

# RV110W 방화벽에서 고급 VPN(Virtual Private Network) 설정 구성

## 목표

VPN(Virtual Private Network)은 공용 네트워크 또는 인터넷을 사용하여 안전하게 통신하기 위한 사설 네트워크를 설정합니다. IKE(Internet Key Exchange)는 두 네트워크 간의 보안 통신을 설정하는 프로토콜입니다. 트래픽 흐름 전에 키를 교환하는 데 사용되며, 이는 VPN 터널의 양쪽 끝에 대한 신뢰성을 보장합니다.

VPN의 양쪽 끝은 동일한 VPN 정책을 따라 서로 정상적으로 통신해야 합니다.

이 문서의 목적은 RV110W 무선 라우터에서 IKE 프로필을 추가하고 VPN 정책을 구성하는 방법을 설명하는 것입니다.

## 적용 가능한 디바이스

·RV110W

## 소프트웨어 버전

·1.2.0.9

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

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
No data to display							
Add Row Edit Delete							

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
No data to display							
Add Row Edit Enable Disable Delete							

Save Cancel

IPSec Connection Status

**Advanced VPN Setup**

**IKE Policy Table**

<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	No data to display			

**Add Row**   **Edit**   **Delete**

**VPN Policy Table**

<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			

**Add Row**   **Edit**   **Enable**   **Disable**   **Delete**

**Save**   **Cancel**

**IPSec Connection Status**

2단계. 새 IKE 정책을 생성하려면 Add Row를 클릭합니다. Advanced VPN Setup 페이지가 열립니다.

**Advanced VPN Setup**

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

**Save**   **Cancel**   **Back**

3단계. Policy Name(정책 이름) 필드에 쉽게 식별할 IKE 정책의 이름을 입력합니다.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode: Main ▼  
Main  
Aggressive

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

4단계. *Exchange Mode* 드롭다운 목록에서 옵션을 선택합니다.

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

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

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm: 

- AES-128
- DES
- 3DES
- AES-128
- AES-192
- AES-256

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

5단계. Encryption Algorithm 드롭다운 목록에서 알고리즘을 선택합니다.

·DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다. DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

·3DES — 3DES(Triple Data Encryption Standard)는 DES를 3번 수행하지만 수행되는 DES 라운드에 따라 키 크기가 168비트에서 112비트로, 112비트에서 56비트로 달라집니다. 3DES는 DES 및 AES보다 안전합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다. AES는 DES보다 빠르고 안전합니다. 일반적으로 AES는 3DES보다 빠르지만 보안 수준이 낮지만 일부 유형의 하드웨어로 인해 3DES가 더 빠릅니다. 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-192는 AES-256보다 빠르지만 안전성이 낮습니다.

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

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm: 

- SHA-1
- MD5
- SHA-1
- SHA2-256

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

6단계. Authentication *Algorithm* 드롭다운 목록에서 원하는 인증을 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.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

**Pre-Shared Key:**

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

7단계. *Pre-Shared Key*(사전 공유 키) 필드에 IKE 정책에서 사용하는 사전 공유 키를 입력합니다.

### Advanced VPN Setup

**Add / Edit IKE Policy Configuration**

Policy Name:

Exchange Mode:

**IKE SA Parameters**

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

8단계. *Diffie-Hellman(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.

·Group 1 - 768비트 —가장 낮은 강도 키 및 가장 안전하지 않은 인증 그룹입니다. 그러나 IKE 키를

계산하는 데 시간이 덜 걸립니다.네트워크 속도가 낮은 경우 이 옵션을 사용하는 것이 좋습니다.

·Group 2 - 1024비트 — 고급 키 및 더 안전한 인증 그룹이지만 IKE 키를 계산하려면 시간이 좀 필요합니다.

·Group 5 - 1536비트 — 최고 강도 키 및 가장 안전한 인증 그룹을 나타냅니다.IKE 키를 계산하려면 더 많은 시간이 필요합니다.네트워크 속도가 높으면 이 옵션을 사용하는 것이 좋습니다.

