RV016, RV042, RV042G 및 RV082 VPN Router에서 게이트웨이 투 게이트웨이 VPN에 대한 고급 설정을 구성합니다

목표

VPN(Virtual Private Network)은 보안을 제공하기 위해 공용 네트워크를 통해 원격 사용자의 디바이스를 가상으로 연결하는 데 사용되는 사설 네트워크입니다. 보다 구체적으로, 게이트웨이 간 VPN 연결에서는 두 라우터가 서로 안전하게 연결할 수 있으며 한 쪽 끝에 있는 클라이언트가 다른 쪽 끝에 있는 동일한 원격 네트워크의 일부인 것처럼 논리적으로 보일 수 있습니다. 이를 통해 데이터와 리소스를 인터넷을 통해 보다 쉽고 안전하게 공유할 수 있습니다. 성공적인 게이트웨이 간 VPN 연결을 설정하려면 연결의 양쪽에서 동일한 컨피그레이션을 수행해야 합니다.

Advanced Gateway to Gateway VPN 컨피그레이션은 VPN 사용자가 보다 쉽게 사용할 수 있도록 VPN 터널의 선택적 컨피그레이션을 구성하는 유연성을 제공합니다. 고급 옵션은 사전 공유 키 모드가 있는 IKE에만 사용할 수 있습니다. 고급 설정은 VPN 연결의 양쪽에서 동일해야 합니다.

이 문서의 목적은 RV016, RV042, RV042G 및 RV082 VPN Router의 게이트웨이 대 게이트웨이 VPN 터널에 대한 고급 설정을 구성하는 방법을 설명하는 것입니다.

참고: 게이트웨이 VPN에 대한 게이트웨이 구성 방법에 대한 자세한 내용은 RV016, RV042, RV042G 및 RV082 VPN Router의 게이트웨이 VPN 구성 기사를 참조하십시오.

