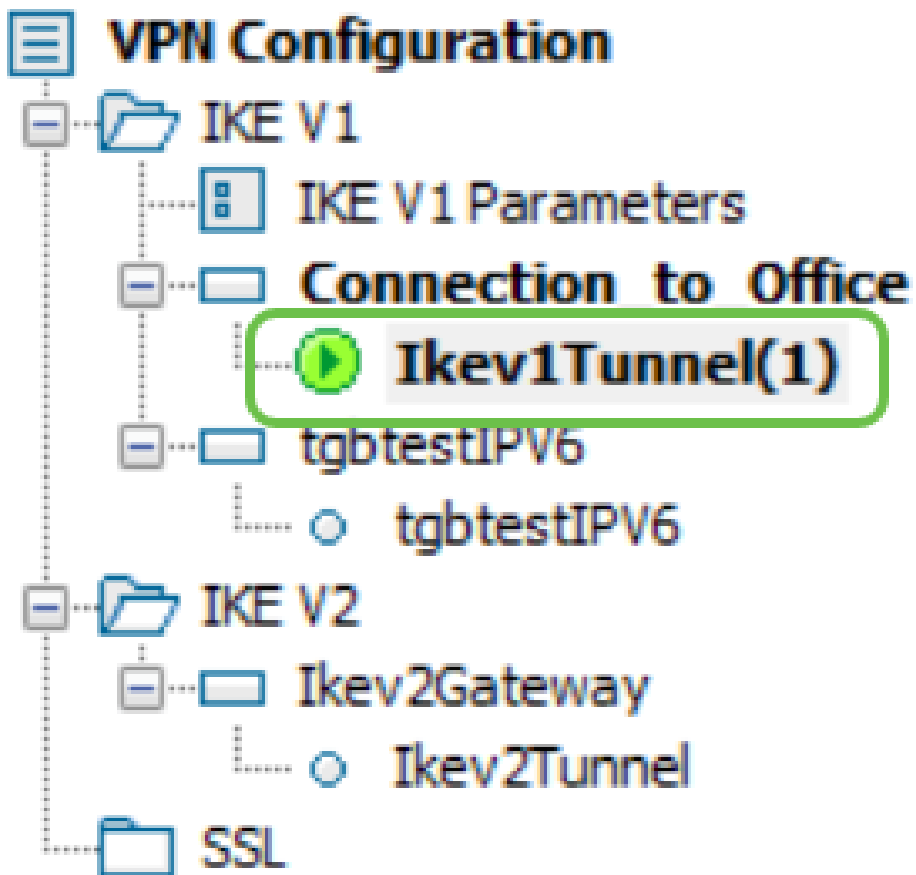
Passaggio 2. (Facoltativo) Se si sta iniziando una nuova sessione e TheGreenBow è stato chiuso, fare clic sull'icona **TheGreenBow VPN Client** sul lato destro della schermata.



