Defina as configurações avançadas de Gateway para Gateway VPN nos roteadores VPN RV016, RV042, RV042G e RV082

Objetivo

Uma Rede Privada Virtual (VPN) é uma rede privada usada para conectar virtualmente dispositivos do usuário remoto através de uma rede pública para fornecer segurança. Mais especificamente, uma conexão VPN de gateway a gateway permite que dois roteadores se conectem uns aos outros com segurança e que um cliente em uma extremidade pareça logicamente fazer parte da mesma rede remota na outra extremidade. Isso permite que dados e recursos sejam compartilhados com mais facilidade e segurança pela Internet. Uma configuração idêntica deve ser feita em ambos os lados da conexão para que uma conexão VPN de gateway a gateway seja estabelecida com êxito.

A configuração avançada de gateway para gateway VPN oferece a flexibilidade de configurar configurações opcionais para que o túnel VPN seja mais amigável para os usuários de VPN. As opções Avançadas estão disponíveis somente para IKE com modo de chave pré-compartilhada. As configurações avançadas devem ser as mesmas em ambos os lados da conexão VPN.

O objetivo deste documento é mostrar a você como definir configurações avançadas para gateway para gateway túnel VPN em RV016, RV042, RV042G e RV082 Roteadores VPN.

Observação: se quiser saber mais sobre como configurar um Gateway para Gateway VPN, consulte o artigo *Configuração de Gateway para Gateway VPN em RV016, RV042, RV042G e RV082 VPN Routers.*

