RV320 및 RV325 VPN Router Series의 게이트웨이-게이트웨이 VPN(Virtual Private Network) 구성

목표

VPN은 공용 또는 공유 인터넷을 통해 VPN 터널을 통해 두 엔드포인트를 통해 매우 안전한 연결을 형성하는 데 사용됩니다.보다 구체적으로 게이트웨이 간 VPN 연결을 사용하면 두 라우터가 서로 안전하게 연결하고 한 쪽 끝에 있는 클라이언트가 다른 쪽 끝에 있는 동일한 원격 네트워크에 논리적으로 표시되도록 할 수 있습니다.이를 통해 데이터와 리소스를 인터넷을 통해 보다 쉽고 안전하게 공유할 수 있습니다.게이트웨이 간 VPN 연결을 성공적으로 설정하려면 연결의 양쪽에서 컨피그레이션을 수행해야 합니다.이 문서의 목적은 RV32x VPN Router Series에서 게이트웨이 간 VPN 연결의 컨피그레이션을 안내하는 것입니다.

적용 가능한 디바이스

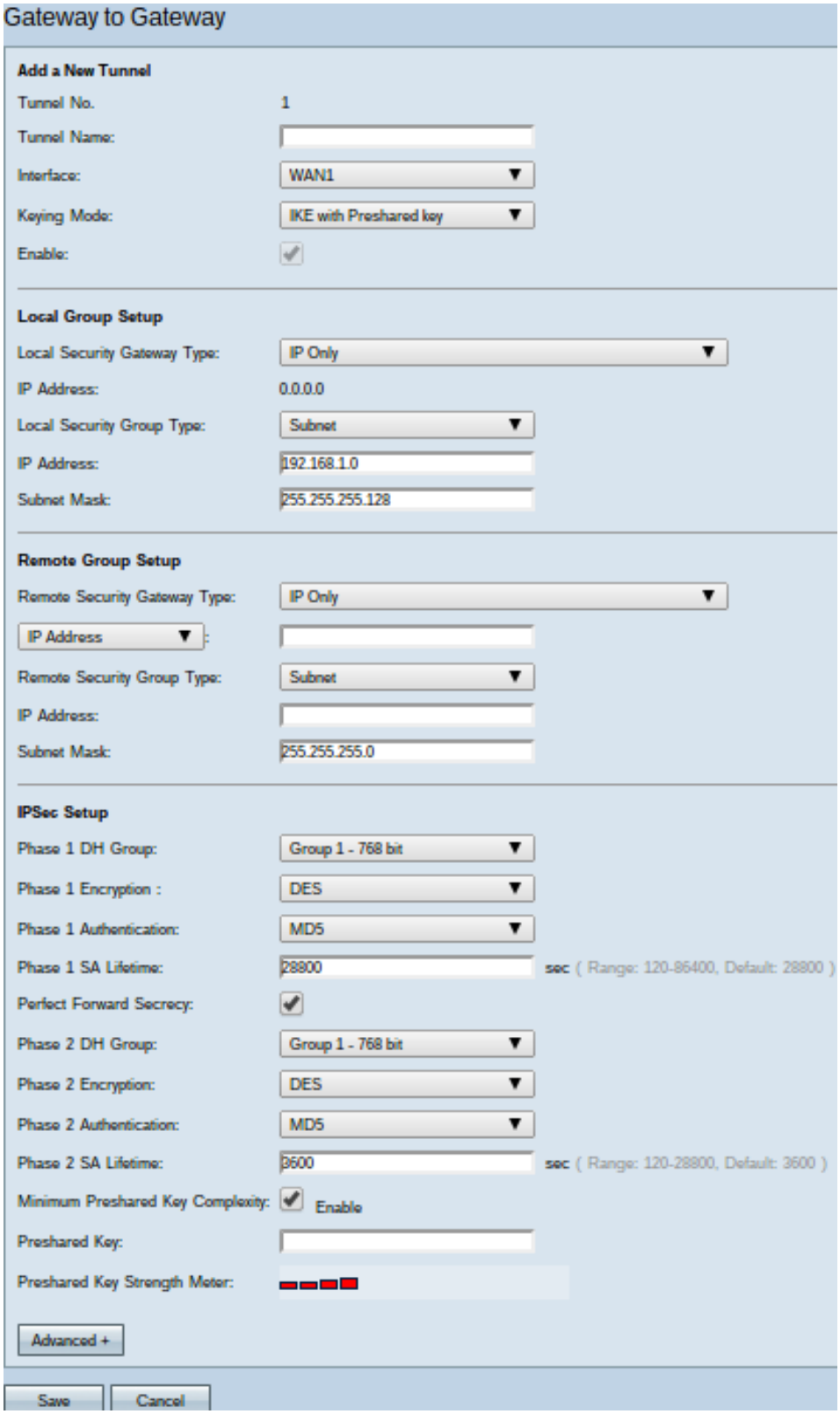
·RV320 Dual WAN VPN Router
· RV325 Gigabit Dual WAN VPN Router

소프트웨어 버전

·v1.1.0.09

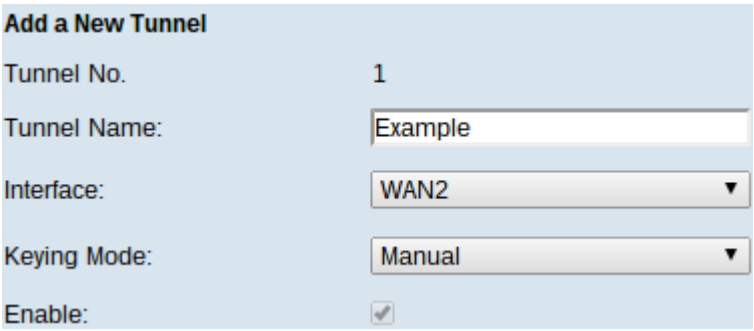
게이트웨이에 대한 게이트웨이

1단계. Web Configuration Utility에 로그인하고 **VPN > Gateway to Gateway를 선택합니다**.게이트웨이에 *대한 게이트웨이* 페이지가 열립니다.



VPN 연결이 제대로 작동하려면 연결의 양쪽에 있는 IPSec(Internet Protocol Security) 값이 동일해야 합니다.연결의 양쪽은 서로 다른 LAN(Local Area Network)에 속해야 하며, 고정 IP 주소 또는 동적 DNS 호스트 이름으로 식별될 라우터 중 하나 이상에 속해야 합니다.

새 터널 추가



·터널 번호— 생성할 현재 터널을 표시합니다.라우터는 100개의 터널을 지원합니다.

1단계. Tunnel Name(터널 이름) 필드에 VPN 터널의 이름을 입력합니다.터널의 다른 끝에서 사용되는 이름과 일치하지 않아도 됩니다.

