RV215W에서 고급 VPN 설정

목표

VPN(Virtual Private Network)은 네트워크 또는 네트워크 간에 설정된 보안 연결입니다 .VPN은 지정된 호스트와 네트워크 간의 트래픽을 무단 호스트 및 네트워크의 트래픽으로부터 격리합니다.이 문서에서는 RV215W에서 Advanced VPN Setup을 구성하는 방법에 대해 설명합니다.

적용 가능한 디바이스

·RV215W

소프트웨어 버전

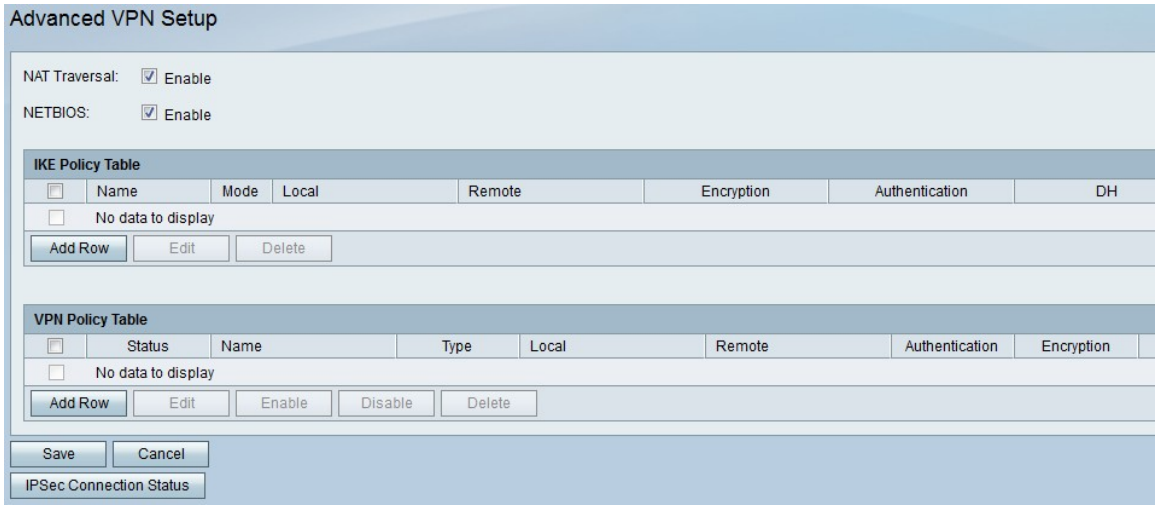
•1.1.0.5

고급 VPN 설정

초기 설정

이 절차에서는 고급 VPN 설정의 초기 설정을 구성하는 방법에 대해 설명합니다.

1단계. 웹 구성 유틸리티에 로그인하고 **VPN > Advanced VPN Setup**을 선택합니다.Advanced *VPN Setup* 페이지가 열립니다.