Advanced VPN Setup

Add / Edit IKE Policy Configuration

Policy Name:

Exchange Mode:

IKE SA Parameters

Encryption Algorithm:

Authentication Algorithm:

Pre-Shared Key:

Diffie-Hellman (DH) Group:

SA-Lifetime:  Seconds (Range: 30 - 86400, Default: 3600)

Dead Peer Detection:  Enable

DPD Delay:  (Range: 10 - 999, Default: 10)

DPD Timeout:  (Range: 30 - 1000, Default: 30)

9단계. SA가 갱신되기 전에 VPN에 대한 SA가 지속되는 기간(초)을 SA-Lifetime 필드에 입력합니다

10단계. (선택 사항) Dead Peer Detection(데드 피어 탐지) 필드에서 Enable(활성화) 확인란을 선택하여 Dead Peer Detection(데드 피어 탐지)을 활성화합니다.증서 피어 탐지는 IKE 피어를 모니터링하여 피어가 작동하지 않는지 확인합니다.Dead Peer Detection(데드 피어 탐지)은 비활성 피어의 네트워크 리소스 낭비를 방지합니다.

11단계. (선택 사항) 9단계에서 DPEER 탐지를 활성화한 경우, DPEER(증서 피어 지연) 필드에서 피어가 활동을 확인하는 빈도(초)를 입력합니다.

12단계. (선택 사항) 9단계에서 Detection Peer Detection을 활성화한 경우 비활성 피어가 삭제될 때까지 대기할 시간(초)을 Detection Peer Detection Timeout 필드에 입력합니다.

13단계. 저장을 클릭하여 모든 설정을 적용합니다.

## VPN 정책 컨피그레이션

1단계. 웹 컨피그레이션 유틸리티에 로그인하고 VPN>Advanced VPN Setup을 선택합니다  
.Advanced VPN Setup 페이지가 열립니다.

## Advanced VPN Setup

IKE Policy Table							
<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>					

VPN Policy Table							
<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input type="checkbox"/>	No data to display						
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>			

## Advanced VPN Setup



Configuration settings have been saved successfully

IKE Policy Table				
<input type="checkbox"/>	Name	Mode	Local	Remote
<input type="checkbox"/>	policy1	Aggressive		
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

VPN Policy Table				
<input type="checkbox"/>	Status	Name	Type	Local
<input type="checkbox"/>	No data to display			
<input type="button" value="Add Row"/>	<input type="button" value="Edit"/>	<input type="button" value="Enable"/>	<input type="button" value="Disable"/>	<input type="button" value="Delete"/>

2단계. VPN Policy(VPN 정책) 테이블에서 Add Row(행 추가)를 클릭합니다. Advanced VPN Policy Setup 창이 나타납니다.

## Advanced VPN Setup

### Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

### Local Traffic Selection

Local IP:

IP Address:  (Hint: 1.2.3.4)

Subnet Mask:  (Hint: 255.255.255.0)

### Remote Traffic Selection

Remote IP:



## VPN 정책 구성 추가/수정

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

1단계. Policy Name(정책 이름) 필드에 정책의 고유한 이름을 입력하여 쉽게 식별합니다.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

2단계. Policy Type 드롭다운 목록에서 적절한 정책 유형을 선택합니다.

·자동 정책 — 매개변수를 자동으로 설정할 수 있습니다.이 경우 정책 외에도 IKE(Internet Key Exchange) 프로토콜이 두 VPN 엔드포인트 간에 협상해야 합니다.

·수동 정책 — 이 경우 VPN 터널 키에 대한 설정을 포함하는 모든 설정은 각 엔드포인트에 대해 수동으로 입력됩니다.

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:  (Hint: 1.2.3.4 or abc.com)

3단계. Remote Endpoint(원격 엔드포인트) 드롭다운 목록에서 원격 엔드포인트에서 게이트웨이를 식별하는 IP 식별자 유형을 선택합니다.

·IP 주소 — 원격 엔드포인트에서 게이트웨이의 IP 주소입니다.이 옵션을 선택하는 경우 필드에 IP 주소를 입력합니다.

