

Configurazione di una VPN da gateway a gateway su router VPN RV016, RV042, RV042G e RV082

Obiettivo

Una rete VPN (Virtual Private Network) viene utilizzata per formare una connessione protetta tra due endpoint su un'Internet pubblica o condivisa tramite quello che viene definito tunnel VPN. In particolare, una connessione VPN da gateway a gateway consente a due router di connettersi in modo sicuro tra loro e al client di un'estremità di apparire logicamente come se facessero parte della rete dell'altra estremità. In questo modo è possibile condividere dati e risorse su Internet in modo più semplice e sicuro.

Per abilitare una VPN da gateway a gateway, è necessario eseguire la configurazione su entrambi i router. Le configurazioni eseguite nelle sezioni *Local Group Setup* e *Remote Group Setup* devono essere invertite tra i due router in modo che il gruppo locale di uno sia il gruppo remoto dell'altro.

L'obiettivo di questo documento è spiegare come configurare la VPN da gateway a gateway sui router VPN serie RV016, RV042, RV042G e RV082.

Dispositivi interessati

RV016
RV042
RV042G
RV082

Versione del software

·v4.2.2.08

Configurare la VPN da Gateway a Gateway

Passaggio 1. Accedere all'utility di configurazione del router e scegliere **VPN > Gateway to Gateway**. Viene visualizzata la pagina *Gateway to Gateway*:

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

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 Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

Per configurare la VPN da gateway a gateway, è necessario configurare le seguenti funzionalità:

1. [Aggiungere un nuovo tunnel](#)
2. [Configurazione gruppo locale](#)
3. [Configurazione gruppo remoto](#)
4. [Configurazione IPSec](#)

Aggiungi nuovo tunnel

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

Tunnel Name :

Interface :

Enable :

Nr. tunnel è un campo di sola lettura che visualizza il tunnel corrente che verrà creato.

Passaggio 1. Immettere un nome per il tunnel VPN nel campo Nome tunnel. Non deve necessariamente corrispondere al nome utilizzato sull'altra estremità del tunnel.

Passaggio 2. Dall'elenco a discesa Interface (Interfaccia), selezionare la porta WAN (Wide Area Network) da utilizzare per il tunnel.

·WAN1: la porta WAN dedicata dei router VPN serie RV0XX.

·WAN2: la porta WAN2/DMZ dei router VPN serie RV0XX. Viene visualizzato nel menu a discesa solo se è stato configurato come WAN e non come porta DMZ (Demilitarize Zone).

Passaggio 3. (Facoltativo) Per abilitare la VPN, selezionare la casella di controllo nel campo **Abilita**. La VPN è abilitata per impostazione predefinita.

Installazione gruppo locale

Nota: La configurazione per l'installazione del gruppo locale su un router deve essere la stessa di quella per l'installazione del gruppo remoto sull'altro router.

Gateway To Gateway

Add a New Tunnel

Tunnel No. 2

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 :

Passaggio 1. Per stabilire un tunnel VPN, scegliere il metodo di identificazione del router

appropriato dall'elenco a discesa Tipo di gateway di sicurezza locale.

- Solo IP: il router locale (questo router) viene riconosciuto da un indirizzo IP statico. È possibile scegliere questa opzione solo se il router ha un IP WAN statico. L'indirizzo IP statico WAN viene visualizzato automaticamente nel campo Indirizzo IP.
- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio. L'indirizzo IP statico WAN viene visualizzato automaticamente nel campo Indirizzo IP.
- Autenticazione IP + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo e-mail nel campo Indirizzo e-mail. L'indirizzo IP statico WAN viene visualizzato automaticamente nel campo Indirizzo IP.
- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.
- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'indirizzo e-mail nel campo Indirizzo e-mail.

Passaggio 2. 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 può accedere al tunnel VPN. Se si sceglie questa opzione, immettere l'indirizzo IP del dispositivo LAN nel campo Indirizzo IP.
- Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP della subnet mask 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.

Passaggio 3. Fare clic su **Save** per salvare le impostazioni.

Installazione gruppo remoto

Nota: La configurazione per l'installazione del gruppo remoto su un router deve essere la stessa di quella per l'installazione del gruppo locale sull'altro router.

Local Group Setup

Local Security Gateway Type :

Email Address : @

IP Address :

Local Security Group Type :

IP Address :

Remote Group Setup

Remote Security Gateway Type :

:

Remote Security Group Type :

IP Address :

Subnet Mask :

Passaggio 1. Dall'elenco a discesa Tipo di gateway di sicurezza remoto, scegliere il metodo per identificare il router remoto per stabilire il tunnel VPN.