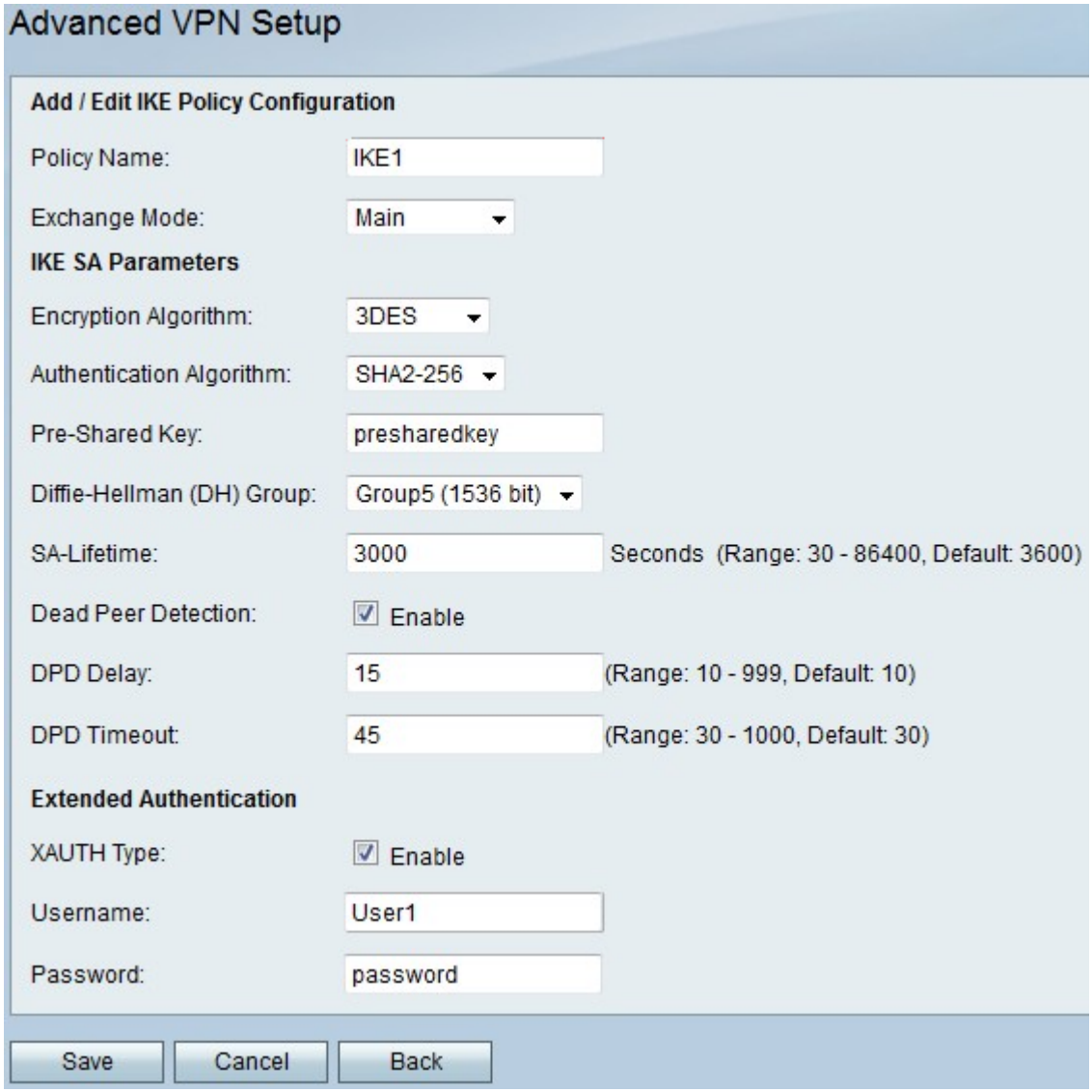
2단계. (선택 사항) VPN 연결에 대해 NAT(Network Address Translation) 통과를 활성화하려면 NAT Traversal 필드에서 Enable 확인란을 선택합니다.NAT 통과를 사용하면 NAT를 사용하는 게이트웨이 간에 VPN 연결을 설정할 수 있습니다.VPN 연결이 NAT 지원 게이트웨이를 통과하는 경우 이 옵션을 선택합니다.

3단계. (선택 사항) VPN 연결을 통해 전송될 Network Basic Input/Output System(NetBIOS) 브로드캐스트를 활성화하려면 NETBIOS 필드에서 Enable 확인란을 선택합니다.NetBIOS를 사용하면 호스트가 LAN 내에서 서로 통신할 수 있습니다.

IKE 정책 설정

IKE(Internet Key Exchange)는 VPN에서 통신을 위한 보안 연결을 설정하는 데 사용되는 프로토콜입니다.이렇게 설정된 보안 연결을 SA(Security Association)라고 합니다. 이 절차에서는 보안에 사용할 VPN 연결에 대한 IKE 정책을 구성하는 방법에 대해 설명합니다.VPN이 제대로 작동하려면 두 엔드포인트에 대한 IKE 정책이 동일해야 합니다.

1단계. IKE Policy Table(IKE 정책 테이블)에서 **Add Row(행 추가)**를 클릭하여 새 IKE 정책을 생성합니다.IKE 정책을 수정하려면 정책에 대한 확인란을 선택하고 Edit를 **클릭합니다** .Advanced *VPN Setup* 페이지가 변경됩니다.

