

# Configurazione di un tunnel di accesso remoto (da client a gateway) per client VPN su router VPN RV016, RV042, RV042G e RV082

## Obiettivo

Questo articolo spiega come configurare il tunnel VPN (Virtual Private Network) di accesso remoto da client a gateway su router VPN RV016, RV042, RV042G e RV082 con l'aiuto di software client VPN di terze parti come The Green Bow o VPN Tracker.

## Introduzione

Una VPN è una rete privata utilizzata per connettere virtualmente i dispositivi dell'utente remoto tramite la rete pubblica per garantire la sicurezza. VPN tunnel di accesso remoto è il processo utilizzato per configurare una VPN tra un computer client e una rete. Il client viene configurato nel desktop o nel notebook degli utenti tramite software client VPN. Consente agli utenti di connettersi in modo sicuro alla rete in remoto. La connessione VPN da client a gateway è utile per consentire ai dipendenti remoti di connettersi alla rete aziendale in modalità remota e protetta.

## Dispositivi interessati

- RV016
- RV042
- RV042G
- RV082

## Versione del software

- v4.2.2.08

## Configurare un tunnel VPN

Passaggio 1. Accedere all'utility di configurazione Web e scegliere **VPN > Da client a gateway**. Viene visualizzata la pagina *Da client a gateway*:

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No.                    1

Tunnel Name :               

Interface :                     ▼

Enable :                       

---

**Local Group Setup**

Local Security Gateway Type :     ▼

IP Address :                    0.0.0.0

Local Security Group Type :     ▼

IP Address :                   

Subnet Mask :                

---

**Remote Client Setup**

Remote Security Gateway Type :     ▼

▼ :               

---

**IPSec Setup**

## Aggiungi nuovo tunnel

Passaggio 1. Fare clic sul pulsante di opzione appropriato in base al tipo di tunnel che si desidera aggiungere.

- Tunnel - Rappresenta un tunnel per un singolo utente remoto.
- Group VPN: rappresenta un tunnel per un gruppo remoto di utenti.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address : 0.0.0.0

Local Security Group Type :

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :

:

---

**IPSec Setup**

Il campo Numero tunnel è un campo generato automaticamente che visualizza il numero del tunnel.

**Client To Gateway**

Add a New Tunnel

Tunnel  Group VPN

Tunnel No. 1

Tunnel Name : tunnel\_1

Interface : WAN1

Enable :

---

**Local Group Setup**

Local Security Gateway Type : IP Only

IP Address : 0.0.0.0

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address :

---

**IPSec Setup**

Passaggio 2. Immettere un nome per il tunnel nel campo Nome tunnel.

Passaggio 3. Selezionare l'interfaccia WAN appropriata da utilizzare per il tunnel VPN dall'elenco a discesa Interface (Interfaccia).

Passaggio 4. (Facoltativo) Per abilitare la VPN, selezionare la casella di controllo nel campo Abilita. Per impostazione predefinita è sempre selezionata.

## Installazione gruppo locale

Passaggio 1. Selezionare il metodo di identificazione del router appropriato per stabilire un tunnel VPN dall'elenco a discesa *Local Security Gateway*. Ignorare questo passaggio se si è scelto Group VPN nel passaggio 1 della sezione *Add A New Tunnel*.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name : tunnel\_1

Interface : WAN1

Enable :

---

**Local Group Setup**

Local Security Gateway Type : IP Only

IP Address : [ ]

Local Security Group Type : [ ]

IP Address : [ ]

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address : [ ]

---

**IPSec Setup**

Keying Mode : IKE with Preshared key

- Solo IP: l'accesso al tunnel è possibile tramite un indirizzo IP statico della WAN. È possibile scegliere questa opzione solo se il router ha un IP WAN statico. L'indirizzo IP statico della WAN viene visualizzato automaticamente.
- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio FQDN (Fully Qualified Domain Name) registrato. L'indirizzo IP statico della WAN è un campo generato automaticamente.
- Autenticazione indirizzo IP + e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail. L'indirizzo IP statico della WAN è un campo generato automaticamente.
- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato.
- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail.

