

CVR100W VPN路由器上的高級VPN設定

目標

虛擬專用網路(VPN)用於通過公共網路(例如Internet)將不同網路上的終端連線在一起。此功能允許遠離本地網路的遠端使用者通過Internet安全地連線到網路。

本文介紹如何在CVR100W VPN路由器上配置高級VPN。有關基本VPN設定，請參閱[CVR100W VPN路由器上的基本VPN設定](#)一文。

適用裝置

- CVR100W VPN路由器

軟體版本

- 1.0.1.19

高級VPN設定

初始設定

以下過程介紹了如何配置高級VPN設定的初始設定。

步驟1. 登入到Web配置實用程式並選擇VPN > Advanced VPN Setup。Advanced VPN Setup 頁面開啟：

Advanced VPN Setup

NAT Traversal: Enable
NETBIOS: Enable

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

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

Save Cancel

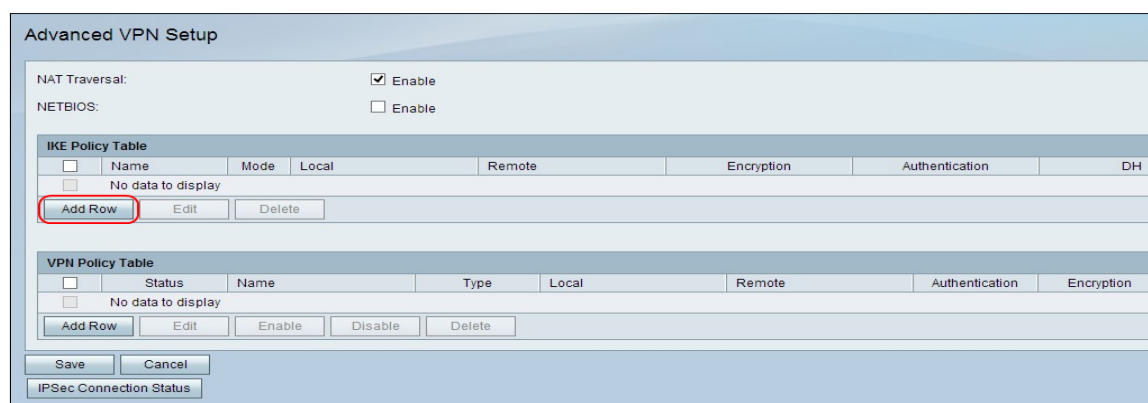
IPSec Connection Status

步驟2. (可選) 要為VPN連線啟用網路地址轉換(NAT)遍歷，請選中NAT遍歷欄位中的Enable 覈取方塊。NAT遍歷允許在使用NAT的網關之間建立VPN連線。如果VPN連線通過啟用了NAT的網關，請選擇此選項。