2단계. Interface(인터페이스) 드롭다운 목록에서 터널에 사용할 WAN(Wide Area Network) 포트를 선택합니다.

·WAN1 — 라우터의 전용 WAN 포트입니다.

·WAN2 — 라우터의 WAN2/DMZ 포트입니다.드롭다운 메뉴에는 WAN으로 구성되었지만 DMZ(Diselectronize Zone) 포트가 아닌 경우에만 표시됩니다.

·USB1 — 라우터의 USB1 포트입니다.포트에 연결된 3G/4G/LTE USB 동글이 있는 경우에만 작동합니다.

·USB2 — 라우터의 USB2 포트입니다.포트에 연결된 3G/4G/LTE USB 동글이 있는 경우에만 작동합니다.

3단계. Keying Mode 드롭다운 목록에서 사용할 터널 보안을 선택합니다.

·수동 — 이 옵션을 사용하면 키를 VPN 연결의 다른 측과 협상하는 대신 수동으로 키를 구성할 수 있습니다.

·사전 공유 키가 있는 IKE — VPN 터널에서 보안 연결을 설정하는 IKE(Internet Key Exchange Protocol)를 활성화하려면 이 옵션을 선택합니다.IKE는 사전 공유 키를 사용하여 원격 피어를 인증합니다.

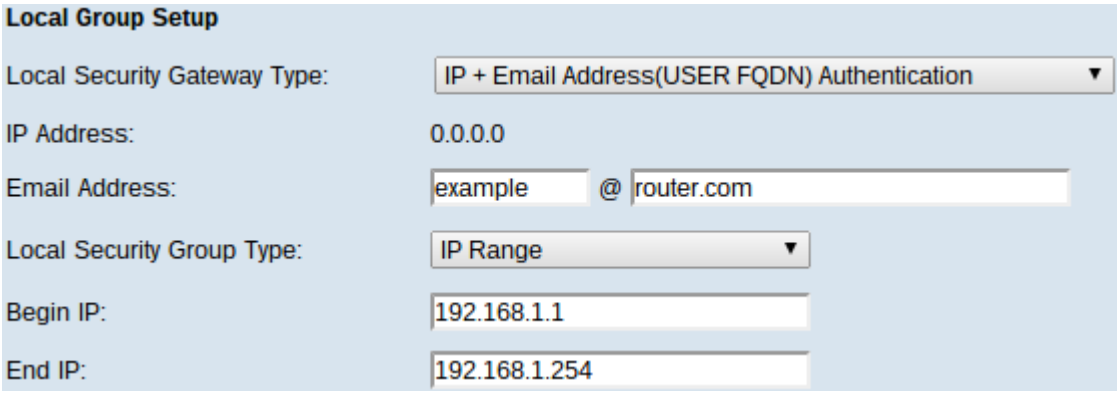
·IKE with Certificate(인증서 포함) — 이 옵션을 선택하면 IKE(Internet Key Exchange) 프로토콜을 인증서와 함께 사용할 수 있습니다. 이 프로토콜은 터널에 대해 더욱 인증되고 안전한 통신을 설정할 수 있도록 사전 공유 키를 자동으로 생성하고 교환하는 보다 안전한 방법을 제공합니다.

4단계. Enable(활성화) 확인란을 선택하여 VPN 터널을 활성화합니다.기본적으로 활성화되어 있습니다.

로컬 그룹 설정

이러한 설정은 VPN 터널의 반대쪽 끝에 있는 라우터의 "Remote Group Setup" 설정과 일치해야 합니다.

참고: Add a New Tunnel start from Step 1(1단계에서 새 터널 추가 시작 단계)의 3단계에서 Keying Mode(키 지정 모드) 드롭다운 목록에서 Manual(수동) 또는 IKE with Preshared(사전 공유 키를 사용하는 IKE)를 선택한 경우 2단계부터 4단계까지 건너뜁니다. Certificate를 사용하는 IKE를 선택한 경우 1단계를 건너뜁니다.



1단계. Local Security Gateway Type(로컬 보안 게이트웨이 유형) 드롭다운 목록에서 VPN 터널을 설정할 라우터를 식별하는 방법을 선택합니다.

·IP Only — 고정 WAN IP를 통해서만 터널에 액세스할 수 있습니다.라우터에만 고정 WAN IP가 있는 경우 이 옵션을 선택할 수 있습니다.고정 WAN IP 주소는 자동 생성 필드입니다.

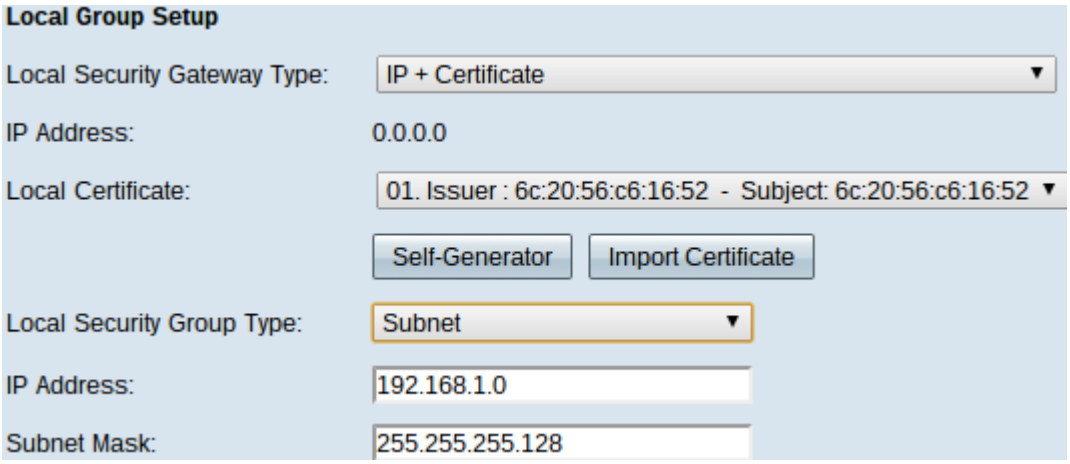
·IP + 도메인 이름(FQDN) 인증 — 고정 IP 주소 및 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.고정 WAN IP 주소는 자동 생성 필드입니다.

·IP + 이메일 주소(USER FQDN) 인증 — 고정 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 이메일 주소 필드에 이메일 주소를 입력합니다.고정 WAN IP 주소는 자동 생성 필드입니다.

·동적 IP + 도메인 이름(FQDN) 인증 — 동적 IP 주소 및 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.

·동적 IP + 이메일 주소(USER FQDN) 인증 — 동적 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 이메일 주소 필드에 이메일 주소를 입력합니다.

참고: Local Group Setup(로컬 그룹 설정) 영역에서 Certificate(인증서)로 IKE를 사용할 때 다음과 같은 변경 사항이 적용됩니다.