Passaggio 2. Immettere il nome del dominio completo registrato nel campo Nome dominio se si sceglie *Autenticazione IP + nome di dominio (FQDN)* o *Autenticazione IP dinamico + nome di dominio (FQDN)* nel passaggio 1.

Passaggio 3. Immettere l'indirizzo e-mail nel campo Indirizzo e-mail se si sceglie *Autenticazione IP + indirizzo e-mail (FQDN UTENTE)* o *Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE)* nel Passaggio 1.

Passaggio 4. Selezionare l'utente LAN locale appropriato o il gruppo di utenti che possono accedere al tunnel VPN dall'elenco a discesa *Gruppo di sicurezza locale*. Il valore predefinito è Subnet.

- IP - Solo un dispositivo LAN specifico può accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP del dispositivo LAN nel campo Indirizzo IP. L'indirizzo IP predefinito è 192.168.1.0.
- Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP e la subnet mask dei dispositivi LAN rispettivamente nei campi Indirizzo IP e Subnet mask. La maschera predefinita è 255.255.255.0.
- Intervallo IP - Una serie di dispositivi LAN può accedere al tunnel. Se si sceglie questa opzione, immettere gli indirizzi IP iniziale e finale rispettivamente nei campi IP iniziale e IP finale. L'intervallo predefinito è compreso tra 192.168.1.0 e 192.168.1.254.

### Client To Gateway

**Add a New Tunnel**

Tunnel       Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :  ▼

Enable :

---

**Local Group Setup**

Local Security Gateway Type :  ▼

IP Address : 0.0.0.0

Local Security Group Type : 
 ▼  
 IP  
 Subnet  
 IP Range

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :  ▼

▼ :

---

**IPSec Setup**

Keying Mode :  ▼

Passaggio 5. Fare clic su **Save** (Salva) per salvare le impostazioni.

## Installazione client remota

Passaggio 1. Se si sceglie Tunnel, scegliere il metodo di identificazione del client appropriato per stabilire un tunnel VPN dall'elenco a discesa *Tipo di gateway di sicurezza remoto*. Il valore predefinito è Solo IP. Ignorare questo passaggio se è stato scelto Group VPN nel Passaggio 1 della sezione *Add A New Tunnel*.

### Client To Gateway

**Add a New Tunnel**

Tunnel     Group VPN

Tunnel No. : 1

Tunnel Name :

Interface :

Enable :

---

**Local Group Setup**

Local Security Gateway Type :

IP Address :

Local Security Group Type :

IP Address :

Subnet Mask :

---

**Remote Client Setup**

Remote Security Gateway Type :

IP Address :

---

**IPSec Setup**

Keying Mode :

- Solo IP: l'accesso al tunnel è possibile solo tramite l'IP WAN statico del client. Per utilizzare questa opzione, è necessario conoscere l'IP WAN statico del client.
- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico del client e un dominio registrato.
- Autenticazione indirizzo IP + e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico del client e un indirizzo e-mail.
- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico del client e un dominio registrato.
- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico del client e un indirizzo e-mail.

Passaggio 2. Immettere l'indirizzo IP del client remoto nel campo *Indirizzo IP* se si sceglie *Autenticazione solo IP*, *IP + nome di dominio (FQDN)* o *IP + indirizzo di posta elettronica (FQDN utente)* nel passaggio 1.

Passaggio 3. Selezionare l'opzione appropriata dall'elenco a discesa per immettere l'indirizzo IP se lo si conosce oppure risolvere l'indirizzo IP dal server DNS se si sceglie *Autenticazione solo IP* o *Autenticazione IP + nome di dominio (FQDN)* o *Autenticazione IP + indirizzo di posta elettronica (FQDN UTENTE)* nel passaggio 1.

- Indirizzo IP: rappresenta l'indirizzo IP statico del client remoto. Immettere l'indirizzo IP statico nel campo.
- IP da DNS risolto: rappresenta il nome di dominio dell'indirizzo IP che recupera automaticamente l'indirizzo IP tramite il server DNS locale se non si conosce l'indirizzo IP statico del client remoto. Immettere il nome di dominio dell'indirizzo IP nel campo.