적용 가능한 디바이스

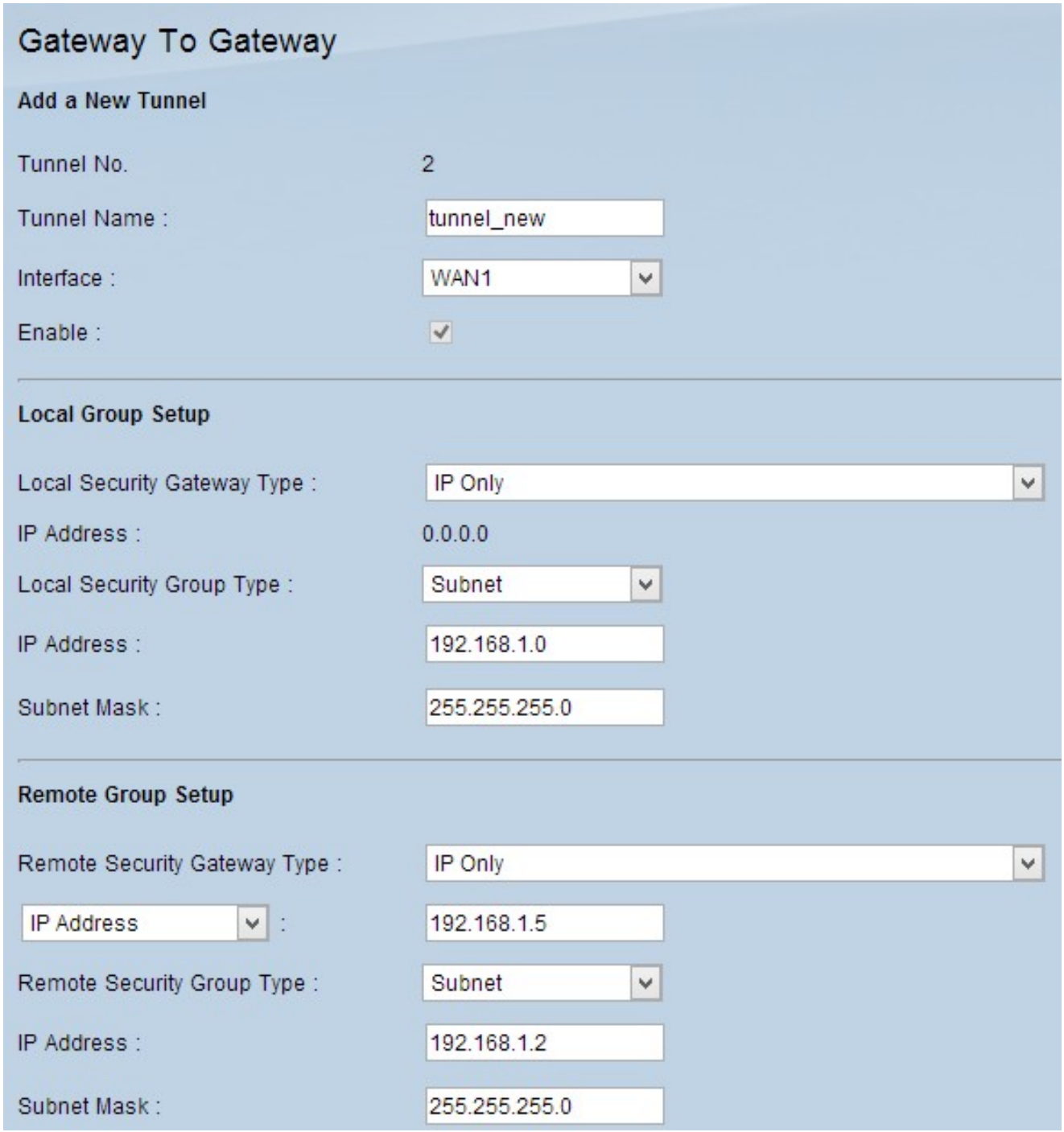
· RV016
· RV042
· RV042G
· RV082

소프트웨어 버전

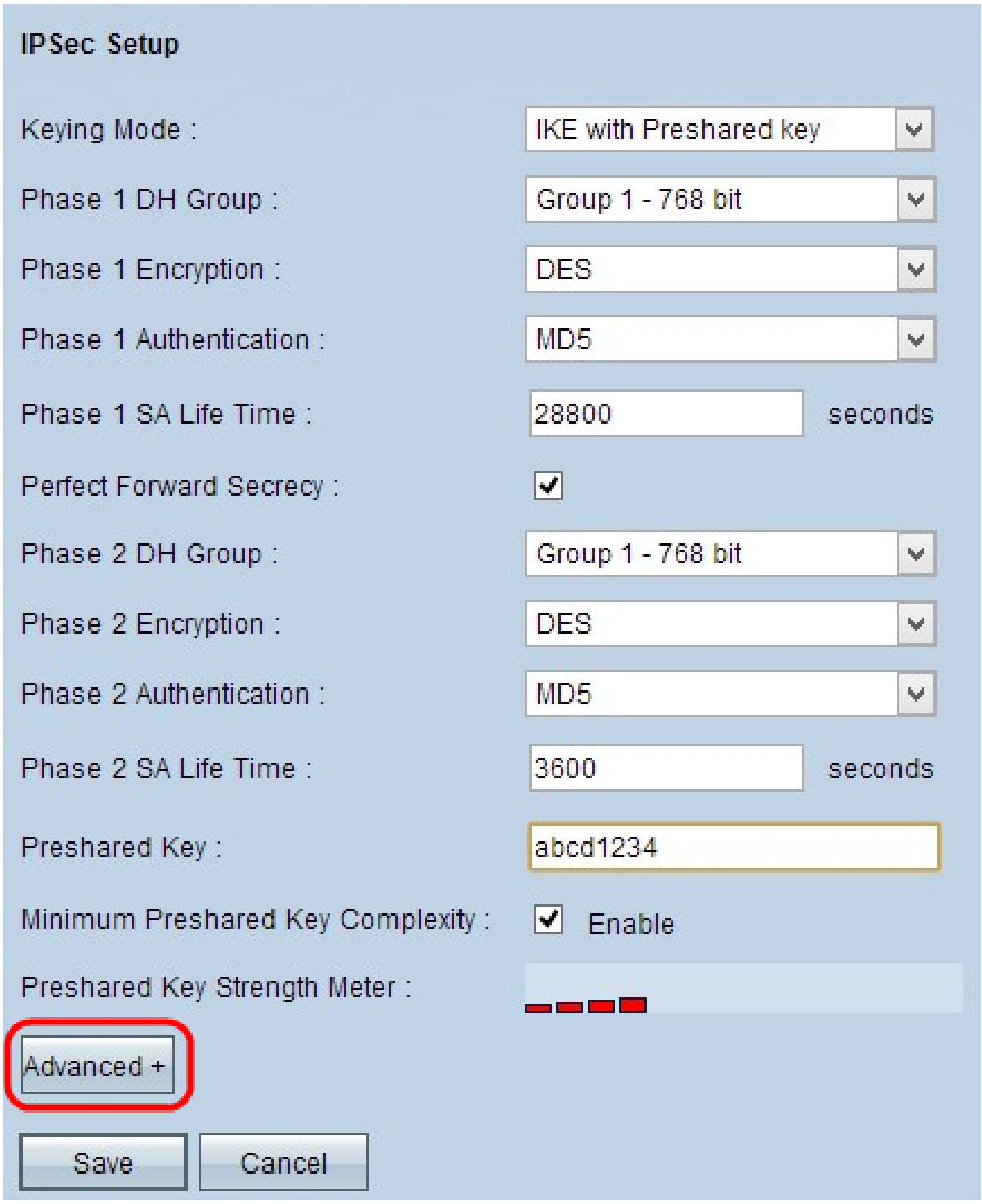
· v4.2.2.08

게이트웨이-게이트웨이 VPN에 대한 고급 설정 구성

1단계. 라우터 컨피그레이션 유틸리티에 로그인하고 VPN > Gateway To Gateway를 선택합니다. Gateway To Gateway 페이지가 열립니다.



2단계. 아래로 스크롤하여 IPSec Setup 섹션으로 이동한 다음 Advanced +를 클릭합니다. Advanced(고급) 영역이 나타납니다.