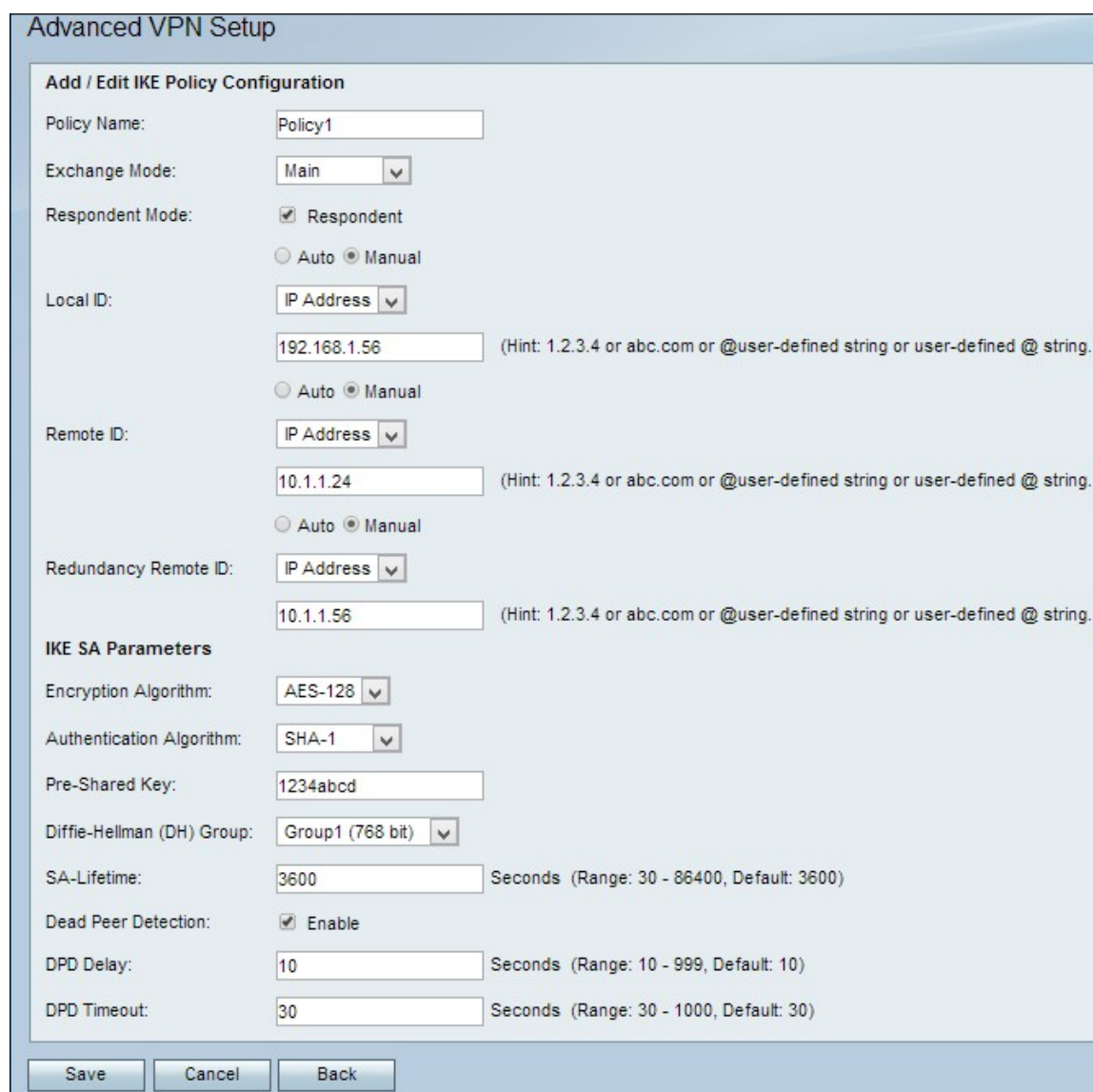
步驟3. (可選) 要啟用通過VPN連線傳送的網路基本輸入/輸出系統(NetBIOS)廣播，請選中NETBIOS欄位中的Enable 覈取方塊。NetBIOS使主機能夠在LAN中相互通訊。

IKE策略設定

Internet金鑰交換(IKE)是一種協定，用於為VPN中的通訊建立安全連線。此已建立的安全連線稱為安全關聯(SA)。以下過程介紹了如何為VPN連線配置IKE策略以用於安全性。要使VPN正常工作，兩個端點的IKE策略應相同。