- Solo IP: l'accesso al tunnel è possibile attraverso un indirizzo IP WAN statico. Se si conosce l'indirizzo IP del router remoto, scegliere Indirizzo IP dall'elenco a discesa visualizzato sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo IP. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto.

- Autenticazione IP + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP statico e un dominio registrato per il router. Se si conosce l'indirizzo IP del router remoto, scegliere Indirizzo IP nell'elenco a discesa direttamente sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto. Immettere il nome di dominio del router nel campo Nome dominio indipendentemente dal metodo scelto per identificarlo.

- Autenticazione indirizzo IP + e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP statico e un indirizzo e-mail. Se si conosce l'indirizzo IP del router remoto, scegliere Indirizzo IP nell'elenco a discesa direttamente sotto il campo Tipo di gateway di sicurezza remoto e immettere l'indirizzo. Scegliere IP da DNS risolto se non si conosce l'indirizzo IP ma si conosce il nome di dominio e immettere il nome di dominio del router nel campo IP da DNS risolto. Immettere l'indirizzo di posta elettronica nel campo Indirizzo di posta elettronica.

- Autenticazione IP dinamico + nome di dominio (FQDN): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un dominio registrato. Se si sceglie questa opzione, immettere il nome del dominio registrato nel campo Nome dominio.

- Autenticazione IP dinamico + indirizzo e-mail (FQDN UTENTE): è possibile accedere al tunnel tramite un indirizzo IP dinamico e un indirizzo e-mail. Se si sceglie questa opzione, immettere l'Indirizzo e-mail nel campo Indirizzo e-mail.

Passaggio 2. Selezionare l'utente LAN remoto o il gruppo di utenti appropriato che può

accedere al tunnel VPN dall'elenco a discesa Tipo di gruppo di sicurezza remoto.

·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.

·Subnet: tutti i dispositivi LAN su una subnet specifica possono accedere al tunnel. Se si sceglie questa opzione, immettere l'indirizzo IP della subnet mask e la subnet mask dei dispositivi LAN rispettivamente nei campi Indirizzo IP e Subnet mask.

·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.

Nota: I due router alle estremità del tunnel non possono trovarsi nella stessa subnet.

Passaggio 3. Fare clic su **Save** per salvare le impostazioni.

Installazione di IPsec

IPsec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 1 - 768 bit

Phase 1 Encryption : DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 28800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit

Phase 2 Encryption : DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter :

Advanced +

Save Cancel

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: Per funzionare correttamente, entrambe le estremità della VPN devono avere gli stessi metodi di crittografia, decrittografia e autenticazione. Immettere le stesse impostazioni di

configurazione IPSec per entrambi i router.

IPSec Setup

Keying Mode : IKE with Preshared key
Manual
IKE with Preshared key

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 1. Scegliere 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](#): una modalità di protezione personalizzata che consente di generare una nuova chiave di protezione autonomamente e non prevede alcuna negoziazione con la chiave. È la soluzione migliore da utilizzare durante la risoluzione dei problemi e in un ambiente statico di piccole dimensioni.

·[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.

Impostazione IPSec per la modalità di impostazione manuale

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Passaggio 1. Immettere il valore esadecimale univoco per l'indice dei parametri di sicurezza (SPI) in ingresso nel campo SPI in ingresso. Lo SPI è contenuto nell'intestazione ESP (Encapsulating Security Payload Protocol) e determina la protezione del pacchetto in arrivo. È possibile immettere un valore compreso tra 100 e 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. È possibile immettere un valore compreso tra 100 e ffffffff. L'SPI in uscita del router remoto deve corrispondere all'SPI in entrata del router locale.

Nota: Nessun tunnel può avere lo stesso SPI.

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

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

- DES: lo standard DES (Data Encryption Standard) 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: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia a 168 bit. 3DES esegue la crittografia dei dati tre volte, garantendo una maggiore protezione rispetto a DES.

IPSec Setup

Keying Mode :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

Encryption Key :

Authentication Key :

Passaggio 4. Scegliere il metodo di autenticazione appropriato per i dati dall'elenco a discesa Autenticazione. L'autenticazione consigliata è SHA1 perché 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) è una funzione hash a 128 bit 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 :

Incoming SPI :

Outgoing SPI :

Encryption :

Authentication :

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 si sceglie MD5 come metodo di autenticazione al passaggio 4, immettere un valore esadecimale a 32 cifre. Se si sceglie SHA1 come metodo di autenticazione al punto 4, immettere un valore esadecimale di 40 cifre. Se non si aggiunge un numero sufficiente di cifre, gli zeri verranno aggiunti alla fine fino a quando il numero di cifre non sarà sufficiente. Il tunnel VPN deve utilizzare la stessa chiave precondivisa per entrambi gli endpoint.

