Configurazione delle impostazioni avanzate per la VPN da gateway a gateway su router VPN RV016, RV042, RV042G e RV082

Obiettivo

Una rete privata virtuale (VPN, Virtual Private Network) è una rete privata utilizzata per connettere virtualmente i dispositivi dell'utente remoto tramite una rete pubblica per garantire la sicurezza. In particolare, una connessione VPN da gateway a gateway consente a due router di connettersi in modo sicuro l'uno all'altro e al client di un'estremità di apparire logicamente come parte della stessa rete remota dell'altra estremità. In questo modo è possibile condividere dati e risorse su Internet in modo più semplice e sicuro. Per stabilire una connessione VPN da gateway a gateway riuscita, è necessario eseguire una configurazione identica su entrambi i lati della connessione.

La configurazione VPN da gateway a gateway avanzata offre la flessibilità necessaria per configurare le configurazioni opzionali per il tunnel VPN in modo da renderlo più intuitivo per gli utenti VPN. Le opzioni Avanzate sono disponibili solo per IKE con modalità chiave già condivisa. Le impostazioni avanzate devono essere le stesse su entrambi i lati della connessione VPN.

L'obiettivo di questo documento è mostrare come configurare le impostazioni avanzate per il tunnel VPN da gateway a gateway sui router VPN RV016, RV042, RV042G e RV082.

Nota: per ulteriori informazioni su come configurare una VPN da gateway a gateway, fare riferimento all'articolo *Configurazione della VPN da gateway a gateway su router VPN RV016, RV042, RV042G e RV082.*

