Configurazione tunnel VPN su RV016, RV042, RV042G e RV082 VPN Router

Obiettivo

Una rete VPN (Virtual Private Network) è una connessione protetta tra due endpoint. Una rete privata, che invia i dati in modo sicuro tra queste due posizioni o reti, viene stabilita da un tunnel VPN. Un tunnel VPN connette due PC o due reti e consente la trasmissione dei dati su Internet come se gli endpoint fossero all'interno di una rete. VPN è una buona soluzione per le aziende che hanno dipendenti che devono viaggiare o rimanere spesso al di fuori della LAN. Con la VPN, questi dipendenti possono accedere alla LAN e utilizzare le risorse disponibili per svolgere il proprio lavoro. Inoltre, la VPN può connettere due o più siti, in modo che le società con filiali diverse possano comunicare tra loro.

Nota: La serie RV Wired Router offre due tipi di VPN, da gateway a gateway e da client a gateway. Affinché la connessione VPN funzioni correttamente, i valori IPSec su entrambi i lati della connessione devono essere uguali. Inoltre, entrambi i lati della connessione devono appartenere a LAN diverse. I passaggi successivi spiegano come configurare la VPN sulla serie RV Wired Router.

Ai fini di questo articolo, la configurazione VPN sarà da Gateway a Gateway.

Questo articolo spiega come configurare un tunnel VPN su router VPN RV016 RV042, RV042G e RV082.

Dispositivi interessati

RV016
RV042
RV042G
RV082

Versione del software

·v4.2.1.02

Configurazione VPN

Passaggio 1. Accedere alla pagina Web Configuration Utility e scegliere **VPN > Gateway to Gateway**. Viene visualizzata la pagina *Gateway to Gateway*:

Nota: Per configurare un client per il tunnel VPN del gateway, scegliere **VPN > Da client a gateway**.

Gateway To Gateway

Add a New Tunnel

Tunnel No.	1
Tunnel Name :	TestTunnel
Interface :	WAN1
Enable :	☑

Local Group Setup

Local Security Gateway Type :	IP Only
IP Address :	156.26.31.119
Local Security Group Type :	Subnet
IP Address :	192.168.1.0
Subnet Mask :	255.255.255.0

Remote Group Setup

Remote Security Gateway Type :	IP Only
IP Address :	192.0.2.2
Remote Security Group Type :	Subnet
IP Address :	192.168.2.0
Subnet Mask :	255.255.255.0

IPSec Setup

Keying Mode :	IKE with Preshared key
Phase 1 DH Group :	Group 1 - 768 bit
Phase 1 Encryption :	DES
Phase 1 Authentication :	MD5
Phase 1 SA Life Time :	28800 seconds
Perfect Forward Secrecy :	☑
Phase 2 DH Group :	Group 1 - 768 bit
Phase 2 Encryption :	DES
Phase 2 Authentication :	MD5

Passaggio 2. Nel campo Nome tunnel, immettere il nome del tunnel VPN.

Passaggio 3. Nell'elenco a discesa Interfaccia, scegliere una delle interfacce WAN disponibili. Questa è l'interfaccia che stabilirà il tunnel VPN con l'altro lato.

Passaggio 4. In Local Group Setup, nell'elenco a discesa Local Security Gateway Type, scegliere una delle opzioni elencate:

·Solo IP: scegliere questa opzione se il router è configurato con un indirizzo IP statico per la connettività Internet.

·Autenticazione IP + nome di dominio (FQDN) — Scegliere questa opzione se il router è configurato con un indirizzo IP statico e un nome di dominio registrato per la connettività Internet.

·Autenticazione IP + indirizzo e-mail (FQDN utente): scegliere questa opzione se il router è configurato con un indirizzo IP statico per la connettività Internet e per l'autenticazione verrà utilizzato un indirizzo e-mail.

·Autenticazione IP dinamico + nome di dominio (FQDN) — Scegliere questa opzione se il router è configurato con un indirizzo IP dinamico e per l'autenticazione verrà utilizzato un nome di dominio dinamico.

·Autenticazione IP dinamico + indirizzo di posta elettronica (FQDN utente): scegliere questa opzione se il router dispone di un indirizzo IP dinamico per la connettività Internet, ma non dispone di un nome di dominio dinamico per l'autenticazione e verrà utilizzato un indirizzo di posta elettronica per l'autenticazione.

Passaggio 5. In Configurazione gruppo locale, nell'elenco a discesa Tipo gruppo di sicurezza locale, scegliere una delle opzioni seguenti:

·Indirizzo IP - Questa opzione consente di specificare un dispositivo che può utilizzare il tunnel VPN. È sufficiente immettere l'indirizzo IP del dispositivo.