Passaggio 4. Immettere il nome di dominio dell'indirizzo IP nel campo Nome di dominio se si sceglie *Autenticazione IP + nome di dominio (FQDN)* o *Autenticazione IP dinamico + nome di dominio (FQDN)* nel passaggio 1.

Passaggio 5. Immettere l'indirizzo e-mail nel campo Indirizzo e-mail se si sceglie *Autenticazione IP + indirizzo e-mail (FQDN UTENTE)* o *Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE)* nel passaggio 1.

Passaggio 6. Se si sceglie Gruppo, scegliere il tipo di client remoto appropriato dall'elenco a discesa *Client remoto*. Ignorare questo passaggio se è stata scelta la VPN del tunnel nel passaggio 1 della sezione *Add A New Tunnel*.

- Nome dominio (FQDN) - È possibile accedere al tunnel tramite un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.
- Indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo e-mail del client. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail.
- Client VPN per Microsoft XP/2000: è possibile accedere al tunnel tramite il software Microsoft XP o Microsoft 2000 Windows. Gli utenti remoti con software client VPN Microsoft possono accedere al tunnel tramite il software.

**Client To Gateway**

**Add a New Group VPN**

Tunnel  Group VPN

Group No. 1

Tunnel Name : Tunnel\_2

Interface : WAN2

Enable :

---

**Local Group Setup**

Local Security Group Type : Subnet

IP Address : 192.168.1.0

Subnet Mask : 255.255.255.0

---

**Remote Client Setup**

Remote Client : Microsoft XP/2000 VPN Client

Domain Name(FQDN)

Email Address(USER FQDN)

Microsoft XP/2000 VPN Client

---

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Passaggio 7. Fare clic su **Save** (Salva) per salvare le impostazioni.

## Installazione di IPSec

IPSec (Internet Protocol Security) è un protocollo di protezione a livello Internet che fornisce protezione completa tramite autenticazione e crittografia durante qualsiasi sessione di comunicazione.

**Nota:** affinché IPSec funzioni correttamente, due estremità della VPN devono avere gli stessi metodi di crittografia, decrittografia e autenticazione. Anche la chiave Perfect Forward Secrecy deve essere la stessa su entrambi i lati del tunnel.

Passaggio 1. Selezionare la modalità di gestione delle chiavi appropriata per garantire la protezione dall'elenco a discesa *Modalità di impostazione chiavi*. La modalità predefinita è *IKE con chiave già condivisa*.

- **Manuale:** modalità di protezione personalizzata che consente di generare una nuova chiave di protezione autonomamente e di non eseguire alcuna negoziazione con la chiave. È la soluzione migliore da utilizzare durante la risoluzione dei problemi e in ambienti statici di piccole dimensioni. Se si sceglie Group VPN nel passo 1 della sezione Add A New Tunnel (Aggiungi un nuovo tunnel), questa opzione è disabilitata.
- **IKE con chiave già condivisa:** il protocollo IKE (Internet Key Exchange) viene utilizzato per generare e scambiare automaticamente una chiave già condivisa per stabilire la comunicazione di autenticazione per il tunnel.

Subnet Mask : 255.255.255.0

**Remote Client Setup**

Remote Security Gateway Type : IP Only

IP Address : 192.168.1.2

**IPSec Setup**

Keying Mode : **IKE with Preshared key** (selected), Manual, IKE with Preshared key

Phase 1 DH Group :

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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

## Configurazione manuale modalità chiave

Passaggio 1. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza (SPI, Security Parameter Index) in ingresso nel campo *SPI in ingresso*. L'indice SPI è contenuto nell'intestazione ESP (Encapsulating Security Payload Protocol) che determina insieme la protezione del pacchetto in ingresso. È possibile immettere da 100 a ffffffff. L'SPI in ingresso del router locale deve corrispondere all'SPI in uscita del router remoto.