·FQDN (Fully Qualified Domain Name) — 원격 끝점에 있는 게이트웨이의 정규화된 도메인 이름을 입력합니다. 이 옵션을 선택하는 경우 제공된 필드에 정규화된 도메인 이름을 입력합니다.

## 로컬 트래픽 선택

Local Traffic Selection	
Local IP:	<input type="text" value="Single"/> <input type="button" value="v"/>
IP Address:	<input type="text" value="Single"/> <input type="text" value="Subnet"/> (Hint: 1.2.3.4)
Subnet Mask:	<input type="text"/> (Hint: 255.255.255.0)

1단계. Local IP 드롭다운 목록에서 엔드포인트에 대해 제공할 식별자 유형을 선택합니다.

Local Traffic Selection	
Local IP:	<input type="text" value="Single"/> <input type="button" value="v"/>
IP Address:	<input type="text" value="192.168.1.1"/> (Hint: 1.2.3.4)
Subnet Mask:	<input type="text"/> (Hint: 255.255.255.0)

·단일 — 정책을 하나의 호스트로 제한합니다.이 옵션을 선택하는 경우 IP 주소 필드에 IP 주소를 입력합니다.

Local Traffic Selection	
Local IP:	<input type="text" value="Subnet"/> <input type="button" value="v"/>
IP Address:	<input type="text" value="192.168.1.1"/> (Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.255.255.0"/> (Hint: 255.255.255.0)

·서브넷 — IP의 경계를 정의하는 마스크입니다.이렇게 하면 지정된 서브넷의 호스트만 VPN에 연결할 수 있습니다.VPN에 연결하려면 논리 AND 작업에 의해 컴퓨터가 선택됩니다.IP가 필요한 동일한 범위에 속하는 경우 컴퓨터가 선택됩니다.이 옵션을 선택하는 경우 IP 주소 및 서브넷 필드에 IP 주소와 서브넷을 입력합니다.

## 원격 트래픽 선택

Remote Traffic Selection	
Remote IP:	<input type="text" value="Single"/> <input type="button" value="v"/>
IP Address:	<input type="text" value="Single"/> <input type="text" value="Subnet"/> (Hint: 1.2.3.4)
Subnet Mask:	<input type="text"/> (Hint: 255.255.255.0)

1단계. Local IP 드롭다운 목록에서 엔드포인트에 제공할 식별자 유형을 선택합니다.

Remote Traffic Selection	
Remote IP:	<input type="text" value="Single"/> <input type="button" value="v"/>
IP Address:	<input type="text" value="192.168.1.5"/> (Hint: 1.2.3.4)
Subnet Mask:	<input type="text"/> (Hint: 255.255.255.0)

·단일 — 정책을 하나의 호스트로 제한합니다.이 옵션을 선택하는 경우 IP 주소 필드에 IP 주소를 입력합니다.

Remote Traffic Selection		
Remote IP:	Subnet ▼	
IP Address:	192.168.1.5	(Hint: 1.2.3.4)
Subnet Mask:	255.255.255.0	(Hint: 255.255.255.0)

·서브넷 — IP의 경계를 정의하는 마스크입니다.이렇게 하면 지정된 서브넷의 호스트만 VPN에 연결할 수 있습니다.VPN에 연결하려면 논리 AND 작업에 의해 컴퓨터가 선택됩니다.IP가 필요한 동일한 범위에 속하는 경우 컴퓨터가 선택됩니다.이 옵션을 선택하는 경우 IP 주소 및 서브넷 필드에 IP 주소와 서브넷을 입력합니다.

## 수동 정책 매개변수

Manual Policy Parameters(수동 정책 매개변수)를 구성하려면 Add/Edit VPN Policy Configuration(VPN 정책 컨피그레이션 추가/수정) 섹션의 2단계의 Policy Type(정책 유형) 드롭다운 목록에서 Manual Policy(수동 정책)를 선택합니다.