Dispositivi interessati

· RV016
RV042
RV042G
RV082

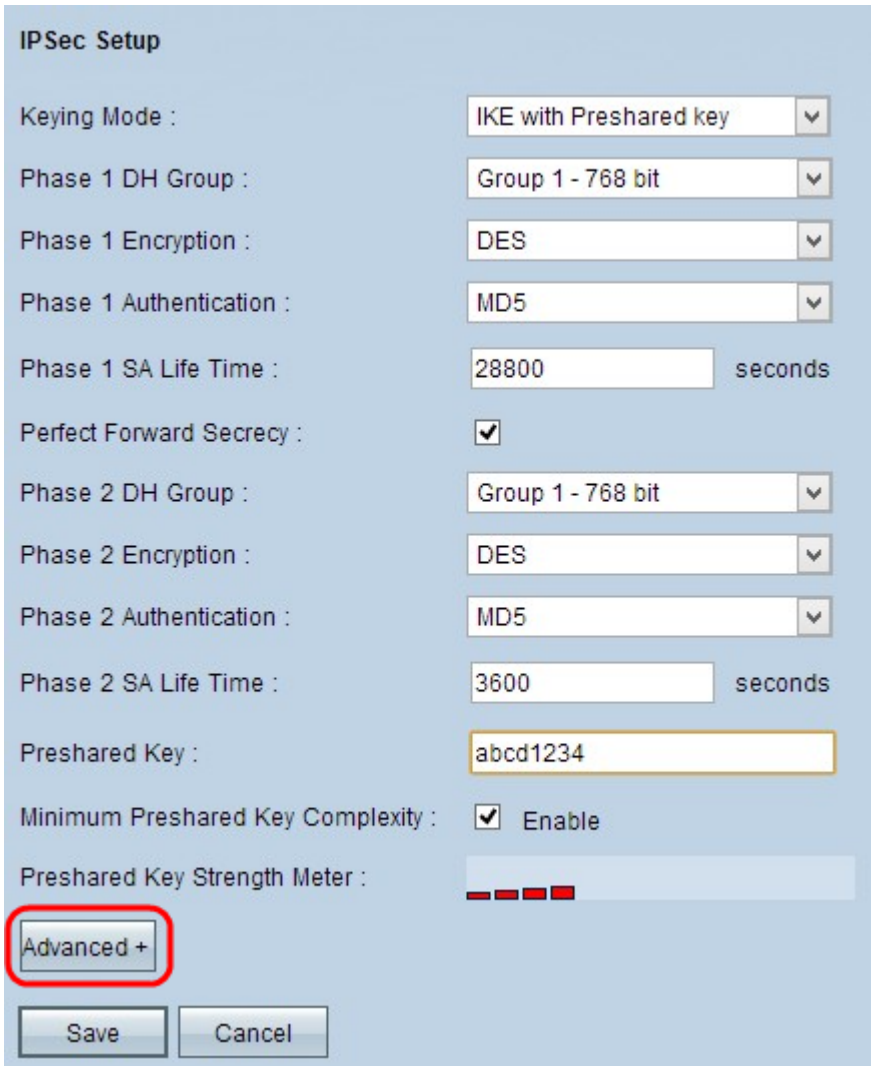
Versione del software

· v4.2.2.08

Configurazione delle impostazioni avanzate per la VPN da gateway a gateway