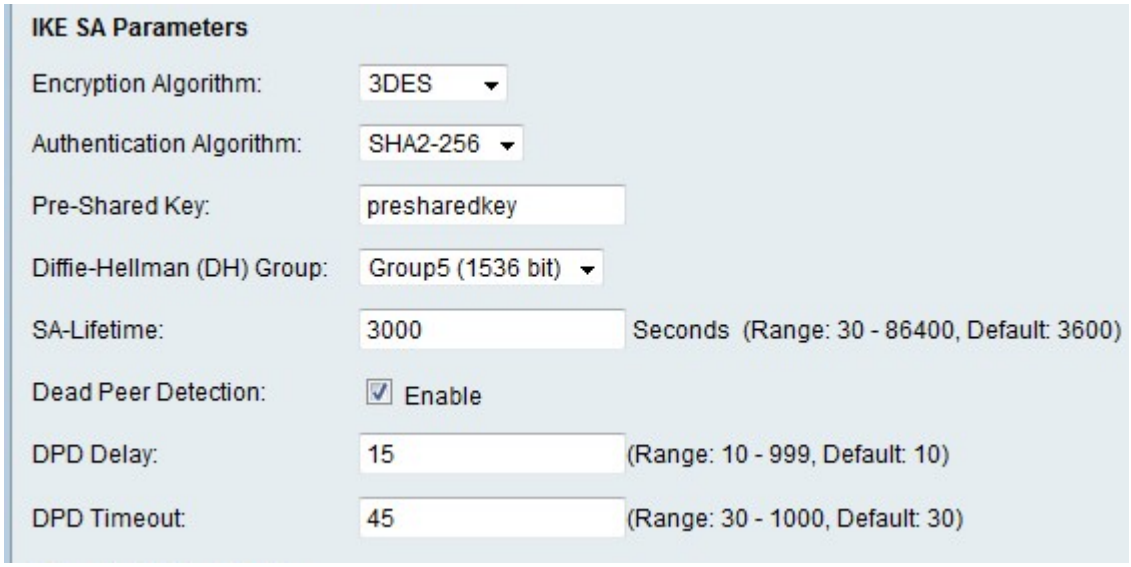


2단계. Policy Name(정책 이름) 필드에 IKE 정책의 이름을 입력합니다.

3단계. Exchange Mode 드롭다운 목록에서 옵션을 선택합니다.

·Main — 이 옵션을 사용하면 IKE 정책이 적극적인 모드보다 더 안전하면서도 속도가 느립니다.더 안전한 VPN 연결이 필요한 경우 이 옵션을 선택합니다.

·적극적인 — 이 옵션을 사용하면 IKE 정책을 주 모드보다 빠르고 안전하게 운영할 수 있습니다.더 빠른 VPN 연결이 필요한 경우 이 옵션을 선택합니다.



4단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 옵션을 선택합니다.

·DES — DES(Data Encryption Standard)는 56비트 오래된 암호화 방법이며, 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트 간단한 암호화 방법입니다.이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르고 안전합니다.AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

·AES-192 — AES-192는 AES 암호화를 위해 192비트 키를 사용합니다.AES-192는 AES-128보다 느리지만 안전성이 높고 AES-256보다 빠르지만 보안성이 낮습니다.

·AES-256 — AES-256은 AES 암호화를 위해 256비트 키를 사용합니다.AES-256은 AES-128 및 AES-192보다 느지만 안전합니다.

5단계. Authentication Algorithm(인증 알고리즘) 드롭다운 목록에서 옵션을 선택합니다.

·MD5 — MD5(Message-Digest Algorithm 5)는 인증에 128비트 해시 값을 사용합니다 .MD5는 안전하지 않지만 SHA-1 및 SHA2-256보다 빠릅니다.

·SHA-1 — SHA-1(Secure Hash Function 1)은 인증에 160비트 해시 값을 사용합니다.SHA-1은 MD5보다 느리지만 보안 수준이 더 높고, SHA-1은 SHA2-256보다 빠르지만 보안 수준이 낮습니다.

·SHA2-256 — 256비트 해시 값(SHA2-256)이 있는 보안 해시 알고리즘 2는 인증에 256비트 해시 값을 사용합니다.SHA2-256은 MD5 및 SHA-1보다 느리지만 안전합니다.

6단계. Pre-Shared Key 필드에 IKE 정책에서 사용하는 사전 공유 키를 입력합니다.