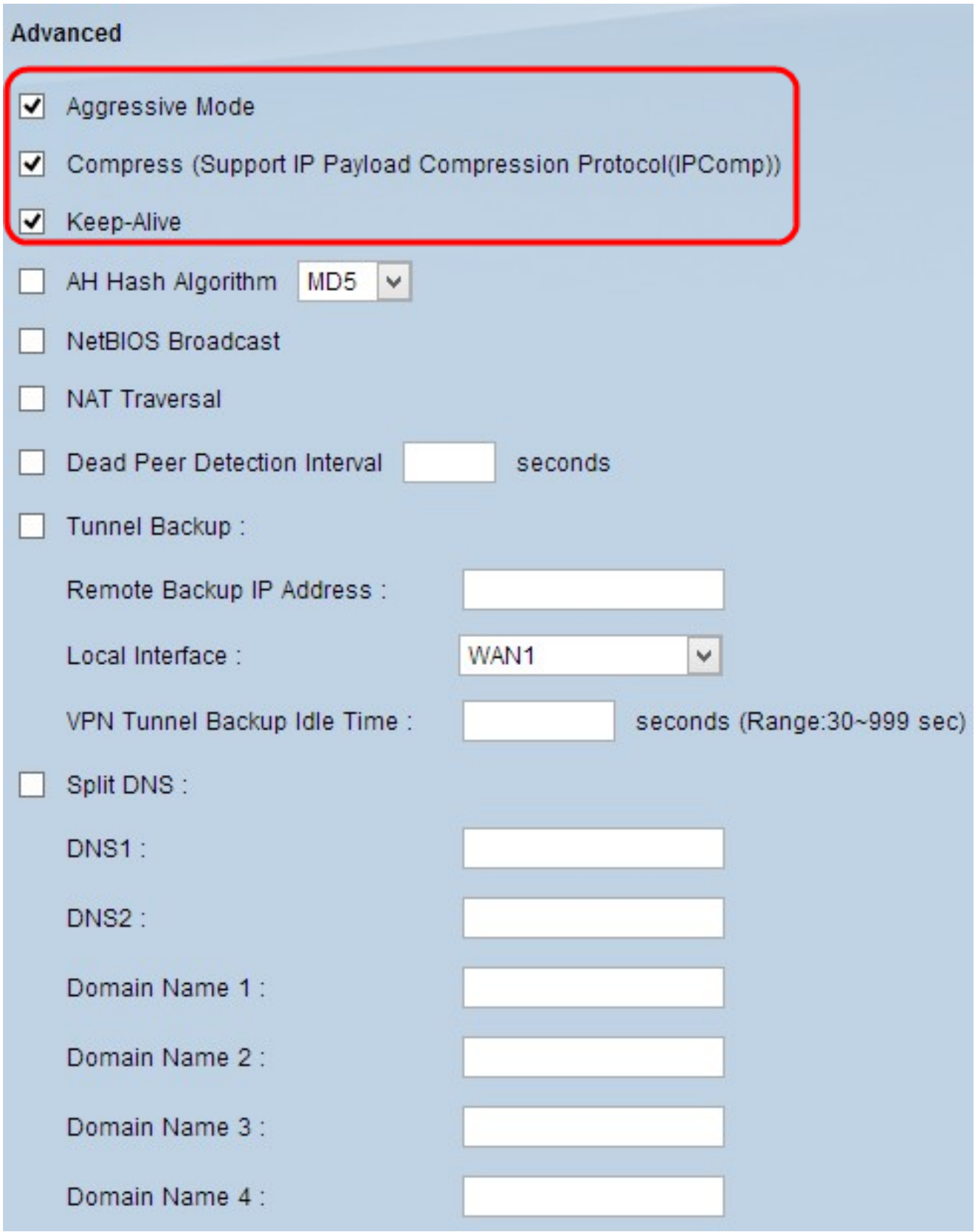


3단계. 네트워크 속도가 낮은 경우 Aggressive Mode 확인란을 선택합니다. 이렇게 하면 SA 연결(1단계) 중에 터널의 엔드포인트 ID가 일반 텍스트로 교환되므로 교환 시간이 짧지만 보안은 떨어집니다.

4단계. IP 데이터그램의 크기를 압축하려면 Compress (Support IP Payload Compression Protocol (IPComp))(압축(IPComp(IP 페이로드 압축 프로토콜 지원)))) 확인란을 선택합니다.

IPComp는 IP 데이터그램의 크기를 압축하는 데 사용되는 IP 압축 프로토콜입니다. IP 압축은 네트워크 속도가 느리고 사용자가 느린 네트워크를 통해 손실 없이 데이터를 빠르게 전송하고자 할 때 유용하지만 어떤 보안도 제공하지 않습니다.

5단계. 항상 VPN 터널의 연결을 활성 상태로 유지하려는 경우 Keep-Alive 확인란을 선택합니다. Keep-Alive를 사용하면 연결이 비활성화될 경우 즉시 연결을 다시 설정할 수 있습니다.