Manual Policy Parameters	
SPI-Incoming:	014C
SPI-Outgoing:	014C
Encryption Algorithm:	AES-128 ▼
Key-In:	
Key-Out:	
Integrity Algorithm:	SHA-1 ▼
Key-In:	
Key-Out:	

1단계. SPI-Incoming 필드에 3에서 8 사이의 16진수 값을 입력합니다.SPI(Stateful Packet Inspection)는 Deep Packet Inspection이라고 하는 기술입니다.SPI는 컴퓨터 네트워크를 안전하게 유지하는 데 도움이 되는 다양한 보안 기능을 구현합니다.SPI-Incoming 값은 이전 장치의 SPI-Outgoing에 해당합니다.원격 VPN 엔드포인트의 SPI-Outgoing 필드에 동일한 값이 있는 경우 모든 값이 허용됩니다.

2단계. SPI-Outgoing 필드에 3에서 8 사이의 16진수 값을 입력합니다.

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm: 


- 3DES
- DES
- AES-128
- AES-192
- AES-256

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

3단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 적절한 암호화 알고리즘을 선택합니다.

·DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다. DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

·3DES — 3DES(Triple Data Encryption Standard)는 DES를 3번 수행하지만 수행되는 DES 라운드에 따라 키 크기가 168비트에서 112비트로, 112비트에서 56비트로 달라집니다. 3DES는 DES 및 AES보다 안전합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다. AES는 DES보다 빠르고 안전합니다. 일반적으로 AES는 3DES보다 빠르지만 보안 수준이 낮지만 일부 유형의 하드웨어로 인해 3DES가 더 빠릅니다. 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-192는 AES-256보다 빠르지만 보안성이 낮습니다.

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

**Manual Policy Parameters**

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

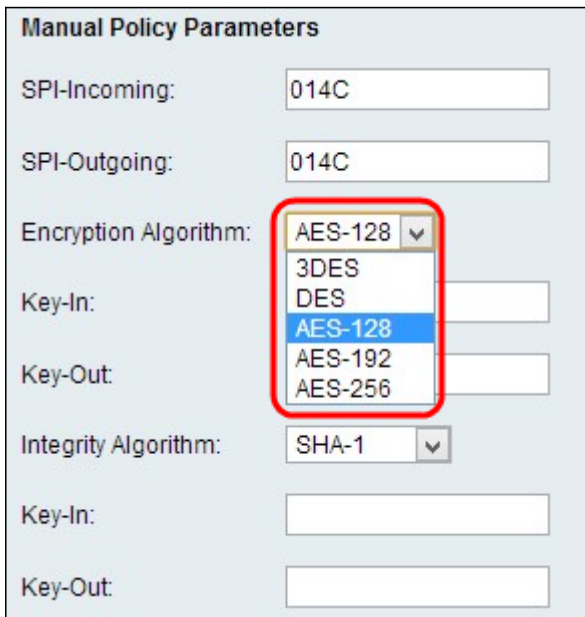
Key-In:

Key-Out:

4단계. Key-In 필드에 인바운드 정책의 암호화 키를 입력합니다. 키의 길이는 3단계에서 선택한 알

고리즘에 따라 달라집니다.

5단계. Key-Out 필드에 아웃바운드 정책의 암호화 키를 입력합니다.



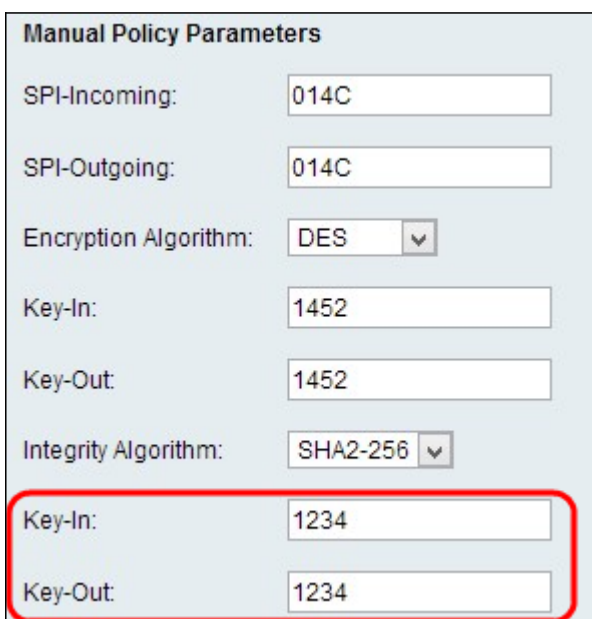
The screenshot shows the 'Manual Policy Parameters' form. The 'Encryption Algorithm' dropdown menu is open, showing options: AES-128 (selected), 3DES, DES, AES-128, AES-192, and AES-256. Other fields include SPI-Incoming: 014C, SPI-Outgoing: 014C, Integrity Algorithm: SHA-1, and empty Key-In and Key-Out fields.