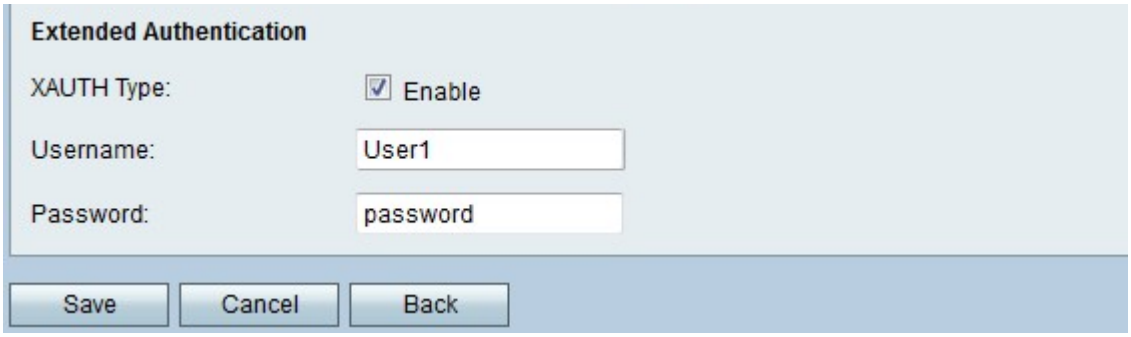
7단계. Diffie-Hellman(DH) Group(DH) 그룹) 드롭다운 목록에서 IKE가 사용하는 DH 그룹을 선택합니다.DH 그룹의 호스트는 서로 모르는 사이에 키를 교환할 수 있습니다.그룹 비트 번호가 높을수록 그룹의 보안이 강화됩니다.

8단계. SA-Lifetime 필드에 SA가 갱신되기 전에 VPN에 대한 SA가 지속되는 시간(초)을 입력합니다.

9단계. (선택 사항) DPD(Dead Peer Detection)를 활성화하려면 Enable 확인란을 Dead Peer Detection 필드에서 선택합니다.DPD는 IKE 피어를 모니터링하여 피어가 작동하지 않는지 확인합니다.DPD는 비활성 피어에 네트워크 리소스가 낭비되는 것을 방지합니다.

10단계. (선택 사항) 9단계에서 DPD를 활성화한 경우 DPD Delay(DPD 지연) 필드에 피어가 활동을 확인하는 빈도(초)를 입력합니다.

11단계. (선택 사항) 9단계에서 DPD를 활성화한 경우 DPD Timeout 필드에 비활성 피어가 삭제되기 전에 대기할 시간(초)을 입력합니다.



12단계(선택 사항) XAUTH Type(XAUTH 유형) 필드에서 Enable(활성화) 확인란을 선택하여 XAUTH(확장 인증)를 활성화합니다.XAUTH를 사용하면 여러 사용자가 각 사용자에 대해 VPN 정책이 아닌 단일 VPN 정책을 사용할 수 있습니다.

13단계(선택 사항) 12단계에서 XAUTH를 활성화한 경우 Username(사용자 이름) 필드에 정책에 사용할 사용자 이름을 입력합니다.

14단계(선택 사항) 12단계에서 XAUTH를 활성화한 경우 Password(비밀번호) 필드에 정책에 사용할 비밀번호를 입력합니다.

15단계. 저장을 **클릭합니다**.원래 *Advanced VPN Setup* 페이지가 다시 나타납니다.

VPN 정책 설정

이 절차에서는 VPN 연결에 사용할 VPN 정책을 구성하는 방법에 대해 설명합니다.VPN이 제대로 작동하려면 두 엔드포인트에 대한 VPN 정책이 동일해야 합니다.

1단계. VPN Policy Table(VPN 정책 테이블)에서 Add Row(**행 추가)**를 클릭하여 새 VPN 정책을 생성합니다.VPN 정책을 수정하려면 정책에 대한 확인란을 선택하고 Edit를 **클릭합니다**.Advanced *VPN Setup* 페이지가 변경됩니다.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name: VPN1

Policy Type: Manual Policy

Remote Endpoint: IP Address

209.165.201.1 (Hint: 1.2.3.4 or abc.com)

Local Traffic Selection

Local IP: Subnet

IP Address: 192.168.1.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP: Subnet

IP Address: 192.168.2.0 (Hint: 1.2.3.4)

Subnet Mask: 255.255.255.0 (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming: 0xABCD

SPI-Outgoing: 0x1234

Encryption Algorithm: AES-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Integrity Algorithm: SHA2-256

Key-In: 123456789012345678!