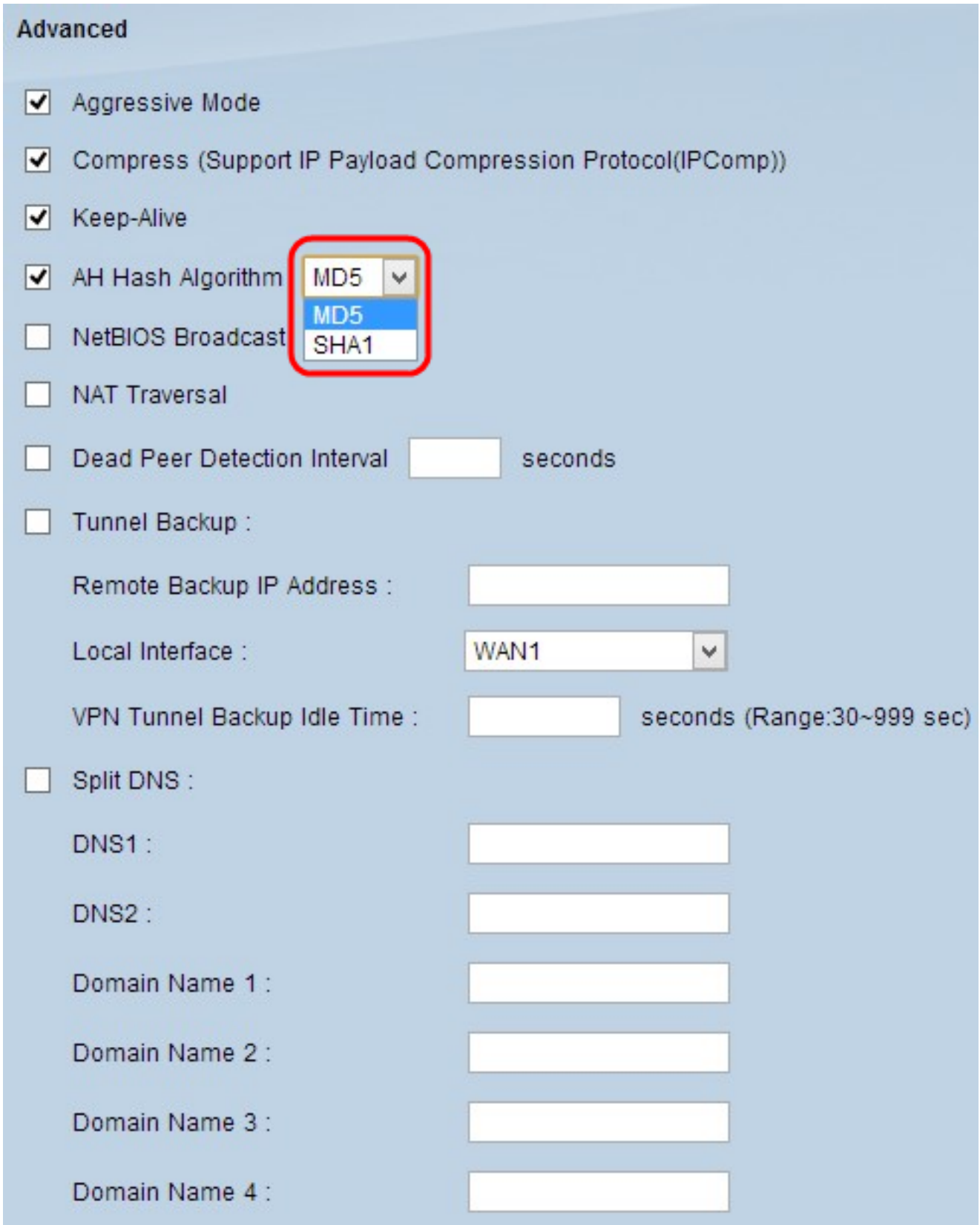


6단계. AH(Authenticate Header)를 활성화하려면 AH Hash Algorithm 확인란을 선택합니다. AH는 원본 데이터에 대한 인증, 체크섬을 통한 데이터 무결성 및 IP 헤더로의 보호를 제공합니다. 터널은 양쪽에 대해 동일한 알고리즘을 사용해야 합니다.

· MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산으로 악의적인 공격으로부터 데

이터를 보호하는 128자리 16진수 해시 함수입니다.

· SHA1 — SHA1(Secure Hash Algorithm version 1)은 160비트 해시 함수로 MD5보다 안전하지만 계산에는 시간이 더 걸립니다.