Passaggio 2. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza (SPI) in uscita nel campo *SPI in uscita*. L'indice SPI è contenuto nell'intestazione ESP (Encapsulating Security Payload Protocol) che determina insieme la protezione del pacchetto in uscita. È possibile immettere da 100 a ffffffff. L'SPI in uscita del router remoto deve corrispondere all'SPI in entrata del router locale.

The screenshot shows a configuration interface with two sections: "Remote Client Setup" and "IPSec Setup".

- Remote Client Setup:**
  - Remote Security Gateway Type: IP Only
  - IP Address: 192.168.1.2
- IPSec Setup:**
  - Keying Mode: Manual
  - Incoming SPI: 100A
  - Outgoing SPI: 1BCD
  - Encryption: DES
  - Authentication: MD5
  - Encryption Key: (empty field)
  - Authentication Key: (empty field)

A red rectangle highlights the "Incoming SPI" and "Outgoing SPI" fields.

Passaggio 3. Selezionare il metodo di crittografia appropriato per i dati dall'elenco a discesa *Encryption*. La crittografia consigliata è *3DES*. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.
- 3DES - 3DES (Triple Data Encryption Standard) è un metodo di crittografia semplice a 168 bit. 3DES esegue la crittografia dei dati tre volte, garantendo una maggiore protezione rispetto a DES.

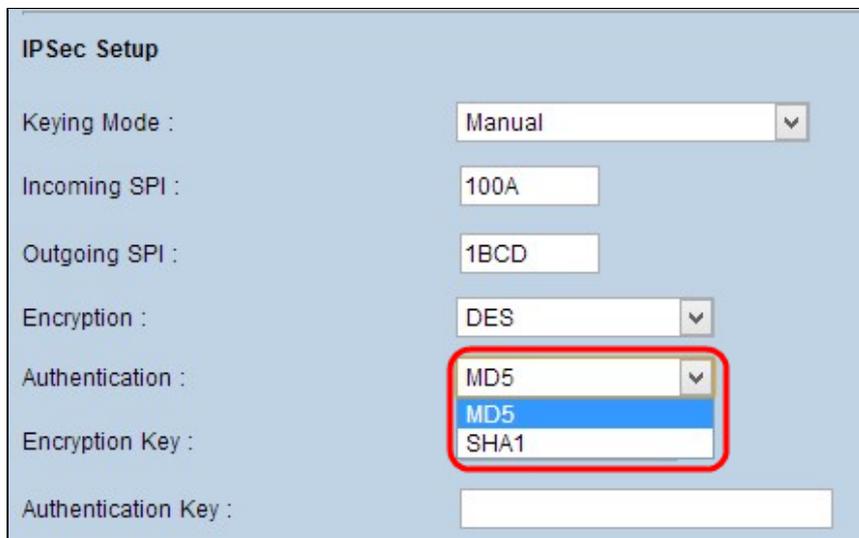
The screenshot shows the "IPSec Setup" section of the configuration interface. The "Encryption" dropdown menu is open, showing the following options:

- DES
- DES
- 3DES

A red rectangle highlights the dropdown menu.

Passaggio 4. Selezionare il metodo di autenticazione appropriato per i dati dall'elenco a discesa *Autenticazione*. L'autenticazione consigliata è *SHA1* poiché è più sicura di MD5. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

Encryption Key :

Authentication Key :

Passaggio 5. Immettere la chiave per crittografare e decrittografare i dati nel campo *Chiave di crittografia*. Se si sceglie DES come metodo di crittografia al punto 3, immettere un valore esadecimale a 16 cifre. Se si sceglie 3DES come metodo di cifratura al punto 3, immettere un valore esadecimale di 40 cifre.

Passaggio 6. Immettere una chiave già condivisa per autenticare il traffico nel campo *Chiave di autenticazione*. Se al passaggio 4 si sceglie MD5 come metodo di autenticazione, immettere un valore esadecimale di 32 cifre. Se si sceglie Agente integrità sistema come metodo di autenticazione al passaggio 4, immettere un valore esadecimale di 40 cifre. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.