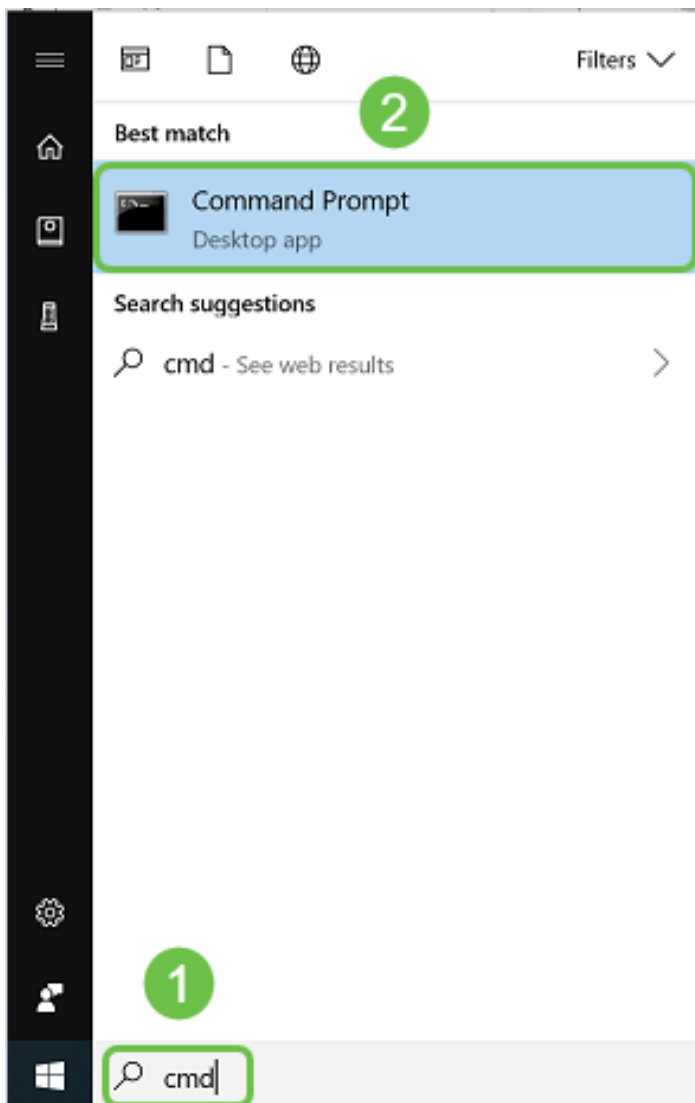
Passaggio 3. (Facoltativo) Questo passaggio è necessario solo se si sta configurando una nuova sessione e si è eseguito il passaggio 2. Scegliere la connessione VPN da utilizzare e quindi fare clic su **APRI**. La connessione VPN dovrebbe avviarsi automaticamente.



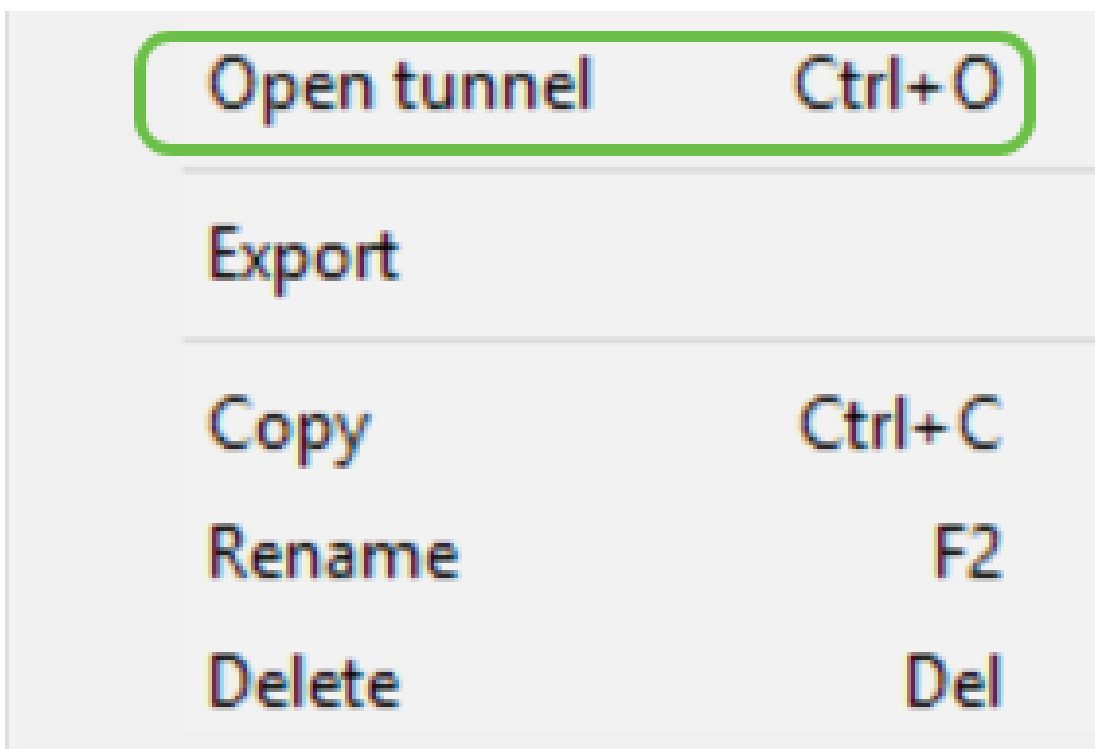
Passaggio 4. Quando il tunnel è connesso, accanto al tunnel viene visualizzato un cerchio verde. Se viene visualizzato un punto esclamativo, è possibile fare clic su di esso per individuare l'errore.