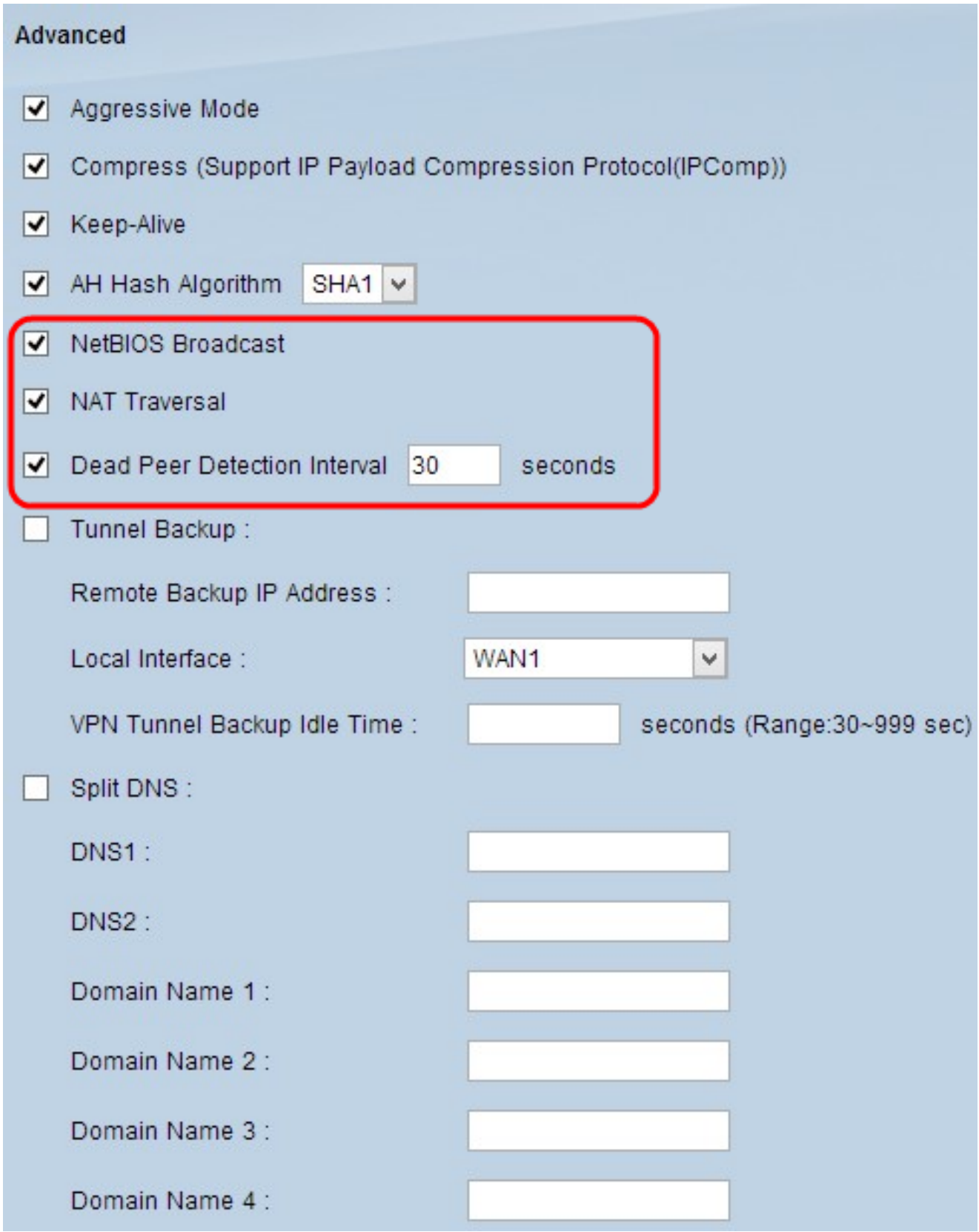


7단계. VPN 터널을 통해 라우팅 불가능한 트래픽을 허용하려면 NetBIOS Broadcast 확인란을 선택합니다. 기본값은 선택 취소입니다. NetBIOS는 Network Neighborhood와 같은 일부 소프트웨어 애플리케이션 및 Windows 기능을 통해 네트워크에서 프린터 및 컴퓨터와 같은 네트워크 리소스를 탐지하는 데 사용됩니다.

8단계. 공용 IP 주소를 통해 사설 LAN에서 인터넷에 액세스하려면 NAT Traversal 확인란을 선택합니다. VPN 라우터가 NAT 게이트웨이 뒤에 있는 경우 NAT 통과를 활성화하려면 이 확인란을 선택합니다. 터널의 양쪽 끝에는 동일한 설정이 있어야 합니다.

9단계. Dead Peer Detection Interval(데드 피어 탐지 간격)을 선택하여 주기적으로 hello 또는 ACK를 통해 VPN 터널의 활성 상태를 확인합니다. 이 확인란을 선택하는 경우 hello 메시지의 간격(초)을 입력합니다.

참고: Dead Peer Detection Interval(데드 피어 탐지 간격)을 선택하지 않으면 11단계로 건너뜁니다.