IPSec Setup

Keying Mode : Manual

Incoming SPI : 100A

Outgoing SPI : 1BCD

Encryption : DES

Authentication : MD5

Encryption Key : ABC12675BC0ACD

Authentication Key : AC67BCD00A12876CB

Passaggio 7. Fare clic su **Save** (Salva) per salvare le impostazioni.

## **IKE con configurazione modalità chiave già condivisa**

Passaggio 1. Selezionare il gruppo DH Fase 1 appropriato dall'elenco a discesa *Gruppo DH Fase 1*. La fase 1 viene utilizzata per stabilire un'associazione di sicurezza logica (SA, Logical Security Association) semplice tra le due estremità del tunnel per supportare la comunicazione di autenticazione protetta. Diffie-Hellman (DH) è un protocollo di scambio di chiave crittografica utilizzato per determinare la forza della chiave durante la fase 1 e condivide inoltre la chiave segreta per autenticare la comunicazione.

- Gruppo 1 - 768 bit - Chiave con il livello di protezione più basso e gruppo di autenticazione con il livello di protezione più basso. Ma serve meno tempo per calcolare le chiavi IKE. Questa opzione è preferibile se la velocità della rete è bassa.
- Gruppo 2 - 1024 bit - Chiave di maggiore potenza e gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.
- Gruppo 5 - 1536 bit - Rappresenta la chiave con il livello di protezione più alto e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : MD5

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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Passaggio 2. Selezionare la crittografia appropriata per la fase 1 dall'elenco a discesa *Crittografia fase 1*. Si consiglia 3DES in quanto rappresenta il metodo di crittografia più sicuro. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.
- 3DES - 3DES (Triple Data Encryption Standard) è un metodo di crittografia semplice a 168 bit. 3DES esegue la crittografia dei dati tre volte, garantendo una maggiore protezione rispetto a DES.
- AES-128 - Advanced Encryption Standard (AES) è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.
- AES-192 - Advanced Encryption Standard (AES) è un metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 12 cicli. AES-192 è più sicuro di AES-128.
- AES-256 - Advanced Encryption Standard (AES) è un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli. AES-256 è il metodo di crittografia più sicuro.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : DES

Phase 1 SA Life Time : 3600 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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Passaggio 3. Selezionare il metodo di autenticazione appropriato per la Fase 1 dall'elenco a discesa *Autenticazione fase 1*. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.

**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 : 3600 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 :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Passaggio 4. Immettere, in secondi, il periodo di tempo durante il quale le chiavi della fase 1 sono valide e il tunnel VPN rimane attivo nel campo *Durata associazione di protezione fase 1*.

Passaggio 5. Selezionare la casella di controllo **Perfect Forward Secrecy** per proteggere ulteriormente le chiavi. Questa opzione consente al router di generare una nuova chiave se una chiave viene compromessa. I dati crittografati vengono compromessi solo tramite la chiave compromessa. In questo modo la comunicazione risulta più sicura e autenticata, poiché protegge altre chiavi anche se compromesse. Si tratta di un'azione consigliata in quanto offre maggiore protezione.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Passaggio 6. Selezionare il gruppo DH Fase 2 appropriato dall'elenco a discesa *Gruppo DH Fase 2*. La fase 2 utilizza l'associazione di sicurezza e viene utilizzata per determinare la sicurezza del pacchetto dati durante il passaggio dei pacchetti dati attraverso i due endpoint.

- Gruppo 1 - 768 bit - Rappresenta la chiave con il livello di protezione più basso e il gruppo di autenticazione con il livello di protezione più basso. Ma ha bisogno di meno tempo per calcolare le chiavi IKE. È preferibile se la velocità della rete è bassa.
- Gruppo 2 - 1024 bit - Rappresenta una chiave di livello superiore e un gruppo di autenticazione più sicuro. Ma ha bisogno di un po' di tempo per calcolare le chiavi IKE.
- Gruppo 5 - 1536 bit - Rappresenta la chiave con il livello di protezione più alto e il gruppo di autenticazione più sicuro. È necessario più tempo per calcolare i tasti IKE. È preferibile se la velocità della rete è elevata.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : MD5