Passaggio 5. (Facoltativo) Per verificare di essere connessi, accedere al prompt dei comandi dal computer client.



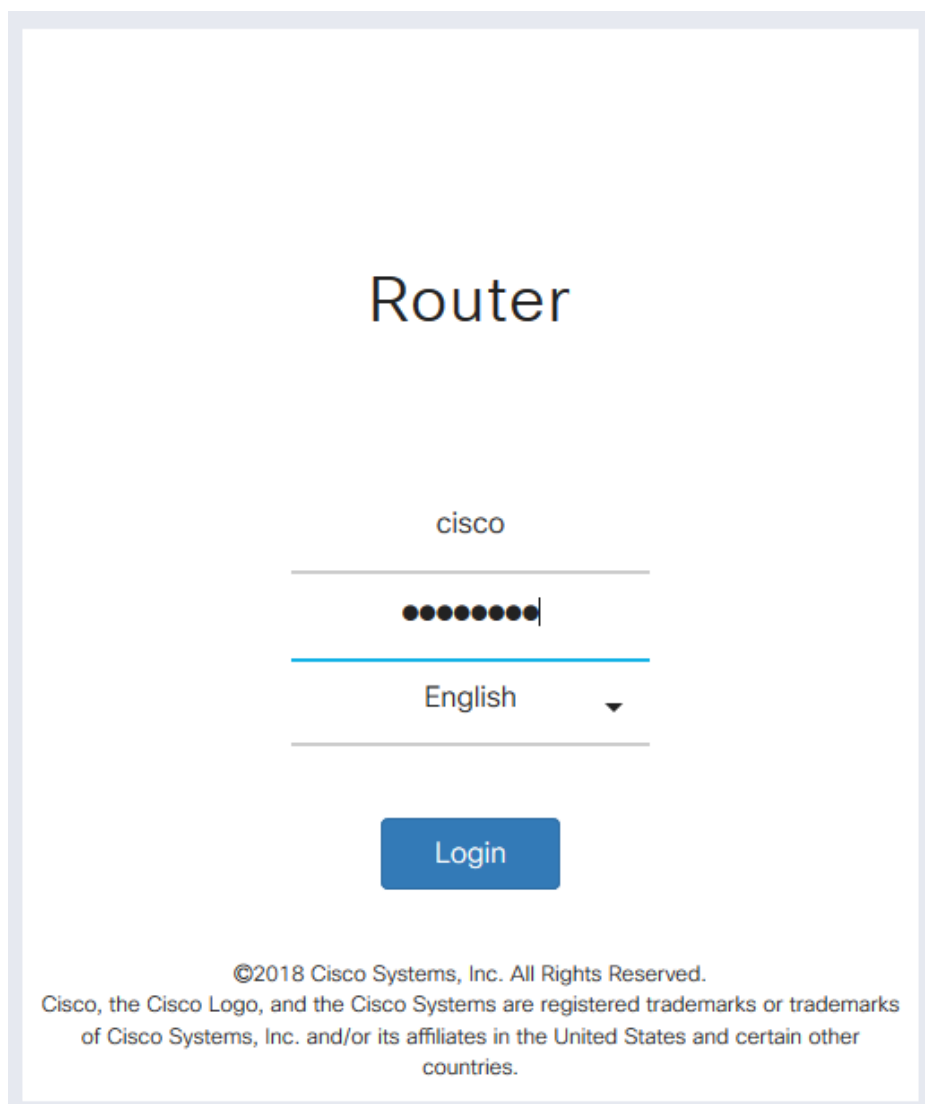
Passaggio 6. (Facoltativo) Immettere ping e quindi l'indirizzo IP della LAN privata del router sul sito. Se si ricevono le risposte, si è connessi.