Local Security Gateway Type(로컬 보안 게이트웨이 유형) 드롭다운 목록을 편집할 수 없게 되고 IP + Certificate(IP + 인증서)가 표시됩니다.터널을 사용할 수 있는 LAN 리소스입니다. IP Address 필드는 디바이스의 WAN IP 주소를 표시합니다.사용자가 편집할 수 없습니다.

2단계. Local Certificate(로컬 인증서) 드롭다운 목록에서 인증서를 선택합니다.인증서는 VPN 연결에 대해 강력한 인증 보안을 제공합니다.

3단계. (선택 사항) **Self-Generator** 버튼을 클릭하여 *Certificate Generator* 창을 표시하여 인증서를 구성하고 생성합니다.

4단계. (선택 사항) Import **Certificate**(인증서 가져오기) 버튼을 클릭하여 *My Certificate(내 인증서)* 창을 표시하여 인증서를 보고 구성합니다.

5단계. Local Security Group Type(로컬 보안 그룹 유형) 드롭다운 목록에서 다음 중 하나를 선택합니다.

·IP Address — 이 옵션을 사용하면 이 VPN 터널을 사용할 수 있는 디바이스를 하나만 지정할 수 있습니다.IP 주소 필드에 디바이스의 IP 주소만 입력하면 됩니다.

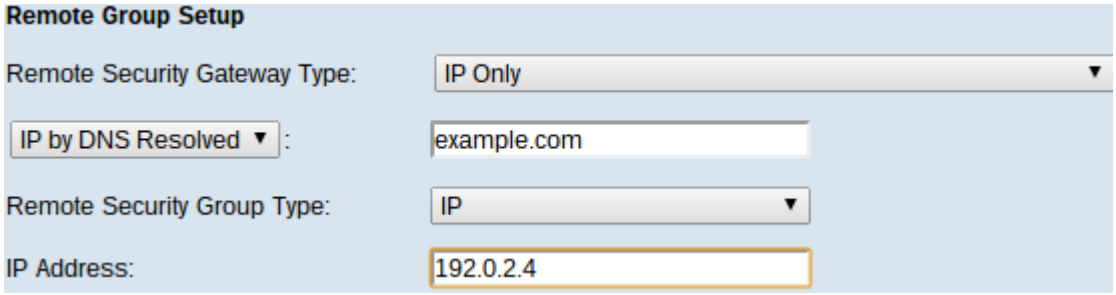
·서브넷 — 동일한 서브넷에 속하는 모든 디바이스가 VPN 터널을 사용하도록 허용하려면 이 옵션을 선택합니다.Subnet Mask(서브넷 마스크) 필드에 네트워크 IP 주소와 해당 서브넷 마스크를 입력해야 합니다.

·IP 범위 — VPN 터널을 사용할 수 있는 디바이스 범위를 지정하려면 이 옵션을 선택합니다.Begin IP(시작 IP) 필드 및 End IP(종료 IP) 필드에 디바이스 범위의 첫 번째 IP 주소와 마지막 IP 주소를 입력해야 합니다.

원격 그룹 설정

이러한 설정은 VPN 터널의 반대쪽 끝에 있는 라우터의 "로컬 그룹 설정" 설정과 일치해야 합니다.

참고: Add a New Tunnel start from Step 1(1단계에서 새 터널 추가 시작 단계) 3의 Keying Mode(키 지정 모드) 드롭다운 목록에서 Manual(수동) 또는 IKE with Preshared(사전 공유 키 포함) 를 선택한 경우 2단계에서 5단계로 건너뜁니다. 또는 IKE with Certificate(인증서 포함)를 선택한 경우 1단계를 건너뜁니다.



1단계. Remote Security Gateway Type(원격 보안 게이트웨이 유형) 드롭다운 목록에서 VPN 터널을 설정할 다른 라우터를 식별하는 방법을 선택합니다.

·IP Only — 고정 WAN IP를 통해서만 터널에 액세스할 수 있습니다.원격 라우터의 IP 주소를 알고 있는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다.IP 주소를 모르지만 도메인 이름을 알고 있는 경우 IP by DNS Resolved(DNS 확인됨)를 선택하고 IP by DNS Resolved(DNS를 통해 IP 확인) 필드에 라우터의 도메인 이름을 입력합니다.

·IP + 도메인 이름(FQDN) 인증 — 고정 IP 주소 및 라우터의 등록된 도메인을 통해 터널에 액세스할 수 있습니다.원격 라우터의 IP 주소를 알고 있는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다.IP 주소를 모르지만 도메인 이름을 알고 있는 경우 IP by DNS Resolved(DNS 확인됨)를 선택하고 IP by DNS Resolved(DNS를 통해 IP 확인) 필드에 라우터의 도메인 이름을 입력합니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.

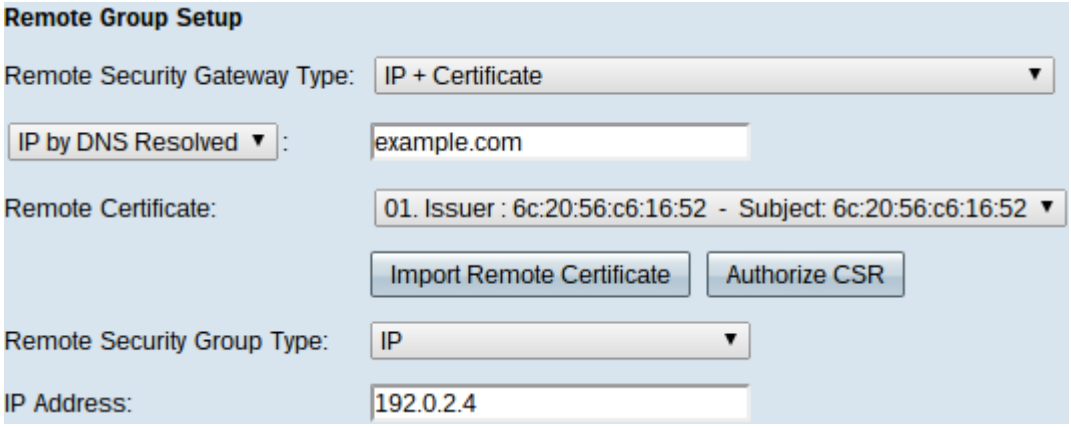
·IP + 이메일 주소(USER FQDN) 인증 — 고정 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.원격 라우터의 IP 주소를 알고 있는 경우 [원격 보안 게이트웨이 유형] 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다.IP 주소를 모르지만 도메인 이름을 알고 있는 경우 IP by DNS Resolved(DNS 확인됨)를 선택하고 IP by DNS Resolved(DNS를 통해 IP 확인) 필드에 라우터의 도메인 이름을 입력합니다.이메일 주소 필드에 이메일 주소를 입력합니다.