Dispositivos aplicáveis

â€¢RV016
â€¢RV042
â€¢RV042G
â€¢RV082

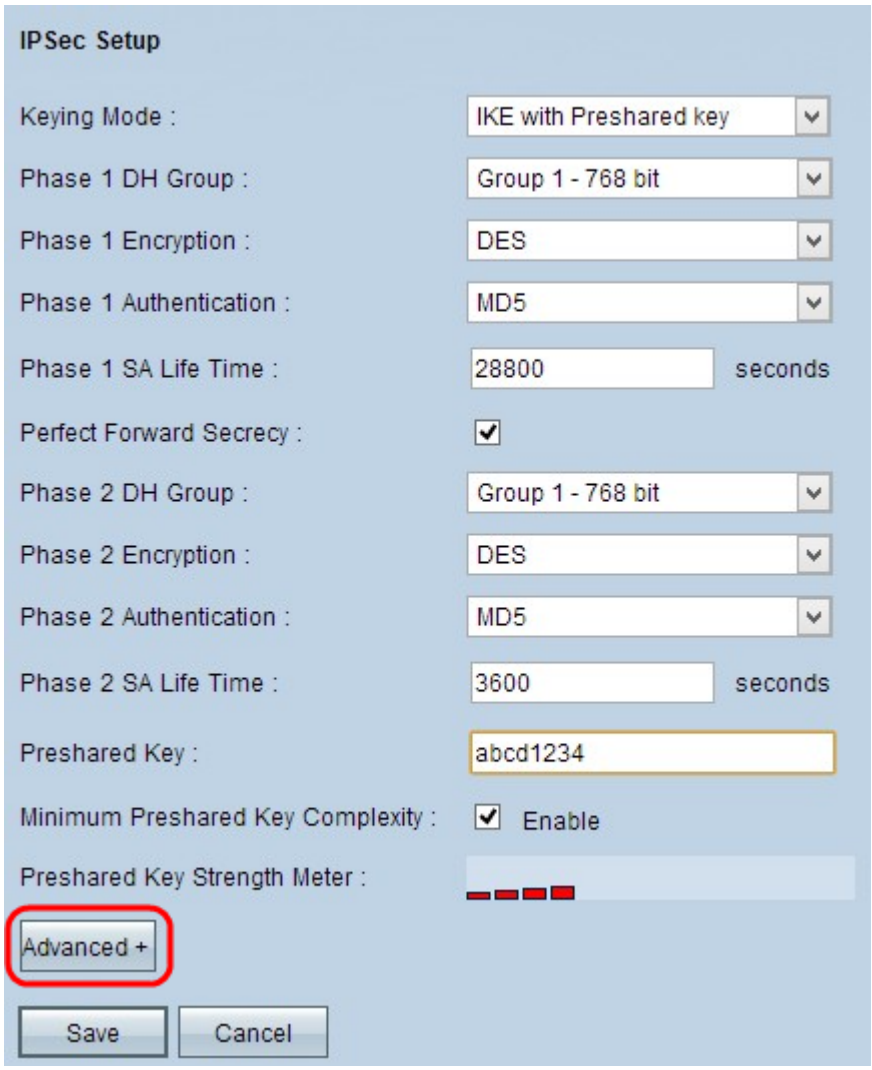
Versão de software

â€¢v4.2.2.08

Configuração de parâmetros avançados para VPN de gateway para gateway

Etapa 1. Faça login no utilitário de