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

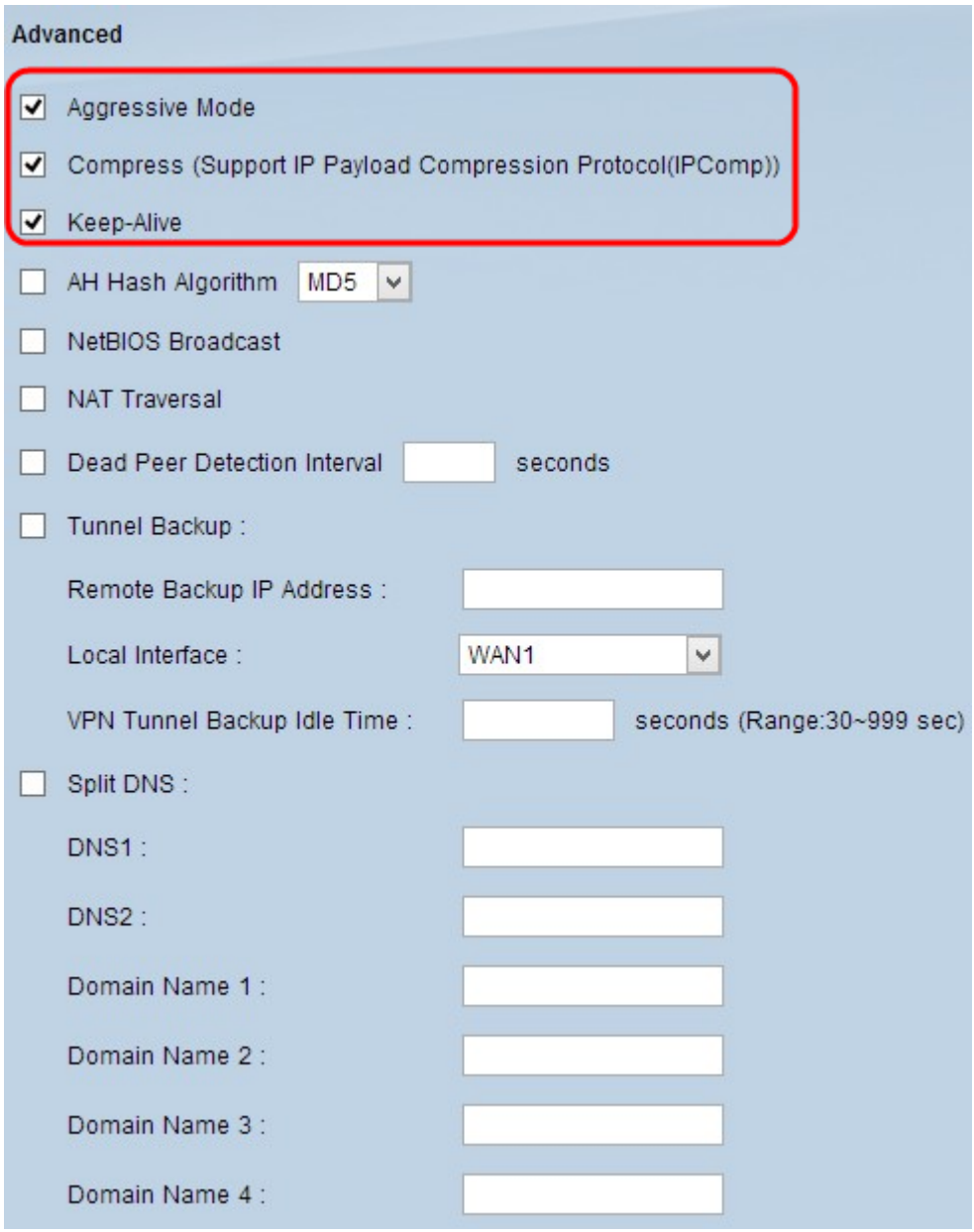
Passaggio 2. Scorrere fino alla sezione *IPSec Setup* e fare clic su **Advanced +**. Viene visualizzata l'area *Avanzate*:



Passaggio 3. 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.

Passaggio 4. 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 dei datagrammi 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.

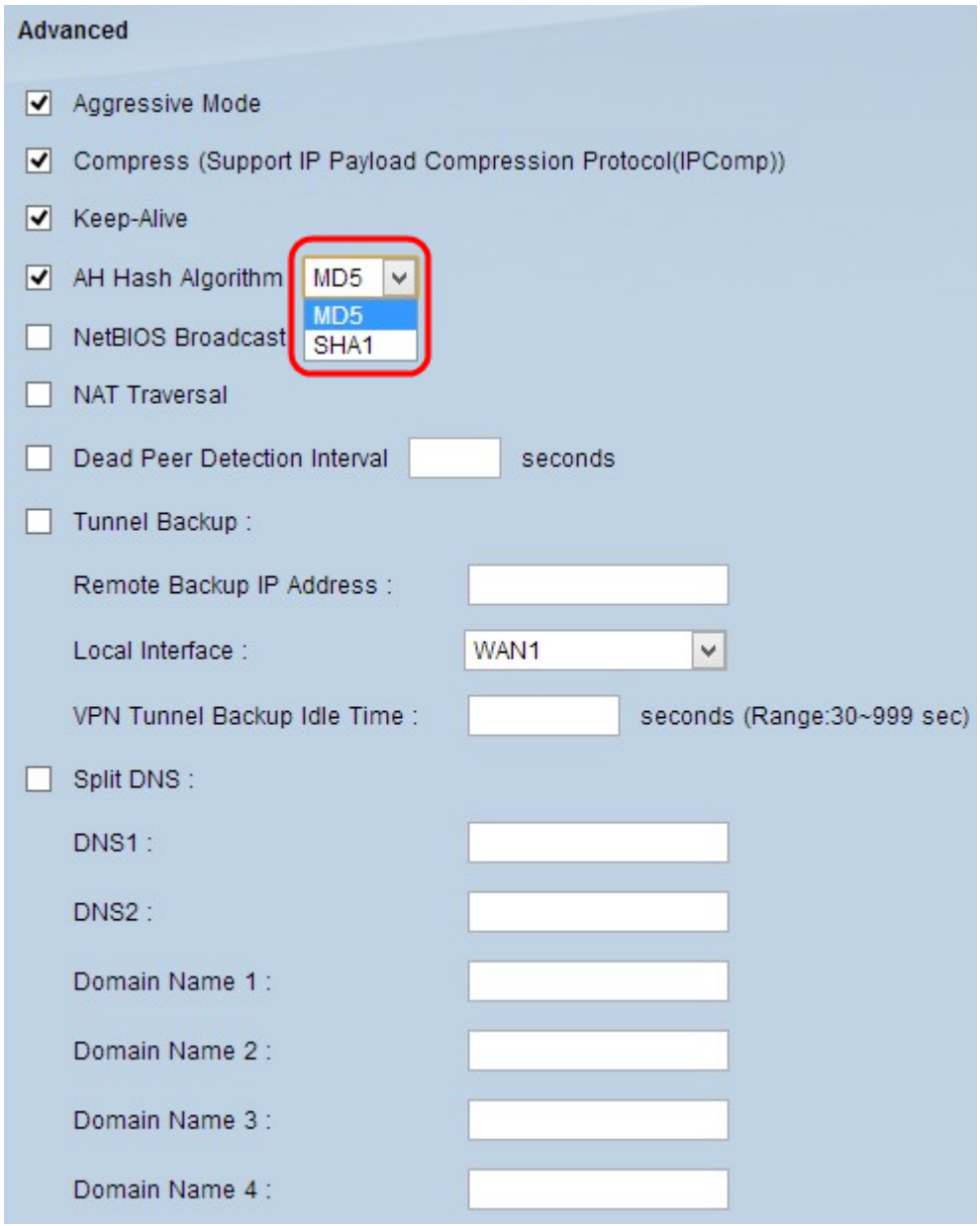
Passaggio 5. Selezionare la casella di controllo **Keep-Alive** se si desidera che la connessione del tunnel VPN rimanga sempre attiva. Keep-Alive consente di ristabilire immediatamente le connessioni quando una connessione diventa inattiva.