·동적 IP + 도메인 이름(FQDN) 인증 — 동적 IP 주소 및 등록된 도메인을 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 Domain Name(도메인 이름) 필드에 등록된 도메인의 이름을 입력합니다.

·동적 IP + 이메일 주소(USER FQDN) 인증 — 동적 IP 주소 및 이메일 주소를 통해 터널에 액세스할 수 있습니다.이 옵션을 선택하는 경우 이메일 주소 필드에 이메일 주소를 입력합니다.

참고:두 라우터에 모두 동적 IP 주소가 있는 경우 두 게이트웨이 모두에 대해 Dynamic IP + Email Address를 선택하지 마십시오.

참고: Remote Group Setup(원격 그룹 설정) 영역의 Following(다음 변경 사항)은 Certificate(인증서)로 IKE를 사용하여 작업할 때 변경됩니다.



Remote Security Gateway Type(원격 보안 게이트웨이 유형) 드롭다운 목록을 편집할 수 없게 되고 IP + Certificate(IP + 인증서)가 표시됩니다.터널을 사용할 수 있는 LAN 리소스입니다.

2단계. 원격 라우터의 IP 주소를 아는 경우 Remote Security Gateway Type(원격 보안 게이트웨이 유형) 필드 바로 아래의 드롭다운 목록에서 IP 주소를 선택하고 주소를 입력합니다.IP 주소를 모르지만 도메인 이름을 아는 경우 IP by DNS Resolved를 선택하고 IP by DNS Resolved 필드에 원격 라우터의 도메인 이름을 입력합니다

3단계. Remote Certificate(원격 인증서) 드롭다운 목록에서 인증서를 선택합니다.인증서는 VPN 연결에 대해 강력한 인증 보안을 제공합니다.

4단계. (선택 사항) **Import Remote Certificate(원격 인증서 가져오기)** 버튼을 클릭하여 새 인증서를 가져옵니다.

5단계. (선택 사항) Authorize CSR(**CSR 권한 부여**) 버튼을 클릭하여 디지털 서명 요청으로 인증서를 식별합니다.

6단계. Local Security Group Type(로컬 보안 그룹 유형) 드롭다운 목록에서 다음 중 하나를 선택합니다.

·IP Address — 이 옵션을 사용하면 이 VPN 터널을 사용할 수 있는 디바이스를 하나만 지정할 수 있습니다.IP 주소 필드에 디바이스의 IP 주소만 입력하면 됩니다.

·서브넷 — 동일한 서브넷에 속하는 모든 디바이스가 VPN 터널을 사용하도록 허용하려면 이 옵션을 선택합니다.Subnet Mask(서브넷 마스크) 필드에 네트워크 IP 주소와 해당 서브넷 마스크를 입력해야 합니다.

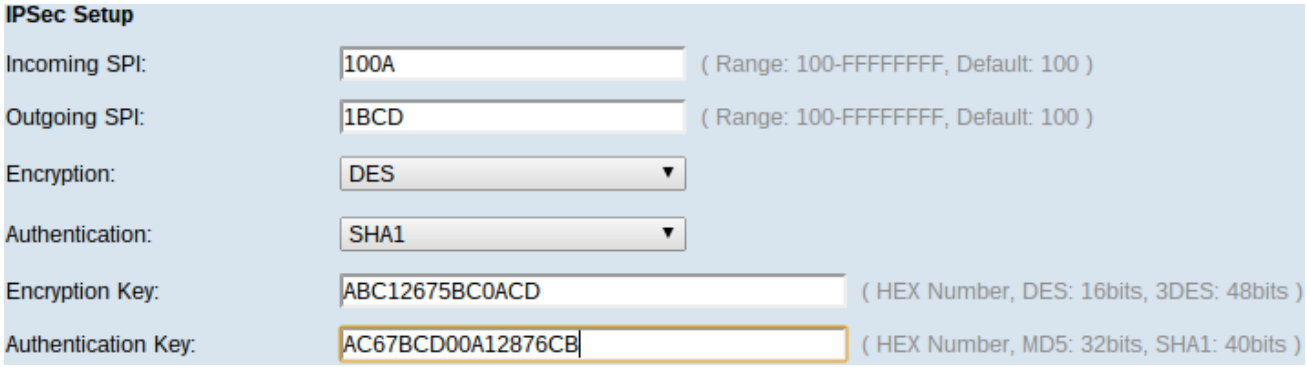
·IP 범위 — VPN 터널을 사용할 수 있는 디바이스 범위를 지정하려면 이 옵션을 선택합니다.디바이스 범위의 첫 번째 IP 주소와 마지막 IP 주소를 입력해야 합니다.Begin IP(시작 IP) 필드 및 End IP(종료 IP) 필드에서

IPSec 설정

VPN 터널의 양쪽 끝 간에 암호화를 제대로 설정하려면 두 암호화 모두 동일한 설정을 가져야 합니다.이 경우 IPSec은 두 디바이스 간에 보안 인증을 생성합니다.두 단계로 이루어집니다.

수동 키잉 모드에 대한 IPSec 설정

Add a New Tunnel(새 터널 추가)의 3단계에서 Keying Mode(키잉 모드) 드롭다운 목록에서 Manual(수동)을 선택한 경우에만 사용할 수 있습니다.이는 키로 협상하지 않고 직접 새 보안 키를 생성하는 사용자 지정 보안 모드입니다.이는 트러블슈팅 및 소규모 정적 환경에서 사용하는 것이 가장 좋습니다.



1단계. 들어오는 SPI 필드에 들어오는 SPI(Security Parameter Index)에 대한 고유한 16진수 값을 입력합니다.SPI는 ESP(Encapsulating Security Payload) 프로토콜 헤더에 포함되어 전달되며, 이 헤더는 함께 들어오는 패킷에 대한 보호를 결정합니다.100에서 FFFFFFFF까지 입력할 수 있습니다.

2단계. Outgoing SPI 필드에 SPI의 고유한 16진수 값을 입력합니다.SPI는 ESP 헤더에 전달되며, 이 헤더는 함께 발신 패킷에 대한 보호를 결정합니다.100에서 FFFFFFFF까지 입력할 수 있습니다.

참고:터널을 설정하려면 수신 및 발신 SPI가 양쪽 끝에서 서로 일치해야 합니다.

3단계. Encryption(암호화) 드롭다운 목록에서 적절한 암호화 방법을 선택합니다.권장되는 암호화는 3DES입니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

·DES — DES(Data Encryption Standard)는 56비트 이전 버전보다 호환성이 높은 암호화 방법으로, 깨지기 쉬우므로 안전하지 않습니다.