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Advanced +

Passaggio 7. Selezionare la crittografia appropriata per la fase 2 dall'elenco a discesa *Crittografia fase 2*. Si consiglia l'AES-256 perché è il metodo di crittografia più sicuro. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES - Data Encryption Standard (DES) utilizza una chiave a 56 bit per la crittografia dei dati. DES è obsoleto e deve essere utilizzato solo se un endpoint supporta solo DES.
- 3DES - 3DES (Triple Data Encryption Standard) è un metodo di crittografia semplice a 168 bit. 3DES esegue la crittografia dei dati tre volte, garantendo una maggiore protezione rispetto a DES.
- AES-128 - Advanced Encryption Standard (AES) è un metodo di crittografia a 128 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 10 cicli.
- AES-192 - Advanced Encryption Standard (AES) è un metodo di crittografia a 192 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 12 cicli. AES-192 è più sicuro di AES-128.
- AES-256 - Advanced Encryption Standard (AES) è un metodo di crittografia a 256 bit che trasforma il testo normale in testo cifrato attraverso ripetizioni di 14 cicli. AES-256 è il metodo di crittografia più sicuro.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : **DES**

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Passaggio 8. Selezionare il metodo di autenticazione appropriato dall'elenco a discesa *Autenticazione fase 2*. Il tunnel VPN deve utilizzare lo stesso metodo di autenticazione per entrambe le estremità.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 32 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.
- Null - Non viene utilizzato alcun metodo di autenticazione.

**IPSec Setup**

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : DES

Phase 1 Authentication : SHA1

Phase 1 SA Life Time : 27600 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 :

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter : 

Advanced +

Passaggio 9. Immettere, in secondi, il periodo di tempo durante il quale le chiavi della fase 2 sono valide e il tunnel VPN rimane attivo nel campo *Durata associazione di sicurezza fase 2*.

Passaggio 10. Immettere una chiave condivisa in precedenza tra i peer IKE per autenticare i peer nel campo *Chiave già condivisa*. È possibile utilizzare fino a 30 caratteri esadecimali come chiave già condivisa. Il tunnel VPN deve utilizzare la stessa chiave già condivisa per entrambe le estremità.

**Nota:** si consiglia di modificare frequentemente la chiave già condivisa tra peer IKE in modo che la VPN rimanga protetta.

Passaggio 11. Selezionare la casella di controllo **Complessità minima chiave già condivisa** se si desidera attivare il misuratore di intensità per la chiave già condivisa. Viene utilizzato per determinare l'intensità della chiave già condivisa tramite le barre di colore

**Nota:** il *misuratore dell'intensità della chiave già condivisa* mostra l'intensità della chiave già condivisa tramite barre colorate. Il rosso indica una forza debole, il giallo indica una forza accettabile e il verde indica una forza forte.

**IPSec Setup**

Keying Mode :

Phase 1 DH Group :

Phase 1 Encryption :

Phase 1 Authentication :

Phase 1 SA Life Time :  seconds

Perfect Forward Secrecy :

Phase 2 DH Group :

Phase 2 Encryption :

Phase 2 Authentication :

Phase 2 SA Life Time :  seconds

Preshared Key :

Minimum Preshared Key Complexity :  Enable

Preshared Key Strength Meter :

Passaggio 12. Fare clic su **Save** (Salva) per salvare le impostazioni.

### Configurazione IKE avanzata con modalità chiave già condivisa

Passaggio 1. Fare clic su **Avanzate** per visualizzare le impostazioni avanzate di IKE con chiave già condivisa.