步驟1.在IKE策略表中，按一下**Add Row**以建立新的IKE策略。「*Advanced VPN Setup*」頁將更改：



步驟2.在Policy Name欄位中，輸入IKE策略的名稱。

步驟3.從Exchange Mode下拉選單中，選擇用於標識IKE策略運行方式的選項。

·主要 — 此選項允許IKE策略更安全地運行。比主動模式慢。如果需要更安全的VPN連線

，請選擇此選項。

- 積極 — 此選項允許IKE策略更快地運行，但安全性不如主模式。如果需要更快的VPN連線，請選擇此選項。

步驟4. (可選) 要啟用響應方模式，請選中**響應方**竅取方塊。如果啟用了響應者模式，則CVR100W VPN路由器只能從遠端VPN終端接收VPN請求。

步驟5.在Local ID欄位中，按一下所需的單選按鈕以確定如何指定本地ID。

- 自動 — 此選項自動分配本地ID。
- 手動 — 此選項用於手動分配本地ID。

步驟6. (可選) 從Local ID下拉選單中，為本地網路選擇所需的標識方法。

- IP地址 — 此選項通過公共IP地址標識本地網路。
- FQDN — 此選項使用完全限定域名(FQDN)來標識本地網路。

步驟7. (可選) 在Local ID欄位中，輸入IP地址或域名。該條目取決於步驟6中選擇的選項。

步驟8.在Remote ID欄位中，按一下所需的單選按鈕以確定如何指定遠端ID。

- 自動 — 此選項自動分配遠端ID。
- 手動 — 此選項用於手動分配遠端ID

步驟9. (可選) 從Remote ID下拉選單中，為遠端網路選擇所需的標識方法。

- IP地址 — 此選項通過公共IP地址標識遠端網路。
- FQDN — 此選項使用完全限定域名(FQDN)來標識遠端網路。

步驟10. (可選) 在Remote ID欄位中，輸入IP地址或域名。該條目取決於步驟9中選擇的選項。

步驟11.在Redundancy Remote ID欄位中，按一下所需的單選按鈕以標識如何指定Redundancy Remote ID。冗餘遠端ID是用於設定遠端網關上的VPN隧道的備用遠端ID。

- 自動 — 此選項自動分配冗餘遠端ID。
- 手動 — 此選項用於手動分配冗餘遠端ID。

步驟12. (可選) 從Redundancy Remote ID下拉選單中，為冗餘網路選擇所需的標識方法。

- IP地址 — 此選項通過公共IP地址標識冗餘遠端網路。
- FQDN — 此選項使用完全限定域名(FQDN)來標識冗餘遠端網路。

步驟13. (可選) 在Redundancy Remote ID欄位中，輸入IP地址或域名。該條目取決於在步驟12中選擇的選項。

IKE SA Parameters	
Encryption Algorithm:	AES-128 ▼
Authentication Algorithm:	SHA-1 ▼
Pre-Shared Key:	1234abcd
Diffie-Hellman (DH) Group:	Group1 (768 bit) ▼
SA-Lifetime:	3600 Seconds (Range: 30 - 86400, Default: 3600)
Dead Peer Detection:	<input checked="" type="checkbox"/> Enable
DPD Delay:	10 Seconds (Range: 10 - 999, Default: 10)
DPD Timeout:	30 Seconds (Range: 30 - 1000, Default: 30)

步驟14.從Encryption Algorithm下拉選單中，選擇協商安全關聯(SA)的選項。

- DES — 資料加密標準(DES)使用56位金鑰大小進行資料加密。DES已過時，如果某個端點僅支援DES，則應使用。
- 3DES — 三重資料加密標準(3DES)執行DES三次，但金鑰大小從168位變為112位，從112位變為56位，具體取決於所執行的DES循環。3DES比DES和AES更安全。
- AES-128 — 具有128位金鑰的高級加密標準(AES-128)使用128位金鑰進行AES加密。AES比DES更快、更安全。某些型別的硬體使3DES更快。AES-128比AES-192和AES-256更快，但安全性較低。
- AES-192 — AES-192使用192位金鑰進行AES加密。AES-192比AES-128速度較慢但更安全，而AES-192比AES-256速度更快但安全性較低。
- AES-256 — AES-256使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步驟15.從Authentication Algorithm下拉選單中，選擇用於驗證VPN報頭的選項。

- MD5 — 消息摘要演算法5(MD5)使用128位雜湊值進行身份驗證。MD5的安全性較低，但比SHA-1和SHA2-256更快。
- SHA-1 — 安全雜湊演算法1(SHA-1)使用160位雜湊值進行身份驗證。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。
- SHA2-256 — 安全雜湊演算法2(SHA2-256)使用256位雜湊值進行身份驗證。SHA2-256比MD5和SHA-1速度慢但安全。