·3DES — 3DES(Triple Data Encryption Standard)는 168비트 간단한 암호화 방법으로, 데이터를 3회 암호화하여 키 크기를 증가시켜 DES보다 더 많은 보안을 제공합니다.

4단계. Authentication(인증) 드롭다운 목록에서 적절한 인증 방법을 선택합니다.권장되는 인증은 SHA1입니다. VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

·MD5 — MD5(Message Digest Algorithm-5)는 체크섬 계산에 의해 악의적인 공격으로부터

데이터를 보호하는 32자리 16진수 해시 함수를 나타냅니다.

·SHA1 — SHA1(Secure Hash Algorithm 버전 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.

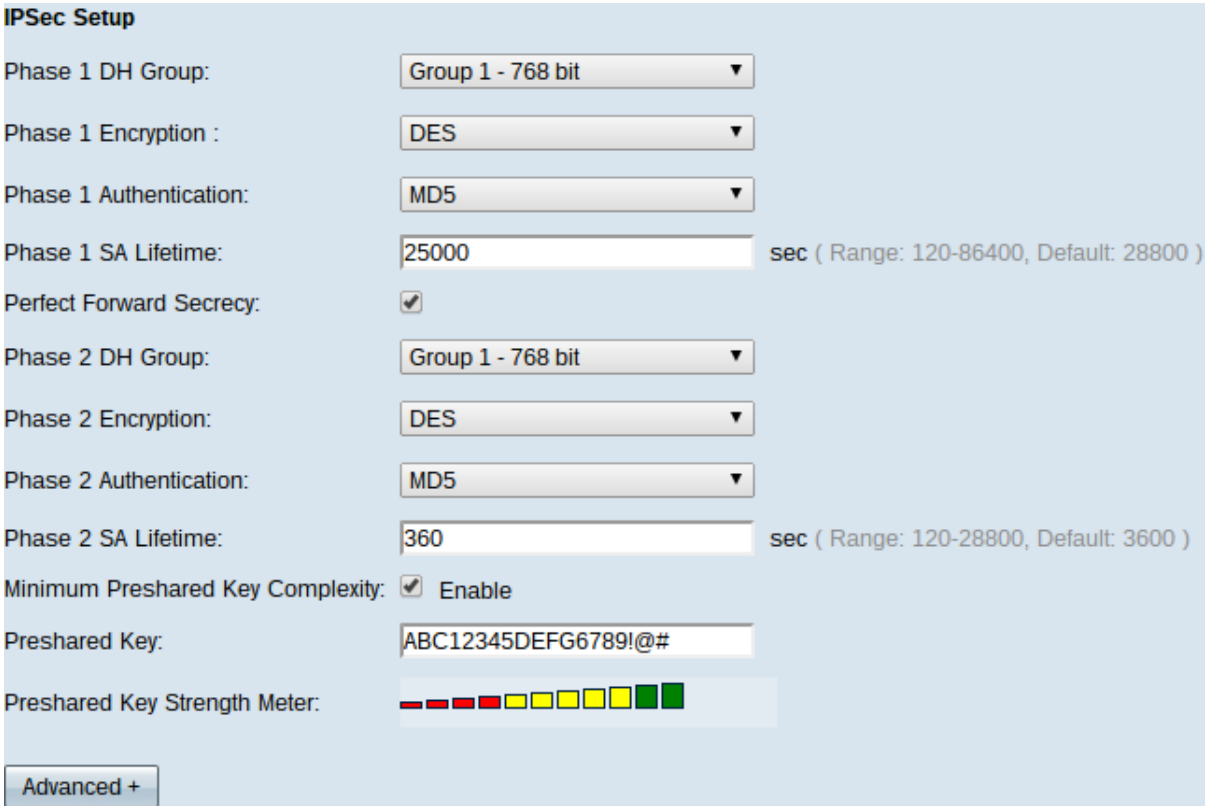
5단계. 암호화 키 필드에 데이터를 암호화하고 해독할 키를 입력합니다.3단계에서 DES를 암호화 방법으로 선택한 경우 16자리 16진수 값을 입력합니다.3단계에서 3DES를 암호화 방법으로 선택한 경우 40자리 16진수 값을 입력합니다.

6단계. Authentication Key(인증 키) 필드에 트래픽을 인증하려면 사전 공유 키를 입력합니다.4단계에서 인증 방법으로 MD5를 선택한 경우 32자리 16진수 값을 입력합니다.4단계에서 인증 방법으로 SHA를 선택한 경우 40자리 16진수 값을 입력합니다.VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

8단계. **저장**을 클릭하여 설정을 저장합니다.

사전 공유 키가 있는 IKE용 IPSec 설정

Add a New Tunnel(새 터널 추가)의 3단계에서 Keying Mode(키 지정 모드) 드롭다운 목록에서 Preshared key(사전 공유 키 포함)를 선택한 경우에만 사용할 수 있습니다.



1단계. 1단계 DH 그룹 드롭다운 목록에서 적절한 1단계 DH 그룹을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 논리적 SA(Security Association)를 설정하는 데 사용됩니다.DH(Diffie-Hellman)는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

·Group 1 - 768비트 — 최고 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.

·Group 2 - 1024비트 — 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 시간이 좀 필요합니다.

·Group 5 - 1536비트 — 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.IKE 키를 계산하는 데 소요되는 시간이 줄어듭니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.

2단계. Phase 1 Encryption(1단계 암호화)을 선택하여 Phase 1 Encryption(1단계 암호화) 드롭다운 목록에서 키를 암호화합니다.AES-128, AES-192 또는 AES-256이 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

·DES — DES(Data Encryption Standard)는 56비트, 오래된 암호화 방식이며 오늘날 매우 안전하지 않은 암호화 방법입니다.

·3DES — 3DES(Triple Data Encryption Standard)는 168비트 간단한 암호화 방법으로, 데이터를 3회 암호화하여 키 크기를 증가시켜 DES보다 더 많은 보안을 제공합니다.

·AES-128 — AES(Advanced Encryption Standard)는 128비트 암호화 방법으로 일반 텍스트를 암호 텍스트로 변환하여 10회 반복됩니다.

·AES-192 — 12주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 192비트 암호화 방법입니다.

·AES-256 — 14주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 256비트 암호화 방법입니다.

3단계. 1단계 인증 드롭다운 목록에서 적절한 인증 방법을 선택합니다.VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.SHA1이 권장됩니다.

·MD5 — MD5(Message Digest Algorithm-5)는 32자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의해 악의적인 공격으로부터 데이터를 보호합니다.

·SHA1 — MD5보다 더 안전한 160비트 해시 기능입니다.

4단계. Phase 1 SA Life Time 필드에 VPN 터널이 활성 상태로 유지되는 시간(초)을 입력합니다.