**Advanced**

Aggressive Mode

Compress (Support IP Payload Compression Protocol(IPComp))

Keep-Alive

AH Hash Algorithm

NetBIOS Broadcast

NAT Traversal

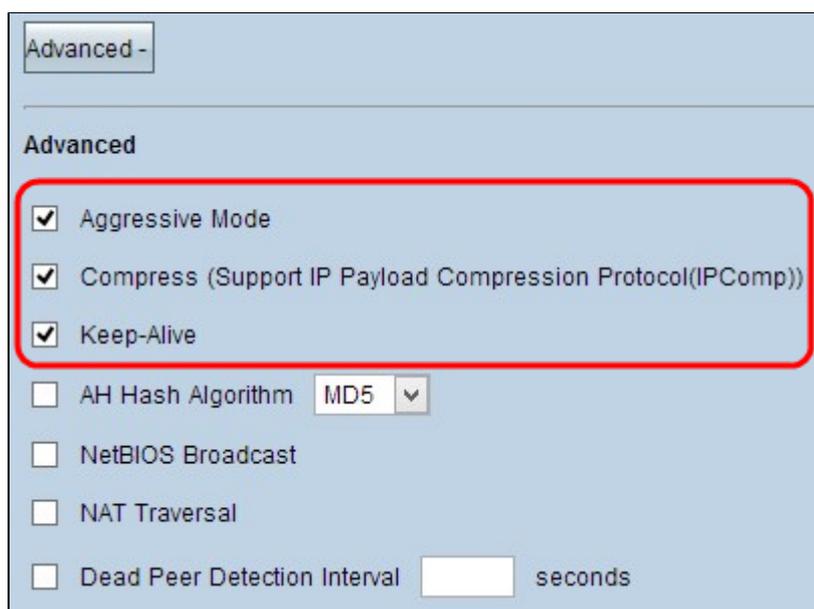
Dead Peer Detection Interval  seconds

Passaggio 2. Selezionare la casella di controllo **Modalità aggressiva** se la velocità di rete è bassa. In questo modo gli ID dei punti finali del tunnel vengono scambiati in testo non crittografato durante la connessione SA (fase 1), che richiede meno tempo per lo scambio ma è meno sicuro.

**Nota:** la modalità aggressiva non è disponibile per la connessione VPN da client a gateway di gruppo.

Passaggio 3. Per comprimere le dimensioni dei datagrammi IP, selezionare la casella di controllo **Comprimi (Support IP Payload Compression Protocol (IPComp))**. IPComp è un protocollo di compressione IP utilizzato per comprimere le dimensioni del datagramma IP. La compressione IP è utile se la velocità della rete è bassa e l'utente desidera trasmettere rapidamente i dati senza alcuna perdita attraverso la rete lenta, ma non fornisce alcuna protezione.

Passaggio 4. Selezionare la casella di controllo **Keep-Alive** se si desidera che la connessione del tunnel VPN rimanga sempre attiva. Keep Alive consente di ristabilire immediatamente le connessioni nel caso in cui una connessione diventi inattiva.



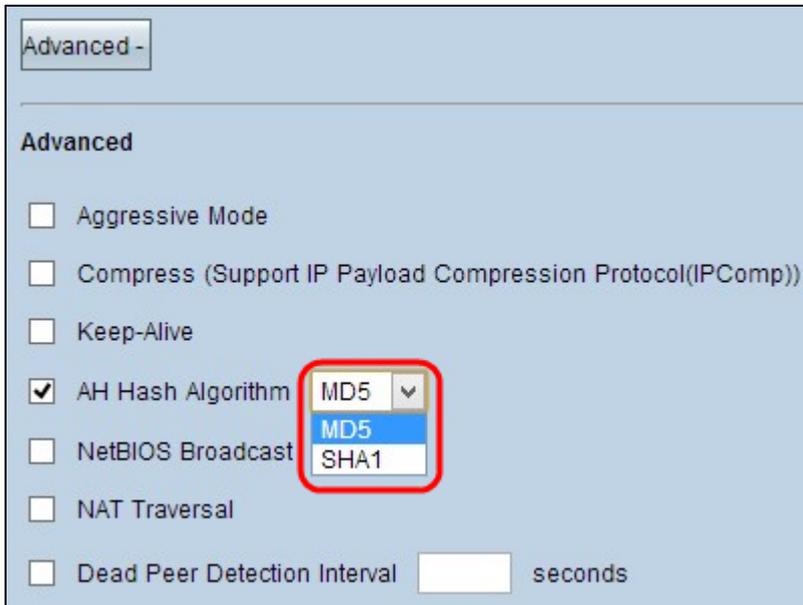
Advanced -

Advanced

- Aggressive Mode
- Compress (Support IP Payload Compression Protocol(IPComp))
- Keep-Alive
- AH Hash Algorithm MD5
- NetBIOS Broadcast
- NAT Traversal
- Dead Peer Detection Interval seconds