步驟16.在Pre-Shared Key欄位中，輸入IKE策略使用的預共用金鑰。

步驟17.從Diffie-hellman(DH)組下拉選單中，選擇IKE使用的DH組。DH組中的主機可以在彼此不知情的情況下交換金鑰。組位號越高，組越安全。

步驟18.在SA-Lifetime欄位中，輸入VPN的安全關聯(SA)在續訂SA之前持續的時間（以秒為單位）。

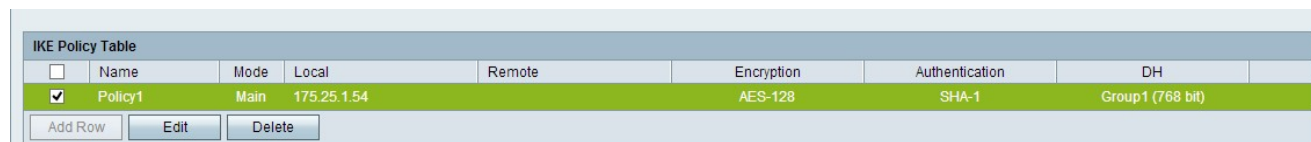
步驟19。（可選）要啟用失效對等體檢測(DPD)，請選中「失效對等體檢測」(Dead Peer Detection)欄位中的啟用覈取方塊。DPD用於監視IKE對等體，以檢查對等體是否停止工作。

DPD可防止非活動對等體上的網路資源浪費。

步驟20。(可選)要指示檢查對等體活動的頻率，請在「DPD延遲」欄位中輸入時間間隔(秒)。如果在步驟19中啟用了DPD，則此選項可用。

步驟21。(可選)要指示在刪除非活動對等體之前等待的時間，請在DPD Timeout欄位中輸入持續時間(以秒為單位)。如果在步驟19中啟用了DPD，則此選項可用。

步驟22.按一下「**Save**」。系統將重新顯示原始*Advanced VPN Setup*頁面。



<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input checked="" type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

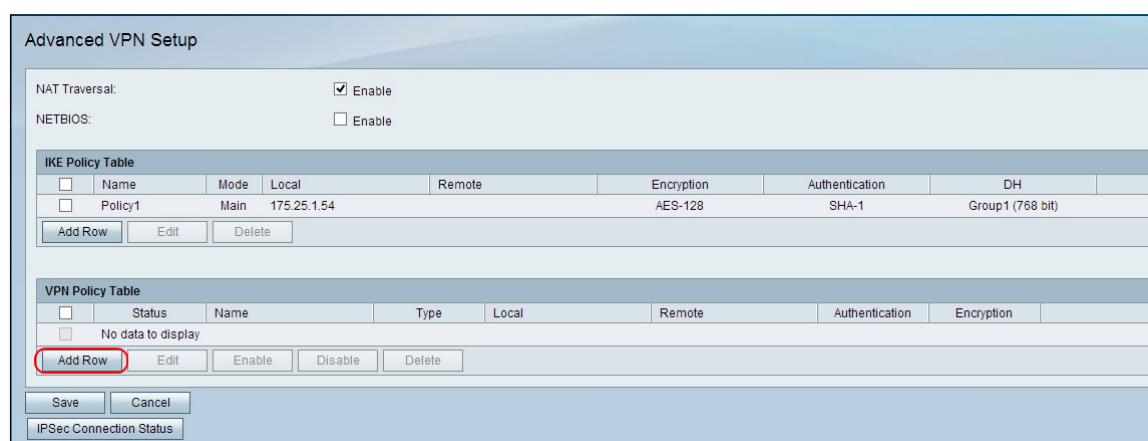
Add Row Edit Delete

步驟23。(可選)要在IKE策略表中編輯IKE策略，請選中該策略的覈取方塊。然後按一下**Edit**，編輯所需的欄位，然後按一下**Save**。

步驟24。(可選)要刪除IKE策略表中的IKE策略，請選中該策略的覈取方塊，然後點選**Delete**，然後點選**Save**。

VPN策略設定

以下過程說明如何配置VPN策略以供VPN連線使用。要使VPN正常工作，兩個端點的VPN策略應該相同。



Advanced VPN Setup

NAT Traversal: Enable
NETBIOS: Enable

<input type="checkbox"/>	Name	Mode	Local	Remote	Encryption	Authentication	DH
<input type="checkbox"/>	Policy1	Main	175.25.1.54		AES-128	SHA-1	Group1 (768 bit)