configuração do roteador e escolha **VPN > Gateway To Gateway**. A página *Gateway To Gateway* é aberta:

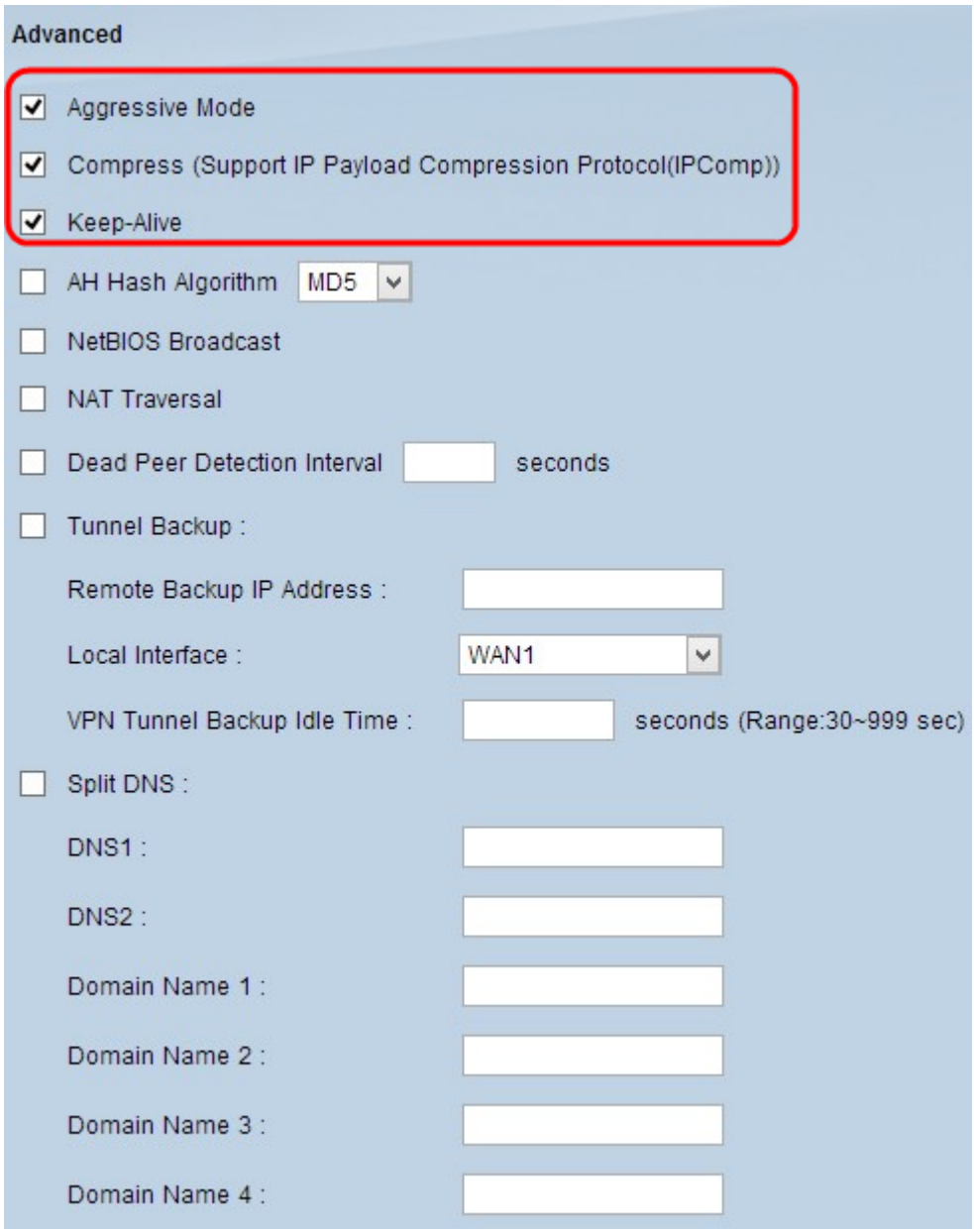
Etapa 2. Role para baixo até a seção *IPSec Setup* e clique em **Advanced +**. A área *Avançado* é exibida:



Etapa 3. Marque a caixa de seleção Aggressive Mode (Modo agressivo) se a velocidade da rede for baixa. Isso troca as IDs dos endpoints do túnel em texto não criptografado durante a conexão do SA (fase 1), o que requer menos tempo para a troca, porém oferece menor segurança.

Etapa 4. Marque a caixa de seleção **Compress (Support IP Payload Compression Protocol (IPComp))** se quiser compactar o tamanho dos datagramas IP. O IPComp é um protocolo de compactação IP usado para compactar o tamanho dos datagramas IP. A compactação de IP é útil se a velocidade da rede é baixa e o usuário deseja transmitir rapidamente os dados sem qualquer perda, mesmo com a rede lenta, porém não oferece segurança.

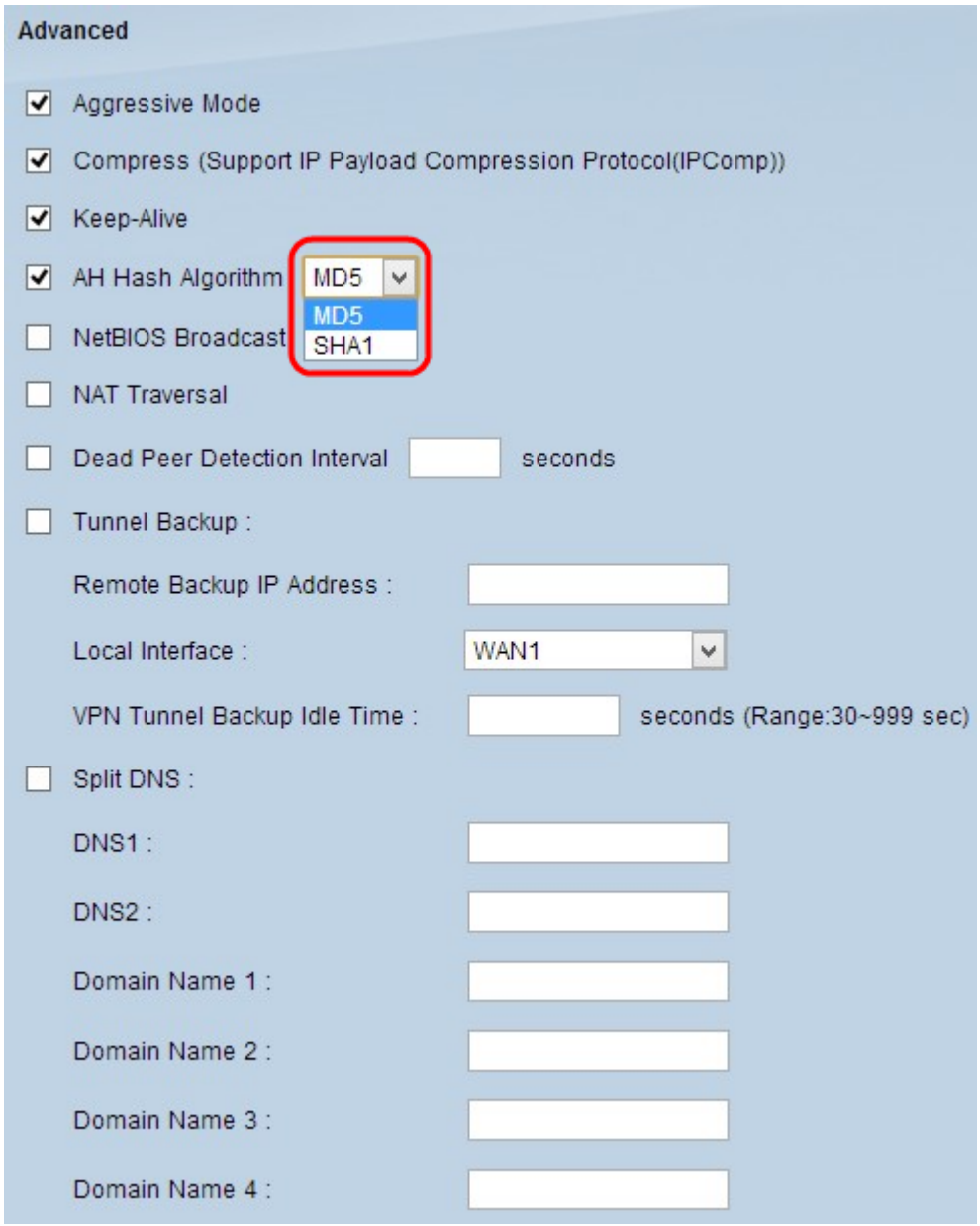
Etapa 5. Marque a caixa de seleção **Keep-Alive** se quiser que a conexão do túnel VPN permaneça ativa. O Keep-Alive ajuda a restabelecer as conexões imediatamente se alguma conexão ficar inativa.