Key-Out: 123456789012345678!

Auto Policy Parameters

SA-Lifetime: 20000 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: AES-256

Integrity Algorithm: SHA2-256

PFS Key Group: Enable

DH-Group 1(768 bit)

Select IKE Policy: IKE1

2단계. Policy Name(정책 이름) 필드에 VPN 정책의 이름을 입력합니다.

3단계. Policy Type(정책 유형) 드롭다운 목록에서 옵션을 선택합니다.

·수동 정책 — 이 옵션을 사용하여 데이터 암호화 및 무결성을 위한 키를 구성할 수 있습니다.

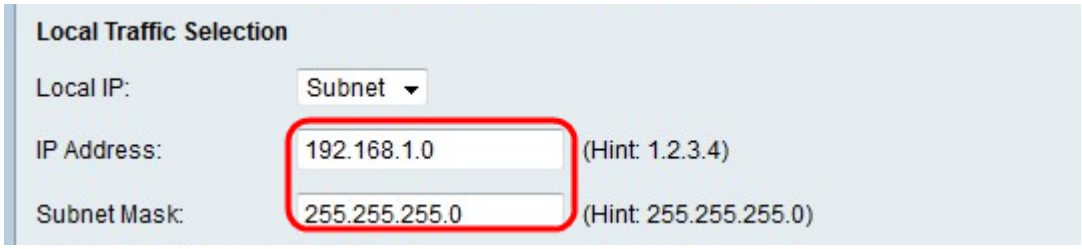
·자동 정책 — 이 옵션은 데이터 무결성 및 암호화 키 교환을 위해 IKE 정책을 사용합니다.

4단계. Remote Endpoint(원격 엔드포인트) 드롭다운 목록에서 옵션을 선택합니다.

·IP 주소 — 이 옵션은 공용 IP 주소로 원격 네트워크를 식별합니다.

·FQDN — 이 옵션은 원격 네트워크를 식별하는 데 FQDN(Fully Qualified Domain Name)을 사용합니다.

5단계. Remote Endpoint(원격 엔드포인트) 드롭다운 목록 아래의 텍스트 입력 필드에 원격 주소의 공용 IP 주소 또는 도메인 이름을 입력합니다.



6단계. Local IP(로컬 IP) 드롭다운 목록에서 옵션을 선택합니다.

·단일 — 이 옵션은 단일 호스트를 로컬 VPN 연결 지점으로 사용합니다.

·서브넷 — 이 옵션은 로컬 네트워크의 서브넷을 로컬 VPN 연결 지점으로 사용합니다.

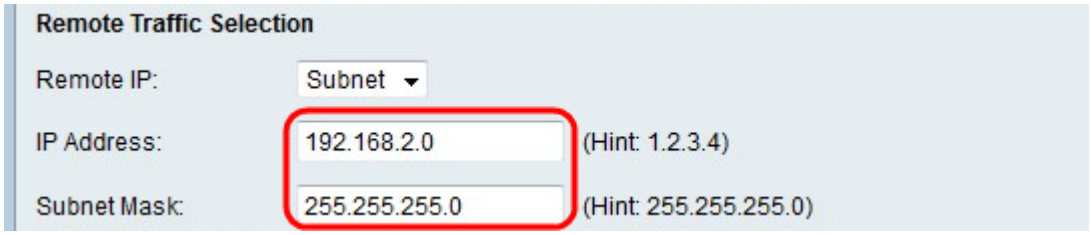
7단계. IP Address 필드에 로컬 서브넷 또는 호스트의 호스트 또는 서브넷 IP 주소를 입력합니다.

8단계. (선택 사항) 6단계에서 서브넷을 선택한 경우 Subnet Mask 필드에 로컬 서브넷의 서브넷 마스크를 입력합니다.

9단계. Remote IP(원격 IP) 드롭다운 목록에서 옵션을 선택합니다.

·단일 — 이 옵션은 단일 호스트를 원격 VPN 연결 지점으로 사용합니다.