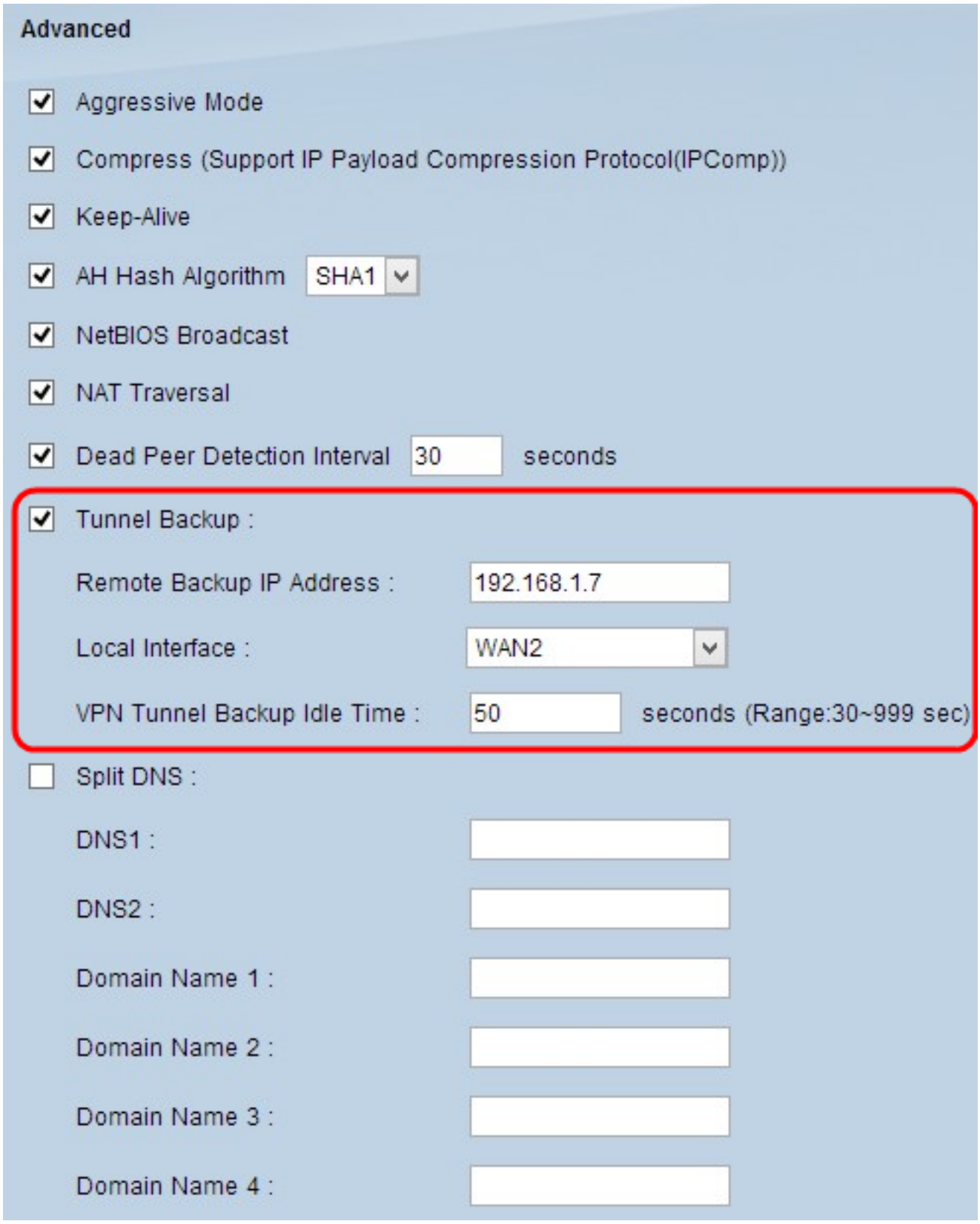


10단계. 터널 백업을 활성화하려면 Tunnel Backup 확인란을 선택합니다. 이 기능은 Dead Peer Detection Interval(데드 피어 탐지 간격)을 선택한 경우에만 사용할 수 있습니다. 이 기능을 사용하면 디바이스에서 대체 로컬 WAN 인터페이스 또는 원격 IP 주소를 통해 VPN 터널을 재설정할 수 있습니다.