5단계. Perfect Forward Secrecy 확인란을 선택하여 키에 대한 보호를 강화합니다.이 옵션을 사용하면 키가 손상된 경우 새 키를 생성할 수 있습니다.암호화된 데이터는 감염된 키를 통해서만 감염됩니다.따라서 키가 손상되더라도 다른 키를 보호하므로 보다 안전하게 통신을 인증하고 인증합니다.이는 더 많은 보안을 제공하기 때문에 권장되는 작업입니다.

6단계. Phase 2 DH Group(2단계 DH 그룹) 드롭다운 목록에서 적절한 Phase 2 DH 그룹을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 논리적 SA(Security Association)를 설정하는 데 사용됩니다.DH는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

·Group 1 - 768비트 — 최고 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.

·Group 2 - 1024비트 — 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다. IKE 키를 계산하려면 시간이 좀 필요합니다.

·Group 5 - 1536비트 — 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.IKE 키를 계산하는 데 소요되는 시간이 줄어듭니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.

참고:새 키가 생성되지 않으므로 5단계에서 Perfect Forward Secrecy를 선택 취소하면 2단계

DH 그룹을 구성할 필요가 없습니다.

7단계. Phase 2 Encryption(2단계 암호화)을 선택하여 Phase 2 Encryption(2단계 암호화) 드롭다운 목록에서 키를 암호화합니다.AES-128, AES-192 또는 AES-256이 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

·DES — DES는 56비트 오래된 암호화 방식이며 오늘날 세계에서 매우 안전하지 않은 암호화 방법입니다.

·3DES — 3DES는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 키 크기를 증가시켜 DES보다 더 많은 보안을 제공합니다.

·AES-128 — AES는 128비트 암호화 방식으로 일반 텍스트를 암호 텍스트로 변환하여 10회 반복됩니다.

·AES-192 — 12주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 192비트 암호화 방법입니다.

·AES-256 — 14주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 256비트 암호화 방법입니다.

8단계. Phase 2 Authentication(2단계 인증) 드롭다운 목록에서 적절한 인증 방법을 선택합니다.VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

·MD5 — MD5는 32자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호합니다.

·SHA1 — SHA1(Secure Hash Algorithm version 1)은 MD5보다 더 안전한 160비트 해시 함수입니다.

·Null — 인증 방법이 사용되지 않습니다.

9단계. Phase 2 SA Life Time 필드에 VPN 터널이 활성 상태로 유지되는 시간을 초 단위로 입력합니다.

10단계. 사전 공유 키에 대해 강도 측정기를 활성화하려면 Minimum Preshared Key Complexity 확인란을 선택합니다.

11단계. 이전에 IKE 피어 간에 공유된 키를 Preshared Key 필드에 입력합니다.최대 30개의 16진수 및 문자를 사전 공유 키로 사용할 수 있습니다.VPN 터널은 양쪽 끝에 동일한 사전 공유 키를 사용해야 합니다.

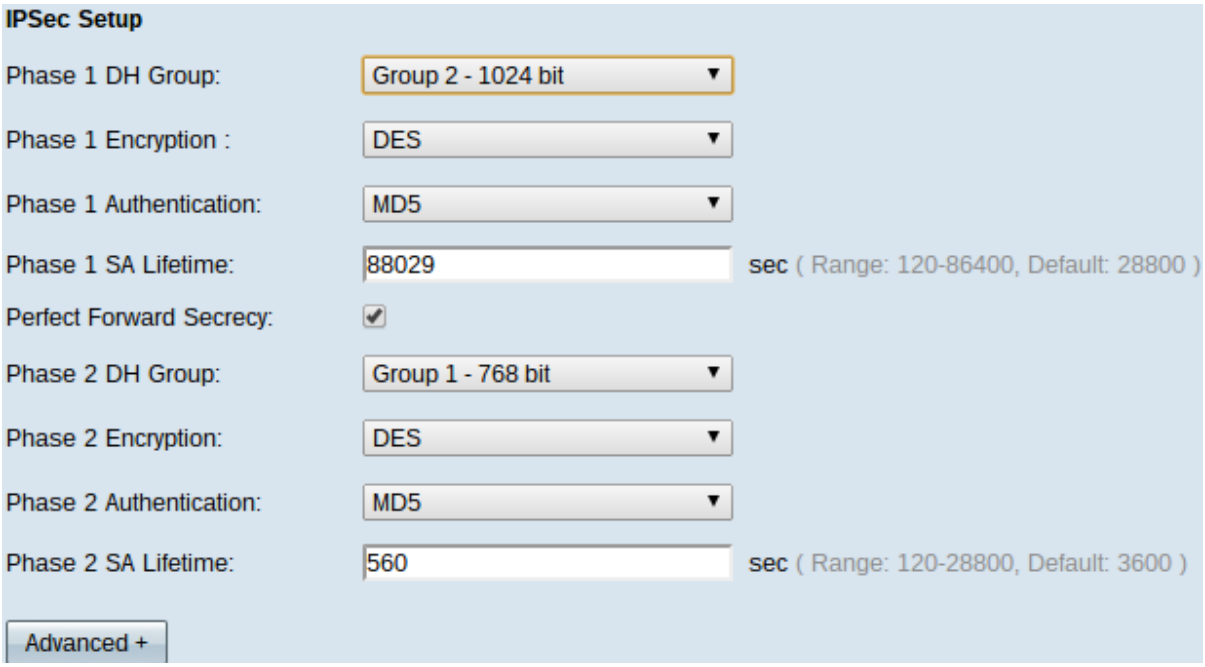
참고:VPN이 안전하게 유지되도록 IKE 피어 간에 사전 공유 키를 자주 변경하는 것이 좋습니다.

사전 공유 키 강도 측정기는 색상 막대를 통해 사전 공유 키의 강도를 보여줍니다.빨간색은 약한 강도를 나타내고, 노란색은 적정 강도를 나타내고, 녹색은 강한 힘을 나타냅니다.

12단계. **저장**을 클릭하여 설정을 저장합니다.

IKE용 IPSec 설정(인증서 포함)

Add a New Tunnel(새 터널 추가)의 3단계에서 Keying Mode(키 지정 모드) 드롭다운 목록에서 IKE with Certificate(인증서가 있는 IKE)를 선택한 경우에만 사용할 수 있습니다.



1단계. 1단계 DH 그룹 드롭다운 목록에서 적절한 1단계 DH 그룹을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 논리적 SA(Security Association)를 설정하는 데 사용됩니다.DH는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

·Group 1 - 768비트 — 최고 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.그러나 IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.

·Group 2 - 1024비트 — 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다.하지만 IKE 키를 계산하려면 시간이 좀 필요합니다.

·Group 5 - 1536비트 — 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.IKE 키를 계산하는 데 소요되는 시간이 줄어듭니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.