Add Row Edit Delete

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

Add Row Edit Enable Disable Delete

Save Cancel

IPSec Connection Status

步驟1.在VPN策略表中，按一下**Add Row**以建立新的VPN策略。「*Advanced VPN Setup*」頁將更改：

Advanced VPN Setup

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type:

Remote Endpoint:

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

(Hint: 1.2.3.4 or abc.com)

Rollback enable

Local Traffic Selection

Local IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Remote Traffic Selection

Remote IP:

IP Address: (Hint: 1.2.3.4)

Subnet Mask: (Hint: 255.255.255.0)

Manual Policy Parameters

SPI-Incoming:

SPI-Outgoing:

Encryption Algorithm:

Key-In:

Key-Out:

Integrity Algorithm:

Key-In:

Key-Out:

Auto Policy Parameters

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

Encryption Algorithm:

Integrity Algorithm:

PFS Key Group: Enable

Select IKE Policy:

Add / Edit VPN Policy Configuration

Policy Name:

Policy Type: ▼

Remote Endpoint: ▼

(Hint: 1.2.3.4 or abc.com)

Redundancy Endpoint: Enable

▼

(Hint: 1.2.3.4 or abc.com)

Rollback enable

步驟2.在Policy Name欄位中，輸入VPN策略的名稱。

步驟3.從Policy Type下拉選單中，選擇用於標識VPN隧道設定生成方式的選項。

- 手動策略 — 此選項可讓您配置用於資料加密和完整性的金鑰。
- 自動策略 — 此選項使用IKE策略進行資料完整性和加密金鑰交換。

步驟4.從「遠端端點」下拉選單中，選擇指定如何手動分配遠端ID的選項。

- IP地址 — 此選項通過公共IP地址標識遠端網路。
- FQDN — 此選項使用完全限定域名(FQDN)來標識遠端網路。

步驟5.在「遠端終端」下拉選單下方的文本輸入欄位中，輸入遠端地址的公共IP地址或域名。

步驟6. (可選) 要啟用冗餘，請選中「冗餘端點」欄位中的**啟用**覈取方塊。冗餘端點選項使CVR100W VPN路由器在主VPN連線失敗時連線到備份VPN端點。

步驟7. (可選) 要手動分配冗餘ID，請從「冗餘端點」下拉選單中選擇一個選項。

- IP地址 — 此選項通過公共IP地址標識冗餘遠端網路。
- FQDN — 此選項使用完全限定域名(FQDN)來標識冗餘遠端網路。

步驟8. (可選) 若要輸入冗餘地址，請在「冗餘端點」下拉選單下方的文本輸入欄位中輸入公共IP地址或域名。

步驟9. (可選) 要啟用回滾，請選中**Rollback enable**覈取方塊。當主VPN連線從故障中恢復時，此選項允許從備份VPN連線自動切換到主VPN連線。

Local Traffic Selection		
Local IP:	<input type="text" value="Subnet"/>	
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)
Remote Traffic Selection		
Remote IP:	<input type="text" value="Subnet"/>	
IP Address:	<input type="text" value="10.1.1.1"/>	(Hint: 1.2.3.4)
Subnet Mask:	<input type="text" value="255.0.0.0"/>	(Hint: 255.255.255.0)