6단계. 무결성 알고리즘 드롭다운 목록에서 적절한 무결성 알고리즘을 선택합니다.이 알고리즘은 데이터의 무결성을 확인합니다.

·MD5 — 이 알고리즘은 키 길이를 16자로 지정합니다.MD5(Message-Digest Algorithm 5)는 충돌 방지 기능이 아니며 이 속성을 사용하는 SSL 인증서 또는 디지털 서명 등의 애플리케이션에 적합합니다.MD5는 모든 바이트 스트림을 128비트 값으로 압축하지만 SHA는 160비트 값으로 압축합니다 .MD5는 컴퓨팅이 약간 더 저렴하지만 MD5는 이전 버전의 해시 알고리즘이며 충돌 공격에 취약합니다.

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

·SHA2-256 — 이 알고리즘은 키 길이를 32자로 지정합니다.



The screenshot shows the 'Manual Policy Parameters' form with the following values: SPI-Incoming: 014C, SPI-Outgoing: 014C, Encryption Algorithm: DES, Key-In: 1452, Key-Out: 1452, Integrity Algorithm: SHA2-256. The bottom two rows, Key-In: 1234 and Key-Out: 1234, are highlighted with a red box.

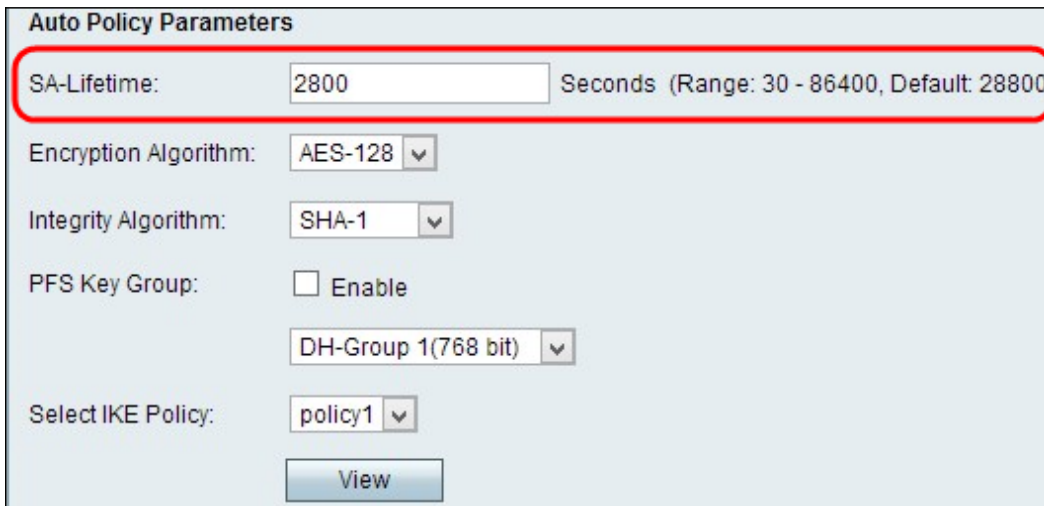
7단계. 인바운드 정책의 무결성 키(무결성 모드가 있는 ESP의 경우)를 입력합니다.키의 길이는 6단계에서 선택한 알고리즘에 따라 달라집니다.

8단계. Key-Out 필드에 아웃바운드 정책의 무결성 키를 입력합니다.VPN 연결은 인바운드 투 바운

드에 대해 설정되므로 한 쪽 끝의 아웃바운드 키는 다른 쪽 끝의 인바운드 키와 일치해야 합니다.