Passaggio 6. 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 â€" Message Digest Algorithm-5 (MD5) è una funzione hash esadecimale a 128 cifre che fornisce protezione ai dati da attacchi dannosi tramite il calcolo del checksum.

· SHA1 â€" Secure Hash Algorithm versione 1 (SHA1) è una funzione hash a 160 bit più sicura di MD5, ma richiede più tempo per l'elaborazione.

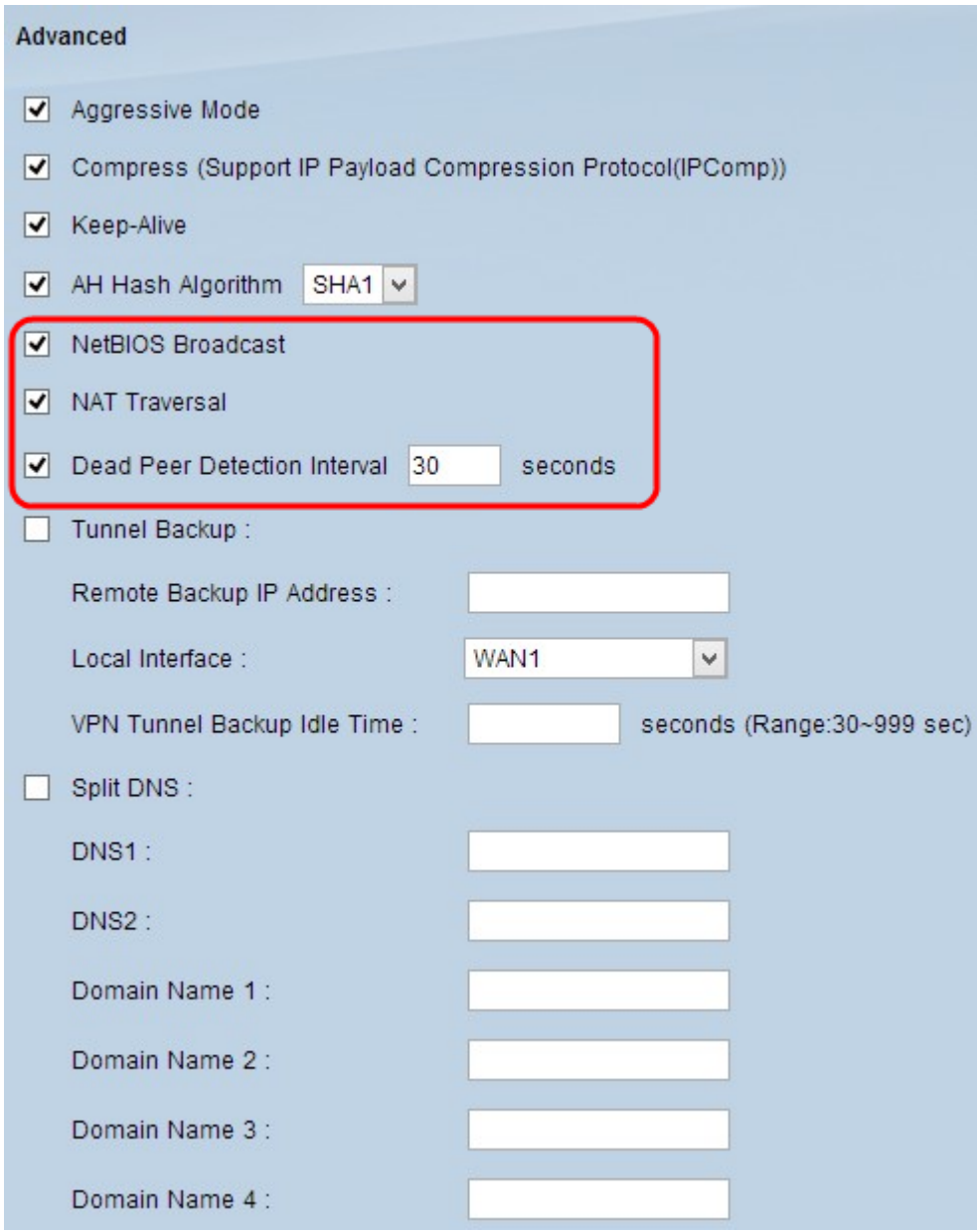


Passaggio 7. Selezionare la casella di controllo **Trasmissione NetBIOS** per consentire il traffico non instradabile attraverso il tunnel VPN. L'opzione di default è deselezionata. NetBIOS viene utilizzato per rilevare risorse di rete quali stampanti e computer nella rete tramite alcune applicazioni software e funzionalità di Windows come Risorse di rete.

Passaggio 8. 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 9. 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 l'intervallo (in secondi) tra i messaggi di saluto.

Nota: se non si seleziona Intervallo di rilevamento peer inattivi, andare al passo 11.