·Subnet: scegliere questa opzione per consentire a tutti i dispositivi che appartengono alla stessa subnet di utilizzare il tunnel VPN. Immettere l'indirizzo IP di rete e la relativa subnet mask.

·Intervallo IP: scegliere questa opzione per specificare un intervallo di dispositivi che possono usare il tunnel VPN. Specificare il primo e l'ultimo indirizzo IP dell'intervallo di dispositivi.

Passaggio 6. In Configurazione gruppo remoto, nell'elenco a discesa Tipo gateway di sicurezza locale remota scegliere una delle opzioni seguenti:

·Solo IP: scegliere questa opzione se il router è configurato con un indirizzo IP statico per la connettività Internet.

·Autenticazione IP + nome di dominio (FQDN) — Scegliere questa opzione se il router è configurato con un indirizzo IP statico e un nome di dominio registrato per la connettività Internet.

·Autenticazione IP + indirizzo e-mail (FQDN utente): scegliere questa opzione se il router è configurato con un indirizzo IP statico per la connettività Internet e per l'autenticazione verrà utilizzato un indirizzo e-mail.

·Autenticazione IP dinamico + nome di dominio (FQDN) — Scegliere questa opzione se il router è configurato con un indirizzo IP dinamico e per l'autenticazione verrà utilizzato un nome di dominio dinamico.

·Autenticazione IP dinamico + indirizzo di posta elettronica (FQDN utente): scegliere questa opzione se il router dispone di un indirizzo IP dinamico per la connettività Internet, ma non dispone di un nome di dominio dinamico per l'autenticazione e verrà utilizzato un indirizzo di posta elettronica per l'autenticazione.

Passaggio 7. Se si sceglie Solo IP come tipo di gateway di sicurezza locale remoto, scegliere una delle seguenti opzioni dall'elenco a discesa:

·IP - Selezionare questa opzione per immettere l'indirizzo IP nel campo adiacente.

·IP da DNS risolto: scegliere questa opzione se non si conosce l'indirizzo IP del gateway remoto, quindi immettere il nome dell'altro router nel campo adiacente.

Passaggio 8. In Configurazione gruppo remoto, nell'elenco a discesa Tipo gruppo di sicurezza remoto, scegliere una delle opzioni seguenti:

·Indirizzo IP - Questa opzione consente di specificare un dispositivo che può utilizzare il tunnel VPN. È sufficiente immettere l'indirizzo IP del dispositivo.

·Subnet: scegliere questa opzione per consentire a tutti i dispositivi che appartengono alla stessa subnet di utilizzare il tunnel VPN. Immettere l'indirizzo IP di rete e la relativa subnet mask.

·Intervallo IP: scegliere questa opzione per specificare un intervallo di dispositivi che possono usare il tunnel VPN. Specificare il primo e l'ultimo indirizzo IP dell'intervallo di dispositivi.

Passaggio 9. In Configurazione IPSec, nell'elenco a discesa Modalità di impostazione chiavi, scegliere una delle opzioni seguenti:

·Manuale - Questa opzione consente di configurare manualmente la chiave anziché negoziarla con l'altro router nella connessione VPN.

·IKE con chiave già condivisa: scegliere questa opzione per abilitare il protocollo IKE (Internet Key Exchange Protocol) che imposta un'associazione di sicurezza nel tunnel VPN. IKE utilizza una chiave già condivisa per autenticare un peer remoto.

Passaggio 10. DH (Diffie - Hellman) è un protocollo di scambio chiave che consente a entrambe le estremità del tunnel VPN di condividere una chiave crittografata. Negli elenchi a discesa Gruppo DH fase 1 e Gruppo DH fase 2 scegliere una delle opzioni seguenti:

·Gruppo 1 - 768 bit: offre una velocità di scambio più elevata, ma una sicurezza inferiore. Se è necessario che la sessione VPN sia veloce e la sicurezza non rappresenta un problema, scegliere questa opzione.

·Gruppo 2 - 1024 bit: offre una maggiore protezione rispetto al gruppo 1, ma richiede più tempo di elaborazione. Si tratta di un'opzione più equilibrata in termini di sicurezza e velocità.

·Gruppo 3 - 1536 bit: offre meno velocità ma maggiore sicurezza. Se la sessione VPN deve essere sicura e la velocità non rappresenta un problema, scegliere questa opzione.

Passaggio 11. Negli elenchi a discesa Crittografia fase 1 e Crittografia fase 2, scegliere una delle opzioni seguenti per la crittografia e la decrittografia della chiave:

·DES: Data Encryption Standard, un algoritmo di base per la crittografia dei dati che codifica la chiave in un pacchetto a 56 bit.