**참고:**성공적으로 연결하려면 VPN 터널의 다른 쪽 끝에서 SPI-Incoming 및 Outgoing, Encryption Algorithm, Integrity Algorithm 및 Keys가 동일해야 합니다.

### 자동 정책 매개변수



1단계. SA 수명 필드에 SA(Security Association) 기간을 초 단위로 입력합니다.SA 수명은 키가 수명이 되면 연결된 SA가 자동으로 재협상됩니다.



2단계. Encryption Algorithm(암호화 알고리즘) 드롭다운 목록에서 적절한 암호화 알고리즘을 선택합니다.

·DES — DES(Data Encryption Standard)는 데이터 암호화에 56비트 키 크기를 사용합니다.DES는 오래되었으며 하나의 엔드포인트가 DES만 지원하는 경우에만 사용해야 합니다.

·3DES — 3DES(Triple Data Encryption Standard)는 DES를 3번 수행하지만 수행되는 DES 라운드에 따라 키 크기가 168비트에서 112비트로, 112비트에서 56비트로 달라집니다.3DES는 DES 및 AES보다 안전합니다.

·AES-128 — 128비트 키(AES-128)가 포함된 고급 암호화 표준은 AES 암호화를 위해 128비트 키를 사용합니다.AES는 DES보다 빠르고 안전합니다.일반적으로 AES는 3DES보다 빠르지만 보안 수준이 낮지만 일부 유형의 하드웨어로 인해 3DES가 더 빠릅니다.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-192는 AES-256보다 빠르지만 안전성이 낮습니다.

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

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1 (selected), SHA-1, SHA2-256, MD5

PFS Key Group: DH-Group 1(768 bit)

Select IKE Policy: policy1

View

3단계. Integrity Algorithm(무결성 알고리즘) 드롭다운 목록에서 적절한 무결성 알고리즘을 선택합니다.이 알고리즘은 데이터의 무결성을 확인합니다.

·MD5 — 이 알고리즘은 키 길이를 16자로 지정합니다.MD5(Message-Digest Algorithm 5)는 충돌 방지 기능이 아니며 이 속성을 사용하는 SSL 인증서 또는 디지털 서명 등의 애플리케이션에 적합합니다.MD5는 모든 바이트 스트림을 128비트 값으로 압축하지만 SHA는 160비트 값으로 압축합니다.MD5는 컴퓨팅이 약간 더 저렴하지만 MD5는 이전 버전의 해시 알고리즘이며 충돌 공격에 취약합니다.

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

·SHA2-256 — 이 알고리즘은 키 길이를 32자로 지정합니다.

Auto Policy Parameters

SA-Lifetime: 2800 Seconds (Range: 30 - 86400, Default: 28800)

Encryption Algorithm: DES

Integrity Algorithm: SHA-1

PFS Key Group:  Enable

DH-Group 1(768 bit)

Select IKE Policy: policy1

View

4단계. (선택 사항) 보안을 개선하기 위해 PFS Key Group(PFS 키 그룹) 필드에서 Enable(활성화) 확인란을 선택합니다.

5단계. **Enable**(4단계 활성화)을 선택한 경우 PFS Key Group(PFS 키 그룹) 필드 드롭다운 목록에서 적절한 Diffie-Hellman 키 교환을 선택합니다.

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

6단계. **Select IKE Policy(IKE 정책 선택)** 드롭다운 목록에서 적절한 IKE 정책을 선택합니다 .IKE(Internet Key Exchange)는 VPN에서 통신을 위한 보안 연결을 설정하는 데 사용되는 프로토콜 입니다.이렇게 설정된 보안 연결을 SA(Security Association)라고 합니다. VPN이 제대로 작동하려면 두 엔드포인트에 대한 IKE 정책이 동일해야 합니다.

7단계. **Save(저장)**를 클릭하여 모든 설정을 적용합니다.

**참고:**성공적으로 연결하려면 VPN 터널의 다른 쪽 끝에서 SA-Lifetime, Encryption Algorithm, Integrity Algorithm, PFS Key Group 및 IKE Policy가 동일해야 합니다.

RV110W에서 더 많은 기사를 보려면 [여기](#)를 클릭하십시오.