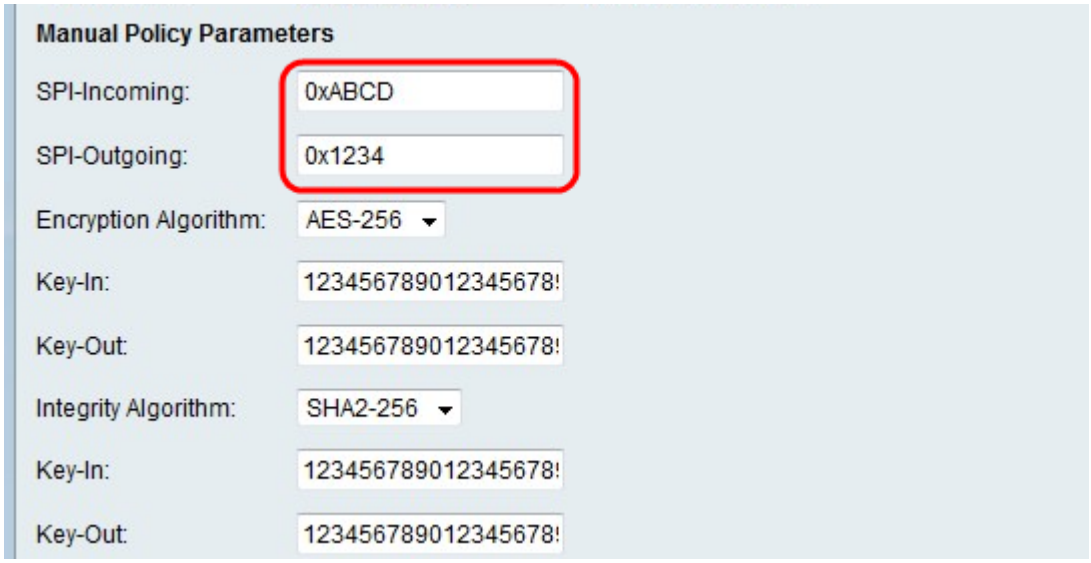
·서브넷 — 이 옵션은 원격 네트워크의 서브넷을 원격 VPN 연결 지점으로 사용합니다.



10단계. IP Address 필드에 원격 서브넷 또는 호스트의 호스트 또는 서브넷 IP 주소를 입력합니다.

11단계. (선택 사항) 9단계에서 서브넷을 선택한 경우 Subnet Mask 필드에 원격 서브넷의 서브넷 마스크를 입력합니다.

참고:3단계에서 Manual Policy(수동 정책)를 선택한 경우 12단계~19단계를 수행합니다.그렇지 않으면 20단계를 건너뜁니다.



12단계. SPI-Incoming 필드에 VPN 연결에서 들어오는 트래픽에 대한 SPI(Security Parameter Index) 태그에 3~8개의 16진수 문자를 입력합니다.SPI 태그는 한 세션의 트래픽과 다른 세션의 트래픽을 구분하는 데 사용됩니다.

13단계. SPI-Outgoing(SPI-발신) 필드에 VPN 연결의 발신 트래픽에 대한 SPI 태그의 3~8개의 16진수 문자를 입력합니다.

14단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 옵션을 선택합니다.

·DES — DES(Data Encryption Standard)는 56비트 오래된 암호화 방법이며, 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

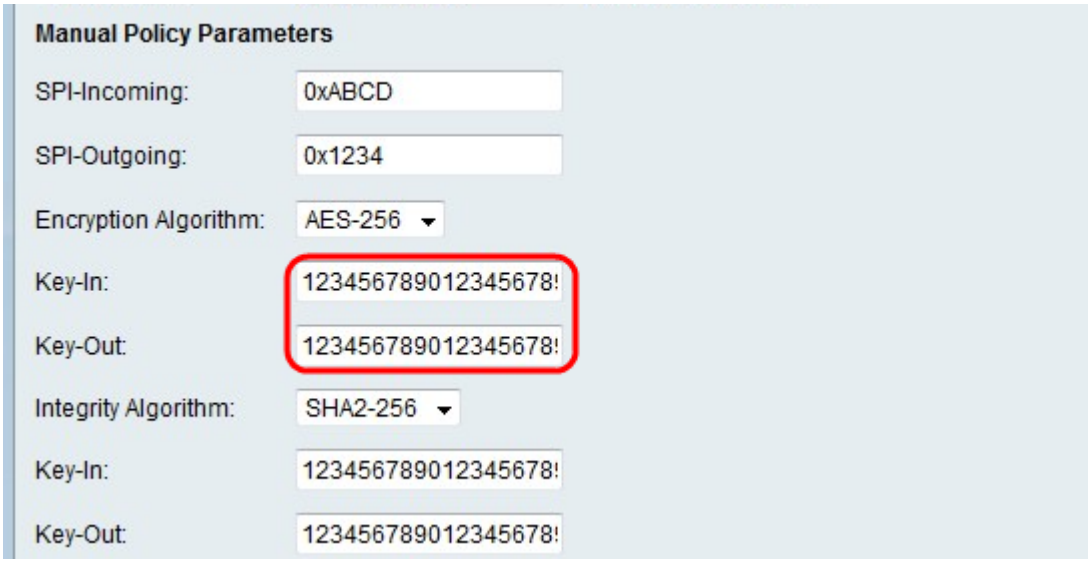
·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트 간단한 암호화 방법입니다.이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르고 안전합니다.AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