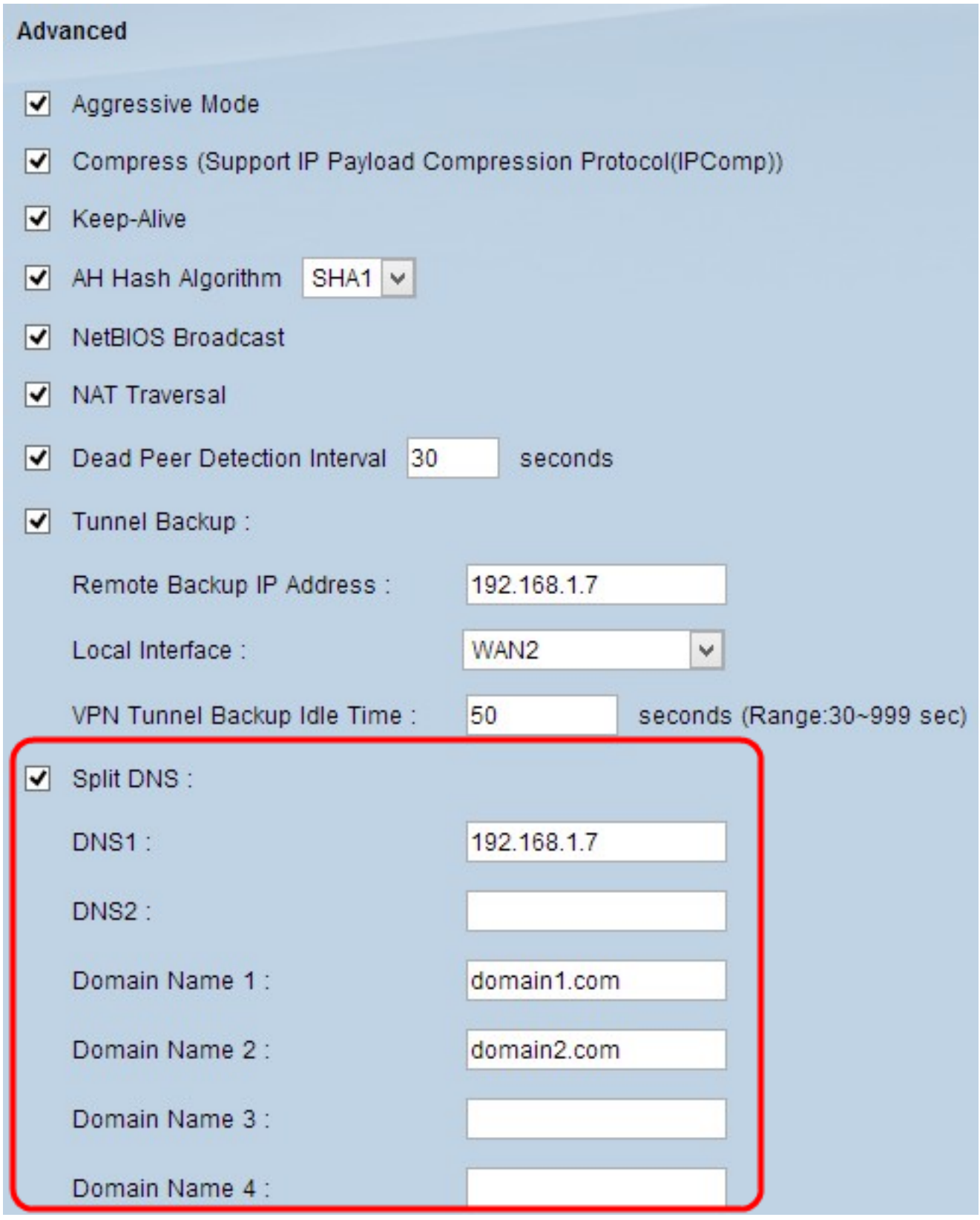
· 원격 백업 IP 주소 — 원격 게이트웨이의 대체 IP 주소를 입력하거나 원격 게이트웨이에 대해 이미 설정된 WAN IP 주소를 이 필드에 입력합니다.

· Local Interface — 연결을 재설정하는 데 사용되는 WAN 인터페이스입니다. 드롭다운 목록에서 원하는 인터페이스를 선택합니다.

· VPN Tunnel Backup Idle Time — 백업 터널이 사용되기 전에 기본 터널이 연결해야 하는 시간(초)을 입력합니다.



11단계. Split DNS(스플릿 DNS) 확인란을 선택하여 스플릿 DNS를 활성화합니다. 스플릿 DNS를 사용하면 지정된 도메인 이름에 대한 요청을 일반적으로 사용되는 것과 다른 DNS 서버에서 처리할 수 있습니다. 라우터가 클라이언트로부터 DNS 요청을 수신하면 DNS 요청을 확인하고 도메인 이름과 일치시킨 후 요청을 특정 DNS 서버로 전송합니다.



12단계. DNS1 필드에 DNS 서버 IP 주소를 입력합니다. 다른 DNS 서버가 있는 경우 DNS2 필드에 DNS 서버 IP 주소를 입력합니다.

13단계. Domain Name 1~Domain Name 4 필드에 도메인 이름을 입력합니다. 이러한 도메인 이름에 대한 요청은 12단계에서 지정한 DNS 서버에서 처리합니다.

14단계. Save(저장)를 클릭하여 변경 사항을 저장합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.