·3DES: Triple Data Encryption Standard, questo algoritmo cripta la chiave in tre pacchetti a 64 bit. È più sicuro di DES.

·AES-128 — Advanced Encryption Standard, questo algoritmo usa la stessa chiave per la crittografia e la decrittografia. Offre maggiore sicurezza rispetto a DES. La sua chiave è di 128 bit

·AES-192: simile a AES-128, ma la sua chiave è di 192 bit.

·AES-256: simile a AES-128, ma con una chiave di 256 bit. Si tratta dell'algoritmo di crittografia più sicuro disponibile.

Passaggio 12. Negli elenchi a discesa Autenticazione fase 1 e Autenticazione fase 2, scegliere una delle seguenti opzioni:

·SHA1: questo algoritmo produce un valore hash di 160 bit. Con questo valore, l'algoritmo verifica l'integrità dei dati scambiati e assicura che i dati non siano stati modificati.

·MD5: è un algoritmo progettato a scopo di autenticazione. Questo algoritmo controlla l'integrità delle informazioni condivise tra le due estremità del tunnel VPN. Genera un valore hash condiviso per autenticare la chiave su entrambe le estremità del tunnel VPN.

Passaggio 13. Nei campi Durata SA fase 1 e Durata SA fase 2, immettere il tempo (in secondi) durante il quale il tunnel VPN è attivo in una fase. Il valore predefinito per la Fase 1 è 2800 secondi. Il valore predefinito per la Fase 2 è 3600 secondi.

Nota: La configurazione della fase 1 e della fase 2 deve essere la stessa su entrambi i router.

Passaggio 14. (Facoltativo) Selezionare la casella di controllo **Perfect Forward Secrecy** per abilitare Perfect Forward Secrecy (PFS). Con PFS, la negoziazione IKE fase 2 genererà nuovi dati per la crittografia e l'autenticazione, che garantiscono una maggiore sicurezza.

Passaggio 15. Nella chiave già condivisa, immettere la chiave che entrambi i router condivideranno per l'autenticazione.

Passaggio 16. (Facoltativo) Selezionare la casella di controllo **Complessità minima chiave già condivisa** per attivare il misuratore di forza della chiave già condivisa, che indica la forza della chiave creata.

Passaggio 17. (Facoltativo) Per configurare opzioni di crittografia più avanzate, fare clic su **Avanzate+**.

Passaggio 18. Fare clic su **Salva per salvare** le configurazioni.