·AES-192 — AES-192는 AES 암호화를 위해 192비트 키를 사용합니다.AES-192는 AES-128보다 느리지만 안전성이 높고 AES-256보다 빠르지만 보안성이 낮습니다.

·AES-256 — AES-256은 AES 암호화를 위해 256비트 키를 사용합니다.AES-256은 AES-

128 및 AES-192보다 느지만 안전합니다.



15단계. Key-In 필드에 인바운드 정책의 키를 입력합니다.키 길이는 14단계에서 선택한 알고리즘에 따라 달라집니다.

·DES는 8자 키를 사용합니다.

·3DES는 24자 키를 사용합니다.

·AES-128은 12자 키를 사용합니다.

·AES-192는 24자 키를 사용합니다.

·AES-256은 32자 키를 사용합니다.

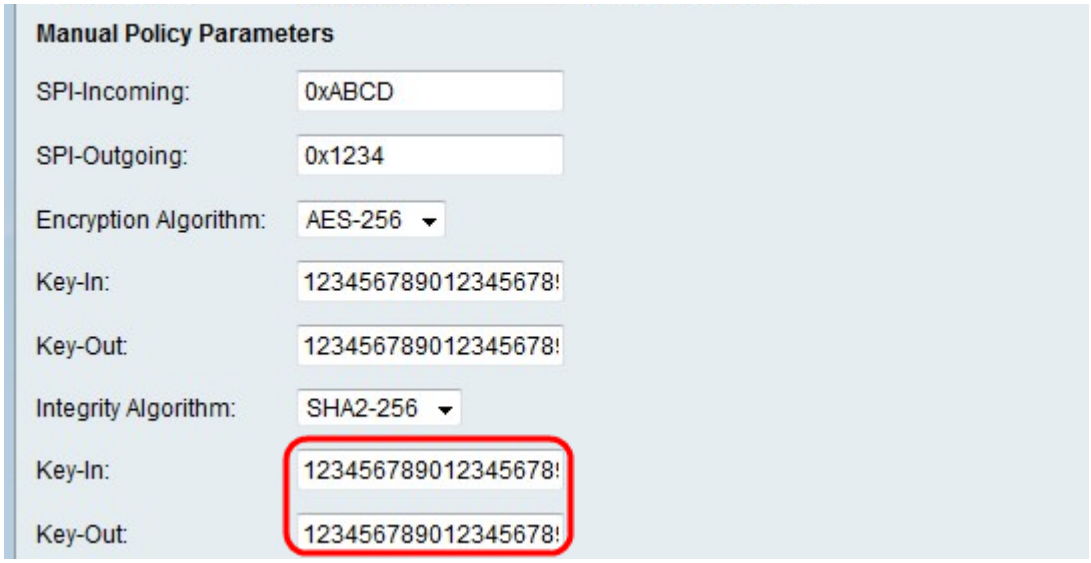
16단계. Key-Out(키 아웃) 필드에 발신 정책의 키를 입력합니다.키 길이는 14단계에서 선택한 알고리즘에 따라 다릅니다. 키 길이는 15단계와 동일합니다.

17단계. 무결성 알고리즘 드롭다운 목록에서 옵션을 선택합니다.

·MD5 — MD5(Message-Digest Algorithm 5)는 데이터 무결성을 위해 128비트 해시 값을 사용합니다.MD5는 안전하지 않지만 SHA-1 및 SHA2-256보다 빠릅니다.