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

IKE con configurazione modalità chiave già condivisa

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 :

Passaggio 1. Scegliere 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: la chiave con il livello di protezione più basso e il gruppo di autenticazione con il livello di protezione più basso, ma che richiede la quantità di tempo minore per il calcolo delle chiavi IKE. Questa opzione è preferibile se la velocità della rete è bassa.
- Gruppo 2 - 1024 bit: una chiave di livello superiore e un gruppo di autenticazione più sicuro rispetto al gruppo 1, ma il calcolo delle chiavi IKE richiede più tempo.
- Gruppo 5 - 1536 bit: la chiave con il livello di protezione più elevato 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 : 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 2. Scegliere la crittografia appropriata per la fase 1 per cifrare la chiave dall'elenco a discesa Crittografia fase 1. Si consigliano AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

- DES: lo standard DES (Data Encryption Standard) 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: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia 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 : 3DES

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 :

Passaggio 3. Scegliere 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. Si consiglia SHA1.

·MD5 — Message Digest Algorithm-5 (MD5) è una funzione hash a 128 bit 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 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 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 4. Immettere il periodo di tempo in secondi durante il quale le chiavi della fase 1 sono valide e il tunnel VPN rimane attivo nel campo Durata ASA 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. Si tratta di un'azione consigliata in quanto offre maggiore protezione.

IPSec Setup

Keying Mode : IKE with Preshared key

Phase 1 DH Group : Group 2 - 1024 bit

Phase 1 Encryption : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 1 - 768 bit


Phase 2 Encryption : 3DES

Phase 2 Authentication : MD5

Phase 2 SA Life Time : 3600 seconds

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Passaggio 6. Scegliere 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 mentre passa attraverso i due endpoint.

- Gruppo 1 - 768 bit: la chiave con il livello di protezione più basso e il gruppo di autenticazione con il livello di protezione più basso, ma che richiede la quantità di tempo minore per il calcolo delle chiavi IKE. Questa opzione è preferibile se la velocità della rete è bassa.
- Gruppo 2 - 1024 bit: una chiave di livello superiore e un gruppo di autenticazione più sicuro rispetto al gruppo 1, ma richiede più tempo per il calcolo delle chiavi IKE.
- Gruppo 5 - 1536 bit: la chiave con il livello di protezione più elevato 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 : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 bit

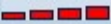
Phase 2 Encryption : **DES**

Phase 2 Authentication :

Phase 2 SA Life Time :

Preshared Key :

Minimum Preshared Key Complexity : Enable

Preshared Key Strength Meter : 

Passaggio 7. Scegliere la crittografia appropriata per la fase 2 per crittografare la chiave dall'elenco a discesa Crittografia fase 2. Si consigliano AES-128, AES-192 o AES-256. Il tunnel VPN deve utilizzare lo stesso metodo di crittografia per entrambe le estremità.

·NULL — Non viene utilizzata alcuna crittografia.

·DES: lo standard DES (Data Encryption Standard) 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: Triple Data Encryption Standard (3DES) è un semplice metodo di crittografia 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 tramite 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 : 3DES

Phase 1 Authentication : MD5

Phase 1 SA Life Time : 27800 seconds

Perfect Forward Secrecy :

Phase 2 DH Group : Group 2 - 1024 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 :

Passaggio 8. Scegliere 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. Si consiglia SHA1.

- MD5 — Message Digest Algorithm-5 (MD5) è una funzione hash esadecimale a 128 bit 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 :

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 9. Immettere il periodo di tempo in secondi durante il quale le chiavi della fase 2 sono valide e il tunnel VPN rimane attivo nel campo Durata associazione di protezione 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 i peer IKE in modo che la VPN rimanga protetta.

Passaggio 11. (Facoltativo) Se si desidera abilitare il misuratore di affidabilità per la chiave già condivisa, selezionare la casella di controllo **Complessità minima chiave già condivisa**. Viene utilizzato per determinare la forza della chiave già condivisa tramite le barre di colore.

·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.

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

Nota: Per configurare le opzioni disponibili nella sezione *Avanzate* per la VPN da gateway a gateway, consultare l'articolo [Configurazione delle impostazioni avanzate per la VPN da gateway 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).