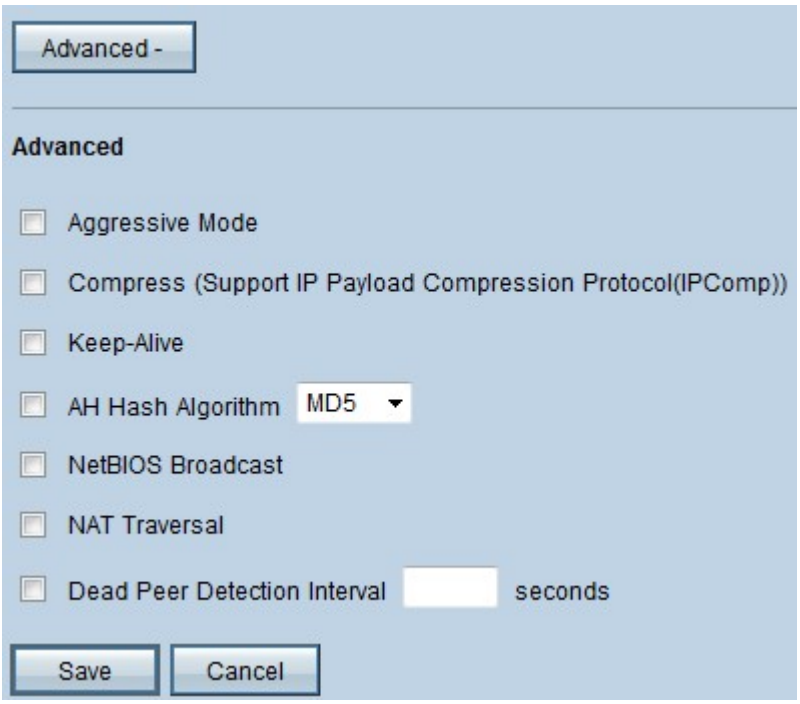
Opzioni VPN avanzate

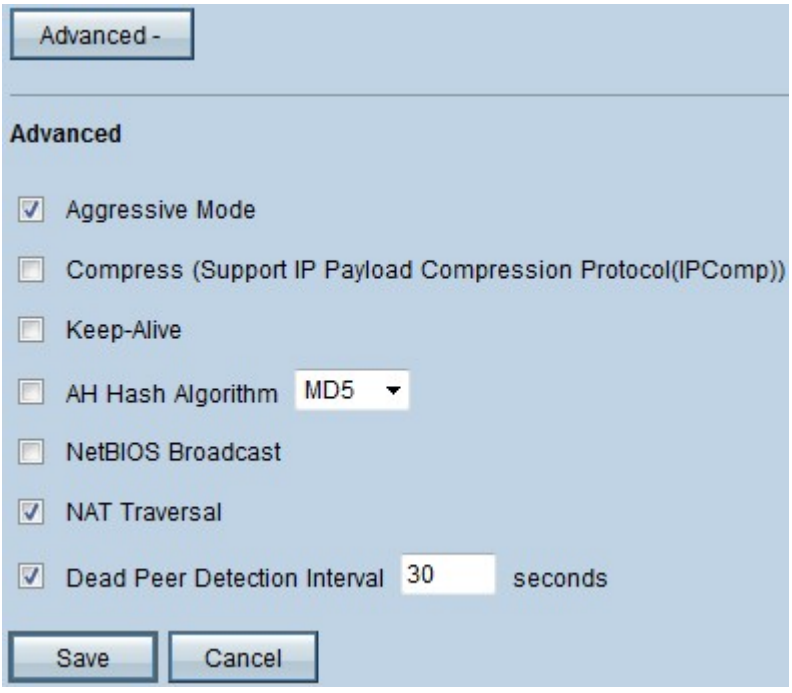
Per aggiungere ulteriori funzionalità alla configurazione della VPN, la serie RV Wired Router offre opzioni avanzate. Queste opzioni migliorano le funzionalità di sicurezza del tunnel VPN.

Queste opzioni sono facoltative, ma se si impostano le opzioni avanzate su un router, assicurarsi di impostare le stesse opzioni sull'altro router. Nella sezione successiva vengono illustrate queste opzioni.

Passaggio 1. Nel campo IPSec fare clic sul pulsante **Advanced+**. Viene visualizzata la pagina *Avanzate*:

Nota: Per configurare le opzioni avanzate del tunnel VPN da client a gateway, scegliere **VPN > Da client a gateway**. Quindi fare clic su **Advanced+**.





L'immagine precedente mostra un esempio di configurazione delle opzioni avanzate.

Passaggio 2. In Avanzate, selezionare le opzioni da aggiungere alla configurazione VPN:

·Modalità aggressiva: con questa opzione, la negoziazione della chiave è più rapida e ciò

riduce la sicurezza. Selezionare la casella di controllo **Modalità aggressiva** per migliorare la velocità del tunnel VPN.

·Compressione (Supporto IP Payload Compression Protocol (IP Comp)): con questa opzione, il protocollo IP Comp riduce le dimensioni dei datagrammi IP. Selezionare la casella di controllo **Comprimi (Support IP Payload Compression Protocol (IP Comp))** per abilitare questa opzione

·Keep Alive: questa opzione tenta di ristabilire la sessione VPN in caso di interruzione. Selezionare la casella di controllo **Keep Alive** per attivare questa opzione.

·AH Hash Algorithm: questa opzione estende la protezione all'intestazione IP per verificare l'integrità dell'intero pacchetto. A tale scopo è possibile utilizzare MD5 o SHA1. Selezionare la casella di controllo **AH Hash Algorithm** e dall'elenco a discesa scegliere MD5 o SHA1 per abilitare l'autenticazione dell'intero pacchetto.

·Trasmissione NetBIOS: protocollo Windows che fornisce informazioni sui diversi dispositivi collegati a una LAN, ad esempio stampanti, computer e file server. In genere, la VPN non trasmette queste informazioni. Selezionare la casella di controllo **NetBIOS Broadcast** per inviare queste informazioni attraverso il tunnel VPN.

·NAT Traversal: Network Address Translation consente agli utenti di una LAN privata di accedere alle risorse Internet utilizzando un indirizzo IP pubblico come indirizzo di origine. Se il router è dietro un gateway NAT, selezionare la casella di controllo **NAT Traversal**.

·Dead Peer Detection Interval: selezionare la casella di controllo **Dead Peer Detection Interval** e immettere (in secondi) l'intervallo prima che il router invii un altro pacchetto per controllare la connettività del tunnel VPN.

Passaggio 3. Fare clic su **Save** (Salva) per salvare le configurazioni.

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).