·SHA-1 — SHA-1(Secure Hash Function 1)은 데이터 무결성을 위해 160비트 해시 값을 사용합니다.SHA-1은 MD5보다 느리지만 보안 수준이 더 높고, SHA-1은 SHA2-256보다 빠르지만 보안 수준이 낮습니다.

·SHA2-256 — 256비트 해시 값(SHA2-256)이 있는 Secure Hash Algorithm 2는 데이터 무결성을 위해 256비트 해시 값을 사용합니다.SHA2-256은 MD5 및 SHA-1보다 느리지만 안전합니다.



18단계. Key-In 필드에 인바운드 정책의 키를 입력합니다.키 길이는 17단계에서 선택한 알고리즘에 따라 달라집니다.

·MD5는 16자 키를 사용합니다.

·SHA-1은 20자 키를 사용합니다.

·SHA2-256은 32자 키를 사용합니다.

19단계. Key-Out(키 아웃) 필드에 발신 정책의 키를 입력합니다.키 길이는 17단계에서 선택한 알고리즘에 따라 다릅니다. 키 길이는 18단계와 동일합니다.

참고:3단계에서 Auto Policy(자동 정책)를 선택한 경우 20단계~25단계를 수행합니다.그렇지 않으면 26단계로 건너뜁니다.

20단계. SA-Lifetime 필드에 SA가 갱신되기 전에 유지되는 시간(초)을 입력합니다.

21단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 옵션을 선택합니다.

·DES — DES(Data Encryption Standard)는 56비트 오래된 암호화 방법이며, 매우 안전한 암호화 방법은 아니지만 이전 버전과의 호환성을 위해 필요할 수 있습니다.

·3DES — 3DES(Triple Data Encryption Standard)는 데이터를 세 번 암호화하므로 키 크기를 늘리는 데 사용되는 168비트 간단한 암호화 방법입니다.이는 DES보다 더 많은 보안을 제공하지만 AES보다 적은 보안을 제공합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르고 안전합니다.AES-128은 AES-192 및 AES-256보다 빠르지만 안전하지 않습니다.

·AES-192 — AES-192는 AES 암호화를 위해 192비트 키를 사용합니다.AES-192는 AES-128보다 느리지만 안전성이 높고 AES-256보다 빠르지만 보안성이 낮습니다.

·AES-256 — AES-256은 AES 암호화를 위해 256비트 키를 사용합니다.AES-256은 AES-128 및 AES-192보다 느지만 안전합니다.

22단계. 무결성 알고리즘 드롭다운 목록에서 옵션을 선택합니다.

·MD5 — MD5(Message-Digest Algorithm 5)는 데이터 무결성을 위해 128비트 해시 값을 사용합니다.MD5는 안전하지 않지만 SHA-1 및 SHA2-256보다 빠릅니다.

·SHA-1 — SHA-1(Secure Hash Function 1)은 데이터 무결성을 위해 160비트 해시 값을 사용합니다.SHA-1은 MD5보다 느리지만 보안 수준이 더 높고, SHA-1은 SHA2-256보다 빠르지만 보안 수준이 낮습니다.

·SHA2-256 — 256비트 해시 값(SHA2-256)이 있는 Secure Hash Algorithm 2는 데이터 무결성을 위해 256비트 해시 값을 사용합니다.SHA2-256은 MD5 및 SHA-1보다 느리지만 안전합니다.

23단계. PFS(Perfect Forward Secrecy)를 활성화하려면 PFS 키 그룹에서 Enable(활성화) 확인란을 선택합니다.PFS는 VPN 보안을 향상하지만 연결 속도를 지연시킵니다.

24단계. (선택 사항) 23단계에서 PFS를 활성화하도록 선택한 경우 아래 드롭다운 목록에 참여할 DH(Diffie-Hellman) 그룹을 선택합니다.그룹 번호가 높을수록 그룹의 보안이 강화됩니다.

25단계. Select IKE Policy(IKE 정책 선택) 드롭다운 목록에서 VPN 정책에 사용할 IKE 정책을 선택합니다.

참고: View(**보기**)를 클릭하면 *Advanced VPN Setup* 페이지의 IKE 컨피그레이션 섹션으로 이동합니다.

26단계. **저장**을 클릭합니다.원래 *Advanced VPN Setup* 페이지가 다시 나타납니다.

27단계. **저장**을 클릭합니다.