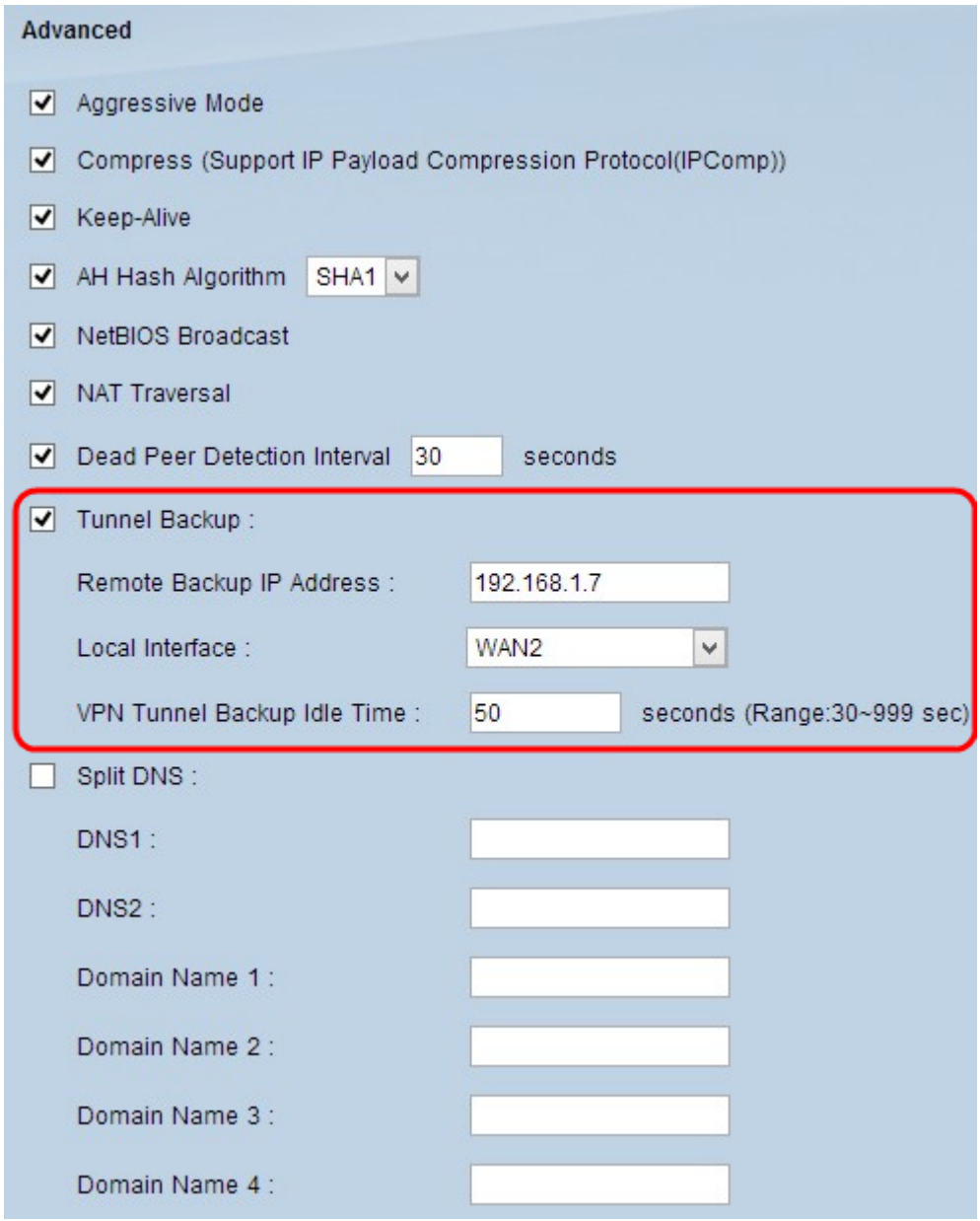


Passaggio 10. Selezionare la casella di controllo **Tunnel Backup** per abilitare il backup del tunnel. Questa funzione è disponibile solo se è stato selezionato Intervallo di rilevamento peer inattivi. Questa funzione consente al dispositivo di ristabilire il tunnel VPN tramite un'interfaccia WAN locale alternativa o un indirizzo IP remoto.