Etapa 6. Marque a caixa de seleção AH Hash Algorithm (Algoritmo hash AH), se quiser ativar o cabeçalho de autenticação (AH). O AH fornece autenticação para dados de origem, integridade de dados por meio de soma de verificação e proteção no cabeçalho IP. O túnel deve ter o mesmo algoritmo para ambos os lados.

· MD5 â€" O MD5 (Message Digest Algorithm-5) é uma função hash hexadecimal de 128 dígitos que fornece proteção aos dados contra ataques mal-intencionados pelo cálculo do checksum.

· SHA1 â€" O Algoritmo de Hash Seguro versão 1 (SHA1) é uma função de hash de 160 bits que é mais segura que o MD5, mas leva mais tempo para ser computada.

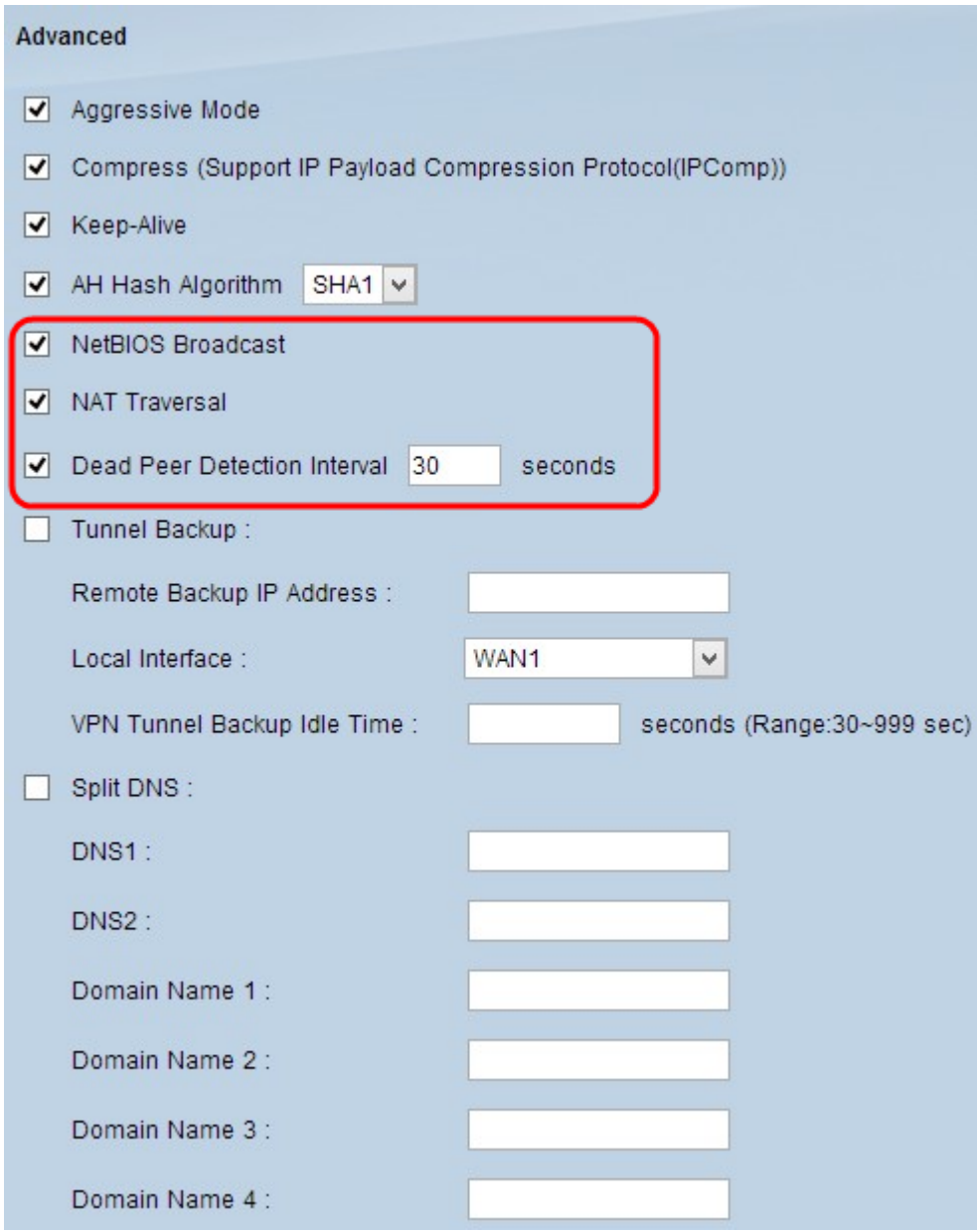


Passo 7. Marque a caixa de seleção **NetBIOS Broadcast** se quiser permitir o tráfego não roteável através do túnel VPN. O padrão é desmarcado. O NetBIOS é usado para detectar recursos de rede, como impressoras e computadores na rede, através de alguns aplicativos de software e recursos do Windows, como o Ambiente de rede.

Etapa 8. Marque a caixa de seleção **NAT Traversal** se desejar acessar a Internet a partir de sua LAN privada por meio de um endereço IP público. Se o roteador VPN estiver atrás de um gateway NAT, marque essa caixa de seleção para ativar a travessia de NAT. Ambas as extremidades do túnel devem ter as mesmas configurações.

Etapa 9. Marque Dead Peer Detection Interval (Intervalo de detecção de par inativo) para verificar a atividade do túnel VPN por Hello ou ACK de forma periódica. Se você marcar essa caixa de seleção, insira o intervalo (em segundos) entre as mensagens de saudação.

Observação: se você não marcar Intervalo de detecção de ponto inativo, vá para a etapa 11.