Verifica stato VPN

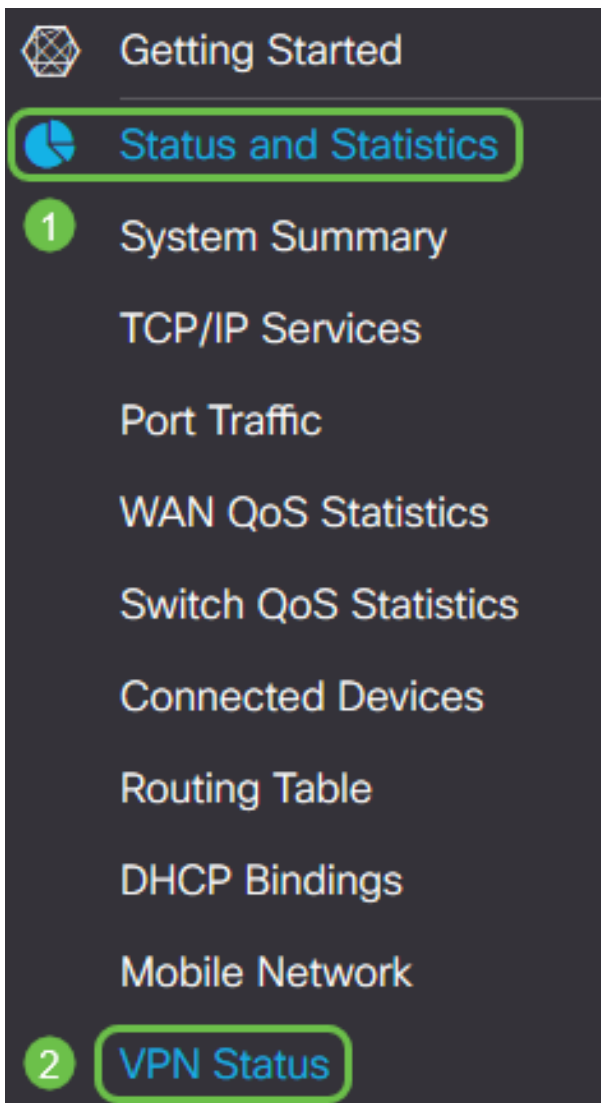
Verifica dello stato della VPN sul sito

Passaggio 1. Accedere all'utility basata sul Web del gateway VPN dell'RV160 o RV260.



The screenshot shows the login interface for a Cisco Router. At the top, the word "Router" is displayed in a large, black, sans-serif font. Below it, the word "cisco" is centered. A horizontal line separates the username field from the password field. The password field contains ten black dots and a vertical cursor. Another horizontal line separates the password field from the language selection field, which shows "English" and a downward-pointing arrow. Below the language field is a blue rectangular button with the word "Login" in white text. At the bottom of the page, there is a copyright notice: "©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. Scegliere **Stato e statistiche** > **Stato VPN**.



Passaggio 3. In *Stato tunnel da client a sito*, controllare la colonna *Connessioni* della *tabella di connessione*. La connessione VPN dovrebbe essere confermata.

Client to Site VPN Status

Connection Table

Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Passaggio 4. Fare clic sull'icona **occhio** per visualizzare ulteriori dettagli.




Client to Site VPN Status

Connection Table

Group/Tunnel Name	Connections	Phase2 Enc/Auth/Grp	Local Group	Action
Client	1	aes128-sha1-modp1024	0.0.0.0/0	

Passaggio 5. Di seguito vengono mostrati i dettagli dello stato della VPN da client a sito. Si noterà l'indirizzo IP WAN del client, l'indirizzo IP locale assegnato dal pool di indirizzi configurato durante l'installazione. Mostra anche i byte e i pacchetti inviati e ricevuti, nonché il tempo di connessione.

Se si desidera disconnettere il client, fare clic sull'icona blu della **catena interrotta** in *Azione*. Fare clic sulla **x** nell'angolo superiore destro per chiudere dopo l'ispezione.

Client IP (Actual)	Client IP (VPN)	TX Bytes	RX Bytes	TX Packets	RX Packets	Connect Time	Action 
108.233. 	10.2.1.1	0	14273	0	181	5 mins.	

Conclusioni

A questo punto, è necessario aver configurato e verificato correttamente la connessione VPN sul router RV160 o RV260 e configurare il client VPN GreenBow per la connessione al router anche tramite VPN.