2단계. Phase 1 Encryption(1단계 암호화)을 선택하여 Phase 1 Encryption(1단계 암호화) 드롭다운 목록에서 키를 암호화합니다.AES-128, AES-192 또는 AES-256이 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

·DES — DES는 56비트 오래된 암호화 방식이며 오늘날 세계에서 매우 안전하지 않은 암호화 방법입니다.

·3DES — 3DES는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 키 크기를 증가시켜 DES보다 더 많은 보안을 제공합니다.

·AES-128 — AES는 128비트 암호화 방식으로 일반 텍스트를 암호 텍스트로 변환하여 10회 반복됩니다.

·AES-192 — 12주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 192비트 암호화 방법입니다.

·AES-256 — 14주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 256비트 암호화 방법입니다.

3단계. 1단계 인증 드롭다운 목록에서 적절한 인증 방법을 선택합니다.VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.SHA1이 권장됩니다.

·MD5 — MD5는 32자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호합니다.

·SHA1 — MD5보다 더 안전한 160비트 해시 기능입니다.

4단계. Phase 1 SA Life Time 필드에 VPN 터널이 활성 상태로 유지되는 시간(초)을 입력합니다.

5단계. Perfect Forward Secrecy 확인란을 선택하여 키에 대한 보호를 강화합니다.이 옵션을 사용하면 키가 손상된 경우 새 키를 생성할 수 있습니다.암호화된 데이터는 감염된 키를 통해서만 감염됩니다.따라서 다른 키가 손상되었을 때 다른 키를 보호하므로 더 안전하고 인증된 통신을 제공합니다.이는 더 많은 보안을 제공하기 때문에 권장되는 작업입니다.

6단계. Phase 2 DH Group(2단계 DH 그룹) 드롭다운 목록에서 적절한 Phase 2 DH 그룹을 선택합니다.1단계는 안전한 인증 통신을 지원하기 위해 터널의 양쪽 끝 사이에 단방향 논리적 SA를 설정하는 데 사용됩니다.DH는 통신을 인증하기 위해 1단계 연결 중에 비밀 키를 공유하는 데 사용되는 암호화 키 교환 프로토콜입니다.

·Group 1 - 768비트 — 최고 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.그러나 IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.

·Group 2 - 1024비트 — 더 높은 강도 키 및 더 안전한 인증 그룹을 나타냅니다.하지만 IKE 키를 계산하려면 시간이 좀 필요합니다.

·Group 5 - 1536비트 — 가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹을 나타냅니다.IKE 키를 계산하는 데 소요되는 시간이 줄어듭니다.네트워크 속도가 낮으면 이 옵션을 사용하는 것이 좋습니다.

참고:새 키가 생성되지 않으므로 5단계에서 Perfect Forward Secrecy를 선택하지 않은 경우 2단계 DH 그룹을 구성할 필요가 없습니다.

7단계. Phase 2 Encryption(2단계 암호화)을 선택하여 Phase 2 Encryption(2단계 암호화) 드롭다운 목록에서 키를 암호화합니다.AES-128, AES-192 또는 AES-256이 권장됩니다.VPN 터널은 양쪽 끝에 동일한 암호화 방법을 사용해야 합니다.

·DES — DES는 56비트 오래된 암호화 방식이며 오늘날 세계에서 매우 안전하지 않은 암호화 방법입니다.

·3DES — 3DES는 168비트의 간단한 암호화 방법으로, 데이터를 3회 암호화하여 키 크기를 증가시켜 DES보다 더 많은 보안을 제공합니다.

·AES-128 — AES는 128비트 암호화 방식으로 일반 텍스트를 암호 텍스트로 변환하여 10회 반복됩니다.

·AES-192 — 12주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 192비트 암호화 방법입니다.

·AES-256 — 14주기 반복을 통해 일반 텍스트를 암호 텍스트로 변환하는 256비트 암호화 방법입니다.

8단계. Phase 2 Authentication(2단계 인증) 드롭다운 목록에서 적절한 인증 방법을 선택합니다.VPN 터널은 양쪽 끝에 동일한 인증 방법을 사용해야 합니다.

·MD5 — MD5는 32자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호합니다.

·SHA1 — SHA1은 MD5보다 더 안전한 160비트 해시 함수입니다.

·Null — 인증 방법이 사용되지 않습니다.

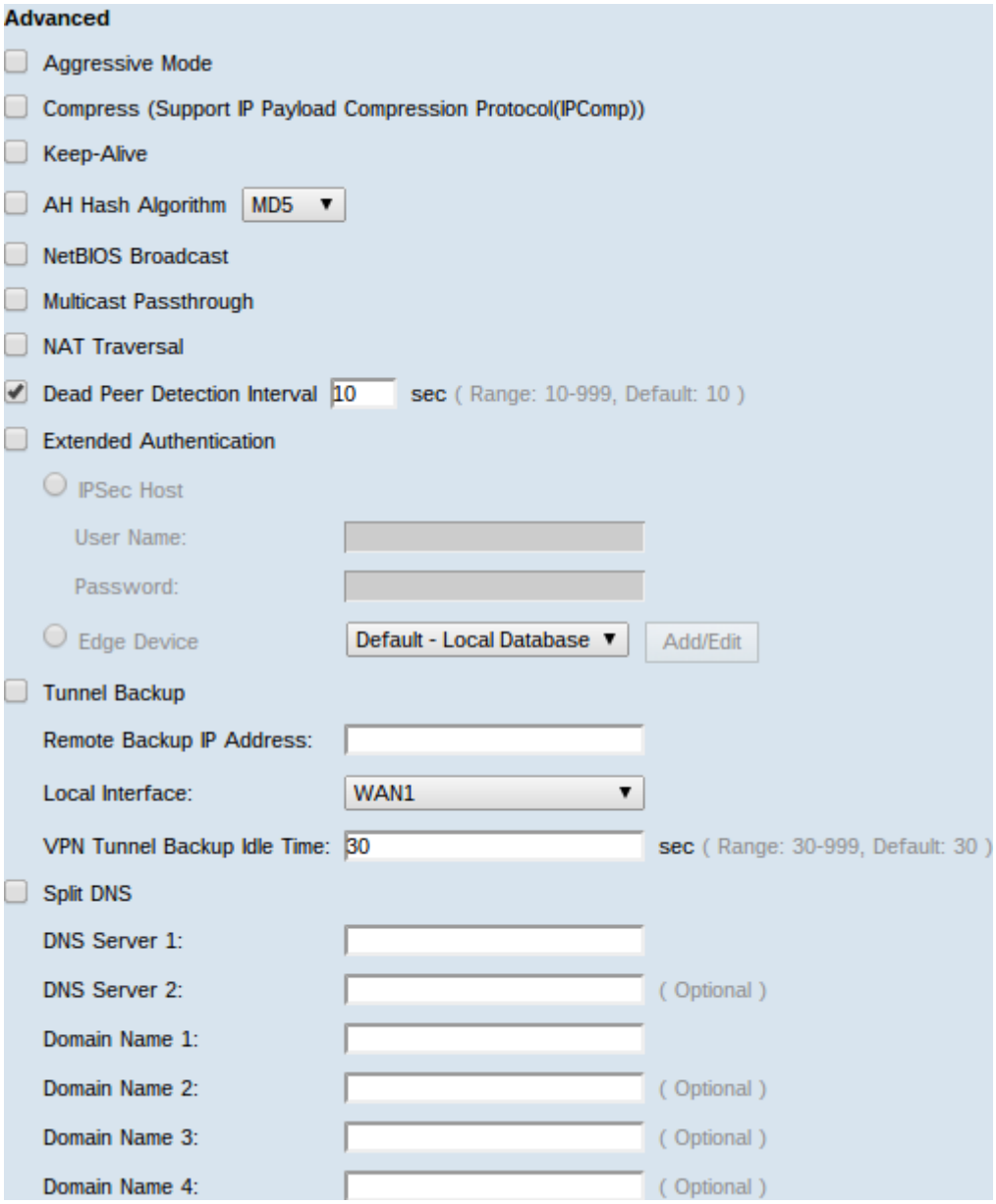
9단계. Phase 2 SA Life Time 필드에 VPN 터널이 활성 상태로 유지되는 시간을 초 단위로 입력합니다.