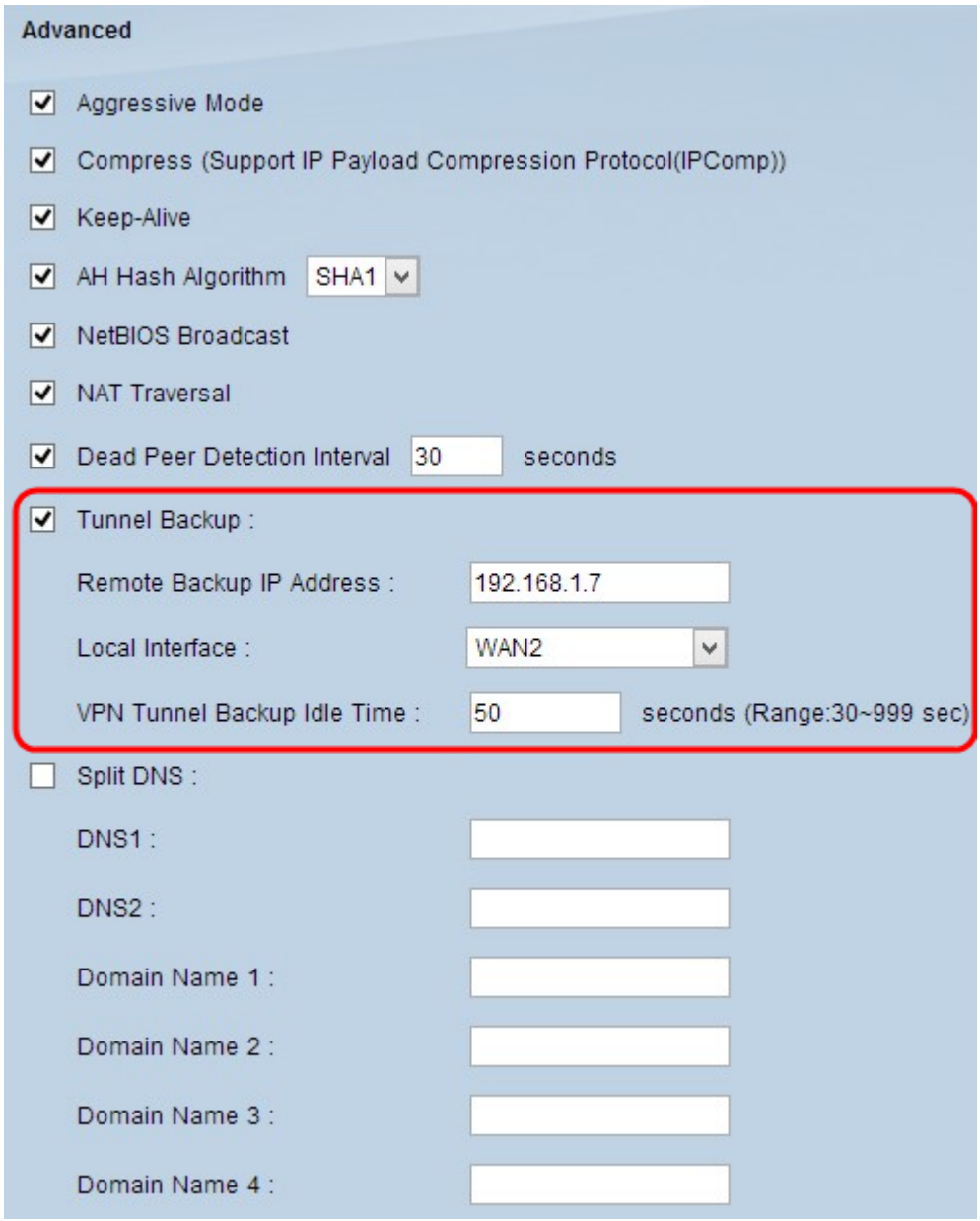


Etapa 10. Marque a caixa de seleção **Tunnel Backup** para ativar o backup de túnel. Este recurso está disponível somente quando a opção Intervalo de detecção de peer inativo está marcada. O recurso permite que o dispositivo restabeleça o túnel VPN através de uma interface WAN local alternativa ou endereço IP remoto.