步驟10.從Local IP下拉選單中選擇一個選項，以確定哪些主機受策略影響。

- 單一 — 此選項使用單個主機作為本地VPN連線點。
- 子網 — 此選項使用本地網路的子網作為本地VPN連線點。

步驟11.在「IP地址」欄位中，輸入本地子網或主機的主機或子網IP地址。

步驟12。（可選）如果在步驟10中選擇了Subnet選項，請在Subnet Mask欄位中輸入本地子網的子網掩碼。

步驟13.從Remote IP下拉選單中選擇一個選項，以確定哪些主機受策略影響。

- 單一 — 此選項使用單個主機作為遠端VPN連線點。
- 子網 — 此選項使用遠端網路的子網作為遠端VPN連線點。

步驟14.在「IP地址」欄位中，輸入遠端子網或主機的主機或子網IP地址。

步驟15。（可選）如果在步驟13中選擇了「子網」選項，請在「子網掩碼」欄位中輸入遠端子網的子網掩碼。

Manual Policy Parameters	
SPI-Incoming:	<input type="text" value="0xABCD"/>
SPI-Outgoing:	<input type="text" value="0x1234"/>
Encryption Algorithm:	<input type="text" value="AES-128"/>
Key-In:	<input type="text" value="12345678ABCDE"/>
Key-Out:	<input type="text" value="12345678ABCDE"/>
Integrity Algorithm:	<input type="text" value="SHA-1"/>
Key-In:	<input type="text" value="12345678ABCD"/>
Key-Out:	<input type="text" value="12345678ABCD"/>

附註：如果在步驟3中選擇了Manual Policy選項，請執行步驟16到步驟23;否則，請跳至[步驟](#)

24。

步驟16.在SPI-Incoming欄位中，為VPN連線上的傳入流量的安全引數索引(SPI)標籤輸入三到八個十六進位制字元。SPI標籤用於區分一個會話的流量和其他會話的流量。通道一端的傳入SPI應該是通道另一端的傳出SPI。

步驟17.在SPI-Outgoing欄位中，為VPN連線上傳出流量的SPI標籤輸入三到八個十六進位制字元。SPI標籤用於區分一個會話的流量和其他會話的流量。通道一端的傳出SPI應該是通道另一端的傳入SPI。

步驟18.從Encryption Algorithm下拉選單中，選擇協商安全關聯(SA)的選項。

- DES — 資料加密標準(DES)使用56位金鑰大小進行資料加密。DES已過時，如果某個端點僅支援DES，則應使用。
- 3DES — 三重資料加密標準(3DES)執行DES三次，但金鑰大小從168位變為112位，從112位變為56位，具體取決於所執行的DES循環。3DES比DES和AES更安全。
- AES-128 — 具有128位金鑰的高級加密標準(AES-128)使用128位金鑰進行AES加密。AES比DES更快、更安全。某些型別的硬體使得3DES更快。AES-128比AES-192和AES-256更快，但安全性較低。
- AES-192 — AES-192使用192位金鑰進行AES加密。AES-192比AES-128速度較慢但更安全，而AES-192比AES-256速度更快但安全性較低。
- AES-256 — AES-256使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步驟19.在Key-In欄位中，輸入入站策略的金鑰。金鑰長度取決於步驟18中選擇的演算法。

- DES使用8個字元的金鑰。
- 3DES使用24個字元的金鑰。
- AES-128使用12個字元的金鑰。
- AES-192使用24個字元的金鑰。
- AES-256使用32個字元的金鑰。

步驟20.在Key-Out欄位中，輸入傳出策略的金鑰。金鑰長度取決於步驟18中選擇的演算法。金鑰長度取決於步驟18中選擇的演算法。

- DES使用8個字元的金鑰。
- 3DES使用24個字元的金鑰。
- AES-128使用12個字元的金鑰。
- AES-192使用24個字元的金鑰。
- AES-256使用32個字元的金鑰。

步驟21.從Integrity Algorithm下拉選單中，選擇用於驗證VPN報頭的選項。

- MD5 — 消息摘要演算法5(MD5)使用128位雜湊值進行身份驗證。MD5的安全性較低，但比SHA-1和SHA2-256更快。

·SHA-1 — 安全雜湊演算法1(SHA-1)使用160位雜湊值進行身份驗證。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。