Passaggio 5. Selezionare la casella di controllo **AH Hash Algorithm** se si desidera abilitare Authenticate Header (AH). AH fornisce l'autenticazione ai dati di origine, l'integrità dei dati tramite checksum e la protezione nell'intestazione IP. Il tunnel deve avere lo stesso algoritmo per entrambi i lati.

- MD5 - Message Digest Algorithm-5 (MD5) rappresenta una funzione hash esadecimale a 128 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.
- SHA1 - Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.

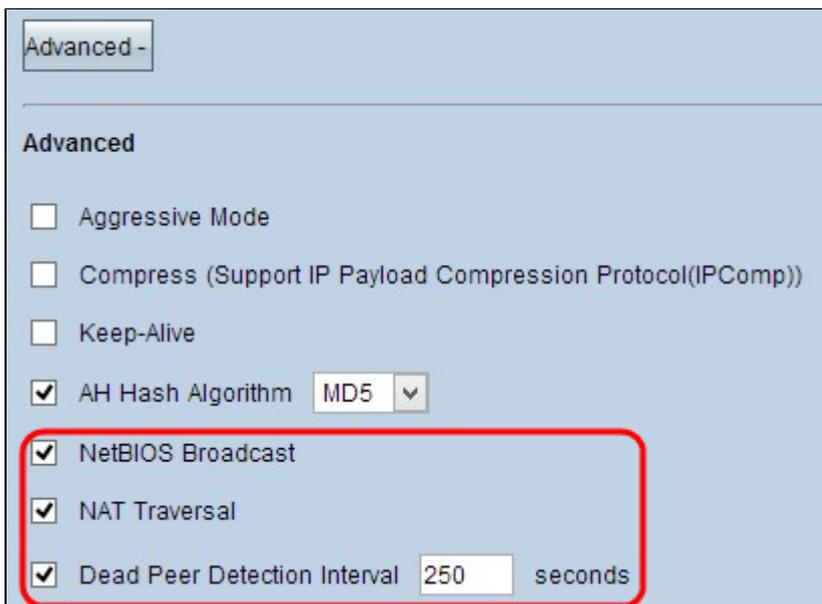


Passaggio 6. Selezionare **NetBIOS Broadcast** per consentire il traffico non instradabile attraverso il tunnel VPN. L'opzione di default è deselezionata. NetBIOS viene utilizzato per rilevare risorse di rete come stampanti, computer e così via nella rete tramite alcune applicazioni software e funzionalità di Windows come Risorse di rete.

Passaggio 7. Selezionare la casella di controllo **NAT Traversal** se si desidera accedere a Internet dalla LAN privata tramite un indirizzo IP pubblico. Se il router VPN è dietro un gateway NAT, selezionare questa casella di controllo per abilitare l'attraversamento NAT. Entrambe le estremità del tunnel devono avere le stesse impostazioni.

Passaggio 8. Selezionare **Dead Peer Detection Interval** per verificare periodicamente la vivacità del tunnel VPN tramite hello o ACK. Se si seleziona questa casella di controllo, immettere la durata o l'intervallo desiderato per i messaggi di benvenuto.

**Nota:** è possibile configurare l'intervallo di rilevamento peer inattivi solo per la connessione VPN da client a gateway singolo e non per la connessione VPN da client a gateway di gruppo.



Passaggio 9. Fare clic su **Save** (Salva) per salvare le impostazioni.

Ora è stato spiegato come configurare il tunnel VPN di accesso remoto da client a gateway sui router VPN RV016, RV042, RV042G e RV082.

## 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).