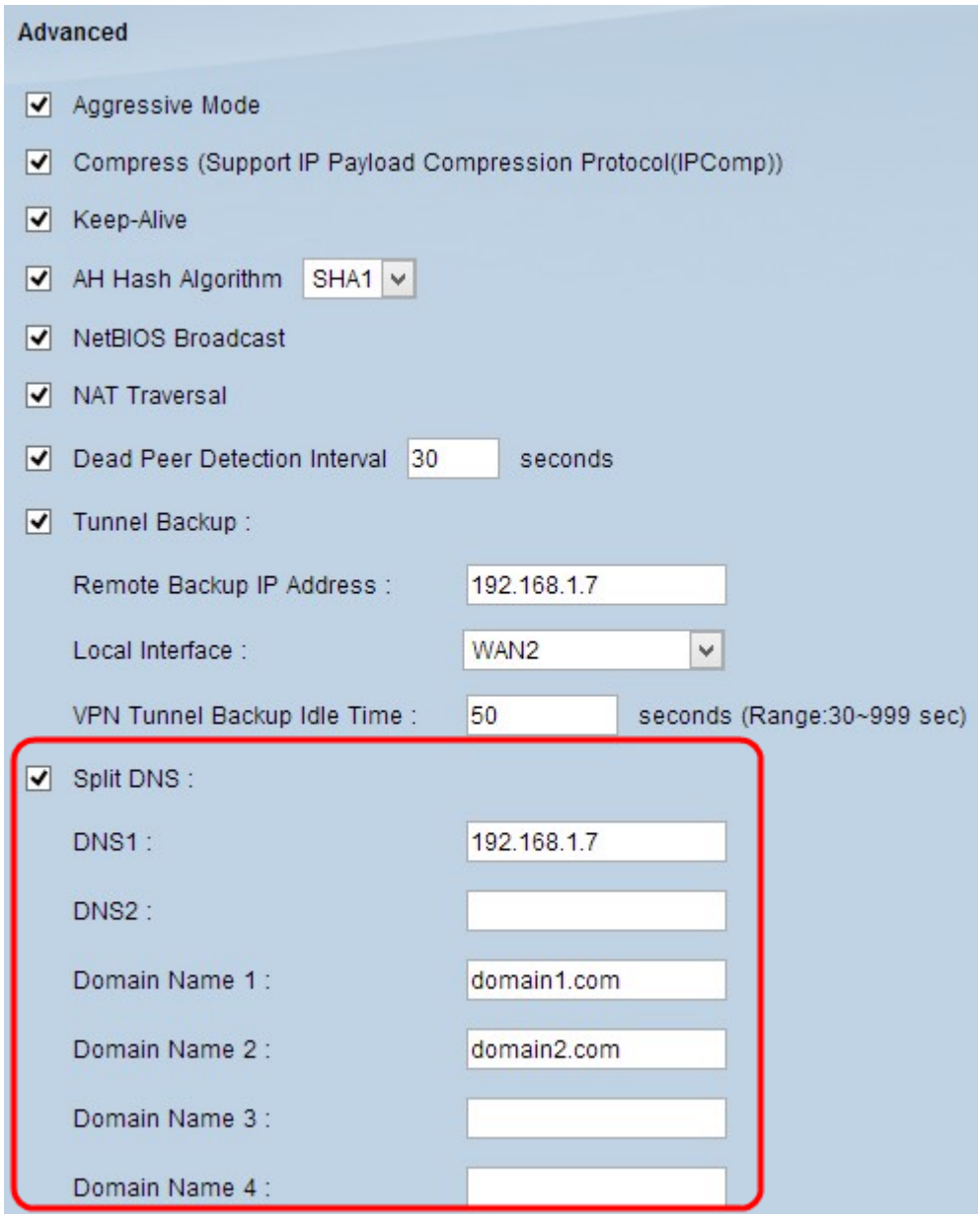
· Endereço IP do backup remoto â€" insira um endereço IP alternativo para o gateway remoto ou insira o endereço IP da WAN que já foi definido para o gateway remoto nesse campo.

· Interface local â€" a interface WAN usada para restabelecer a conexão. Escolha a interface desejada na lista suspensa.

· Tempo ocioso de backup do túnel VPN â€" Digite o tempo (em segundos) que o túnel principal tem para se conectar antes que o túnel de backup seja usado.



Etapa 11. Marque a caixa de seleção **Dividir DNS** para habilitar o DNS dividido. O DNS dividido permite que as solicitações de nomes de domínio especificados sejam tratadas por um servidor DNS diferente do que é normalmente usado. Quando o roteador recebe qualquer solicitação DNS do cliente, ele verifica a solicitação DNS, faz a correspondência com o nome de domínio e envia a solicitação para esse servidor DNS específico.



Etapa 12. Insira o endereço IP do servidor DNS no campo *DNS1*. Se houver outro servidor DNS, insira o endereço IP do servidor DNS no campo *DNS2*.

Etapa 13. Insira os nomes de domínio nos campos *Domain Name 1* a *Domain Name 4*. As solicitações para esses nomes de domínio serão tratadas pelos servidores DNS especificados na Etapa 12.

Etapa 14. Clique em **Salvar** para salvar suas alterações.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.