10단계. **저장**을 클릭하여 설정을 저장합니다.

(선택 사항) IKE용 IPSec 고급 설정(인증서 포함) 및 IKE에 사전 공유 키 사용

고급 옵션은 Add a New Tunnel(새 터널 추가)의 3단계에서 Keying Mode(키 모드) 드롭다운 목록에서 Certificate(인증서 포함) 또는 IKE with Pressed key(키를 누른 IKE)를 선택한 경우에 사용할 수 있습니다.두 가지 키 모드 유형에 대해 동일한 설정을 사용할 수 있습니다.

1단계. 고급 IPSec 옵션을 표시하려면 **Advanced**(고급+) 버튼을 클릭합니다.



2단계. 네트워크 속도가 낮으면 Aggressive Mode(적극적인 모드) 확인란을 선택합니다.SA를 연결하는 동안 터널의 엔드포인트의 ID를 일반 텍스트로 교환하므로 교환 시간은 적지만 보안은 낮습니다.

3단계. IP 데이터그램의 크기를 압축하려면 Compress (Support IP Payload Compression Protocol (IPComp)) 확인란을 선택합니다.IPComp는 IP 데이터그램의 크기를 압축하는 데 사용되는 IP 압축 프로토콜입니다. 네트워크 속도가 낮고 사용자가 저속 네트워크를 통해 손실 없이 신속하게 데이터를 전송하려는 경우,

4단계. VPN 터널의 연결이 항상 활성 상태로 유지되도록 하려면 Keep-Alive 확인란을 선택합니다.연결이 비활성화되면 즉시 연결을 재설정할 수 있습니다.

5단계. AH(Authenticate Header)를 인증하려면 AH Hash Algorithm 확인란을 선택합니다.AH는 데이터 원본에 대한 인증을 제공하며, 체크섬 및 보호를 통한 데이터 무결성은 IP 헤더로 확장됩니다.터널의 양쪽 알고리즘은 동일해야 합니다.

·MD5 — MD5는 128자리 16진수 해시 함수를 나타내며, 이는 체크섬 계산에 의한 악의적인 공격으로부터 데이터를 보호합니다.

·SHA1 — SHA1은 MD5보다 더 안전한 160비트 해시 함수입니다.

6단계. VPN 터널을 통해 라우팅 불가능한 트래픽을 허용하려면 NetBIOS 브로드캐스트를 확인합니다.기본값은 선택되지 않습니다.NetBIOS는 일부 소프트웨어 애플리케이션 및 Network Neighbor와 같은 Windows 기능을 통해 네트워크의 프린터, 컴퓨터 등의 네트워크 리소스를 탐지하는 데 사용됩니다.

7단계. VPN 라우터가 NAT 게이트웨이 뒤에 있는 경우 NAT 통과를 활성화하려면 확인란을 선택합니다.NAT(Network Address Translation)를 사용하면 프라이빗 LAN 주소를 가진 사용자가 공개적으로 라우팅 가능한 IP 주소를 소스 주소로 사용하여 인터넷 리소스에 액세스할 수 있습니다.그러나 인바운드 트래픽의 경우 NAT 게이트웨이는 공용 IP 주소를 프라이빗 LAN의 특정 대상으로 자동 변환하는 방법이 없습니다.이 문제는 IPSec 교환이 성공적으로 수행되지 않도록 합니다.NAT 통과는 이 인바운드 변환을 설정합니다.터널의 양쪽 끝에서 동일한 설정을 사용해야 합니다.

8단계. Dead Peer Detection Interval(데드 피어 탐지 간격)을 선택하여 Hello 또는 ACK를 통해 VPN 터널의 수명을 정기적으로 확인합니다.이 확인란을 선택하는 경우 원하는 hello 메시지의 기간 또는 간격을 초 단위로 입력합니다.

9단계. IPSec 호스트 사용자 이름 및 비밀번호를 사용하여 VPN 클라이언트를 인증하거나 User Management에 있는 데이터베이스를 사용하려면 Extended Authentication(확장 인증)을 선택합니다.두 디바이스에서 모두 활성화하여 작동해야 합니다.IPSec **호스트** 라디오 버튼을 클릭하여 IPSec 호스트 및 사용자 이름을 사용하고 사용자 이름 필드와 비밀번호 필드에 사용자 이름과 비밀번호를 입력합니다.또는 Edge **Device** 라디오 버튼을 클릭하여 데이터베이스를 사용합니다.Edge Device 드롭다운 목록에서 원하는 데이터베이스를 선택합니다.

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

·원격 백업 IP 주소 — 원격 피어를 위한 대체 IP입니다.이 필드에 원격 게이트웨이에 대해 이미 설정된 WAN IP를 입력합니다.

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

·VPN Tunnel Backup Idle Time — 기본 터널이 연결되지 않은 경우 백업 터널을 사용할 때 선택한 시간입니다.초 단위로 입력합니다.

11단계. 스플릿 DNS를 활성화하려면 Split DNS 확인란을 선택합니다.이 기능을 사용하면 지정된 도메인 이름을 기반으로 정의된 DNS 서버로 DNS 요청을 보낼 수 있습니다.DNS Server 1 및 DNS Server 2 필드에 DNS 서버 이름을 입력하고 Domain Name # 필드에 도메인 이름을 입력합니다.

12단계. **저장**을 클릭하여 디바이스 구성을 완료합니다.