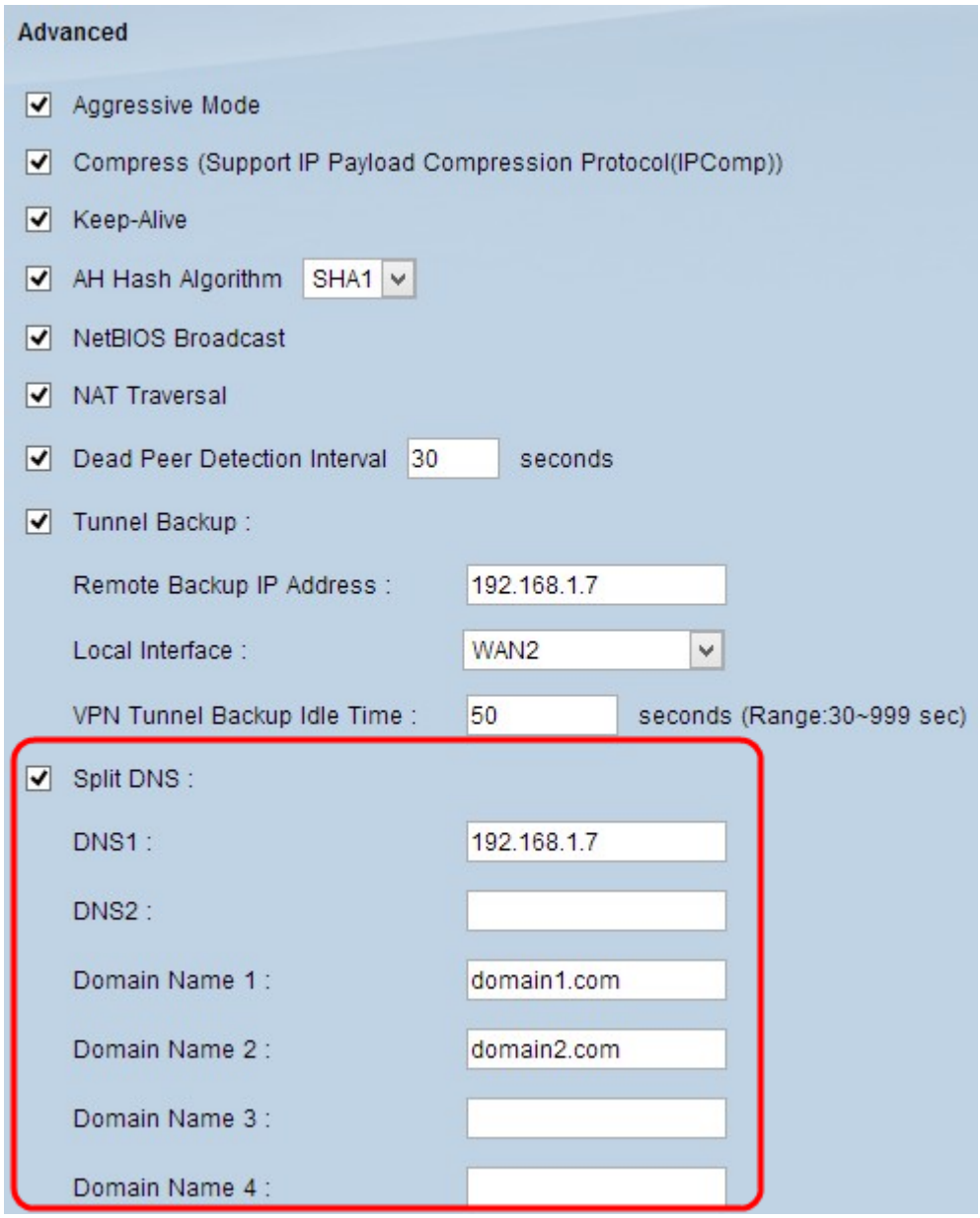
· Indirizzo IP di backup remoto: immettere un indirizzo IP alternativo per il gateway remoto o immettere l'indirizzo IP WAN già impostato per il gateway remoto in questo campo.

· Interfaccia locale: l'interfaccia WAN utilizzata per ristabilire la connessione. Selezionare l'interfaccia desiderata dall'elenco a discesa.

· Tempo di inattività del backup del tunnel VPN: immettere il tempo (in secondi) di connessione del tunnel primario prima che venga utilizzato il tunnel di backup.



Passaggio 11. Selezionare la casella di controllo **Dividi DNS** per abilitare la divisione del DNS. La suddivisione del DNS consente la gestione delle richieste per i nomi di dominio specificati da parte di un server DNS diverso da quello utilizzato in genere. Quando il router riceve una richiesta DNS dal client, controlla la richiesta DNS e le corrispondenze con il nome di dominio e invia la richiesta a tale server DNS specifico.



Passaggio 12. Immettere l'indirizzo IP del server DNS nel campo *DNS1*. Se è presente un altro server DNS, immettere l'indirizzo IP del server DNS nel campo *DNS2*.

Passaggio 13. Immettere i nomi di dominio nei campi *Nome dominio 1-Nome dominio 4*. Le richieste per questi nomi di dominio verranno gestite dai server DNS specificati nel passaggio 12.

Passaggio 14. Fare clic su **Salva** per salvare le modifiche.

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).