·SHA2-256 — 安全雜湊演算法2(SHA2-256)使用256位雜湊值進行身份驗證。SHA2-256比MD5和SHA-1速度更慢，但更安全。

步驟22.在Key-In欄位中，輸入入站策略的金鑰。金鑰長度取決於步驟21中選擇的演算法。

·MD5使用16個字元的金鑰。

·SHA-1使用20個字元的金鑰。

·SHA2-256使用32個字元的金鑰。

步驟23.在Key-Out欄位中，輸入傳出策略的金鑰。金鑰長度取決於步驟21中選擇的演算法。金鑰長度取決於步驟21中選擇的演算法。

·MD5使用16個字元的金鑰。

·SHA-1使用20個字元的金鑰。

·SHA2-256使用32個字元的金鑰。

Auto Policy Parameters

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

Encryption Algorithm: AES-128

Integrity Algorithm: SHA-1

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

Select IKE Policy: Policy1

View

附註：如果您在步驟3中選擇了「Auto Policy (自動策略)」，請執行步驟24到步驟29;否則，請跳至[步驟31](#)。

步驟24.在SA-Lifetime欄位中，輸入SA在續訂之前的持續時間 (以秒為單位)。

步驟25.從Encryption Algorithm下拉選單中，選擇協商安全關聯(SA)的選項。

·DES — 資料加密標準(DES)使用56位金鑰大小進行資料加密。DES已過時，如果某個端點僅支援DES，則應使用。

·3DES — 三重資料加密標準(3DES)執行DES三次，但金鑰大小從168位變為112位，從112位變為56位，具體取決於所執行的DES循環。3DES比DES和AES更安全。

·AES-128 — 具有128位金鑰的高級加密標準(AES-128)使用128位金鑰進行AES加密。AES比DES更快、更安全。某些型別的硬體使3DES更快。AES-128比AES-192和AES-256更快，但安全性較低。

·AES-192 — AES-192使用192位金鑰進行AES加密。AES-192比AES-128速度較慢但更安全，而AES-192比AES-256速度更快但安全性較低。

·AES-256 — AES-256使用256位金鑰進行AES加密。AES-256比AES-128和AES-192慢，但更安全。

步驟26.從Integrity Algorithm下拉選單中，選擇用於驗證VPN報頭的選項。

·MD5 — 消息摘要演算法5(MD5)使用128位雜湊值進行身份驗證。MD5的安全性較低，但比SHA-1和SHA2-256更快。

·SHA-1 — 安全雜湊演算法1(SHA-1)使用160位雜湊值進行身份驗證。SHA-1比MD5更慢但更安全，而SHA-1比SHA2-256更快但更安全。

·SHA2-256 — 安全雜湊演算法2(SHA2-256)使用256位雜湊值進行身份驗證。SHA2-256比MD5和SHA-1速度慢但安全。

步驟27.選中PFS Key Group欄位中的**Enable**覈取方塊以啟用完全向前保密(PFS)。PFS提高了VPN安全性，但降低了連線速度。

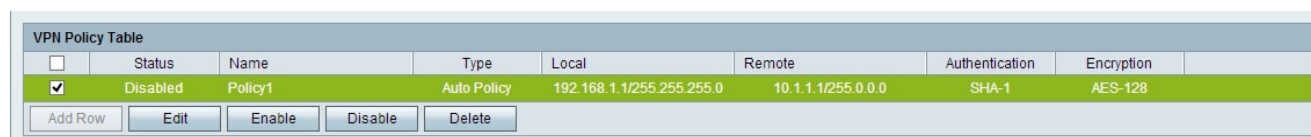
步驟28. (可選) 如果您選擇在步驟27中啟用PFS，請從PFS Key Group欄位下面的下拉選單中選擇要加入的Diffie-Hellman(DH)組。組編號越高，組越安全。

步驟29.從Select IKE Policy下拉選單中，選擇要用於VPN策略的IKE策略。

步驟30. (可選) 如果按一下**檢視**，則會將您引導到*Advanced VPN Setup*頁面的IKE配置部分。

步驟31.按一下「**Save**」。系統將重新顯示原始*Advanced VPN Setup*頁面。

步驟32.按一下「**Save**」。



<input type="checkbox"/>	Status	Name	Type	Local	Remote	Authentication	Encryption
<input checked="" type="checkbox"/>	Disabled	Policy1	Auto Policy	192.168.1.1/255.255.255.0	10.1.1.1/255.0.0.0	SHA-1	AES-128

Buttons: Add Row, Edit, Enable, Disable, Delete

步驟33. (可選) 要在VPN策略表中編輯VPN策略，請選中該策略的覈取方塊。然後按一下**Edit**，編輯所需的欄位，然後按一下**Save**。

步驟34. (可選) 要在VPN策略表中刪除VPN策略，請選中該策略的覈取方塊，按一下**Delete**，然後按一下**Save**。