

# RV260 و RV160 ىلج VPN دادعإ جلاع م نيوكت

يوضح هذا المستند كيفية تكوين معالج إعداد VPN على RV160 و RV260.

وقد تطورت التكنولوجيا، وغالبا ما يجري تسيير الأعمال خارج المكتب. الأجهزة أكثر قابلية للتنقل والموظفين غالبا ما يعملون من المنزل أو أثناء سفرهم. قد يتسبب ذلك في حدوث بعض الثغرات الأمنية. تعد الشبكة الخاصة الظاهرية (VPN) طريقة رائعة لربط العاملين عن بعد بشبكة آمنة. تسمح الشبكة الخاصة الظاهرية (VPN) للمضيف البعيد بالعمل كما لو كان متصلا بالشبكة الآمنة في الموقع.

تقوم الشبكة الخاصة الظاهرية (VPN) بتأسيس اتصال مشفر عبر شبكة أقل أمانا مثل الإنترنت. فهي تضمن مستوى مناسباً من الأمان للنظم المتصلة. يتم إنشاء نفق كشبكة خاصة يمكنها إرسال البيانات بشكل آمن باستخدام تقنيات التشفير والمصادقة المتوافقة مع معايير الصناعة لتأمين البيانات المرسلة. تعتمد شبكة VPN للوصول عن بعد عادة على أمان بروتوكول الإنترنت (IPsec) أو طبقة مأخذ التوصيل الآمنة (SSL) لتأمين الاتصال.

توفر شبكات VPN وصول الطبقة 2 إلى الشبكة الهدف؛ وتتطلب هذه الشبكات بروتوكول نفق مثل بروتوكول الاتصال النفقي من نقطة إلى نقطة (PPTP) أو بروتوكول الاتصال النفقي من الطبقة 2 (L2TP) الذي يعمل عبر اتصال IPsec الأساسي. تدعم الشبكة الخاصة الظاهرية (VPN) ل IPsec شبكة VPN من موقع إلى موقع لنفق من عبارة إلى عبارة. على سبيل المثال، يمكن للمستخدم تكوين نفق VPN في موقع فرعي للاتصال بالموجه في موقع الشركة، حتى يمكن للموقع الفرعي الوصول بشكل آمن إلى شبكة الشركة. كما تدعم الشبكة الخاصة الظاهرية (VPN) ل IPsec شبكة VPN من العميل إلى الخادم للنفق من المضيف إلى البوابة. تعد الشبكة الخاصة الظاهرية (VPN) من العميل إلى الخادم مفيدة عند الاتصال من الكمبيوتر المحمول/الكمبيوتر الشخصي من المنزل إلى شبكة شركة من خلال خادم الشبكة الخاصة الظاهرية (VPN).

يدعم الموجه من السلسلة 10 RV160 أنفاق، بينما يدعم الموجه من السلسلة 20 RV260 نفقا. يرشد معالج إعداد VPN المستخدم عند تكوين اتصال آمن لنفق IPsec من موقع إلى موقع. وهذا يعمل على تبسيط التكوين من خلال تجنب المعلمات المعقدة والاختيارية، وبهذا يمكن لأي مستخدم إعداد نفق IPsec بطريقة سريعة وفعالة.

• الطراز RV160

• الطراز RV260

• 1.0.0.13

**VPN**

الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب على الموجه المحلي لديك.

**ملاحظة:** سنحيل الموجه المحلي كالموجه A والموجه البعيد كموجه B. في هذا المستند، سنستخدم إثنين من RV160 لتوضيح معالج إعداد VPN.



# Router

cisco

●●●●●●●●

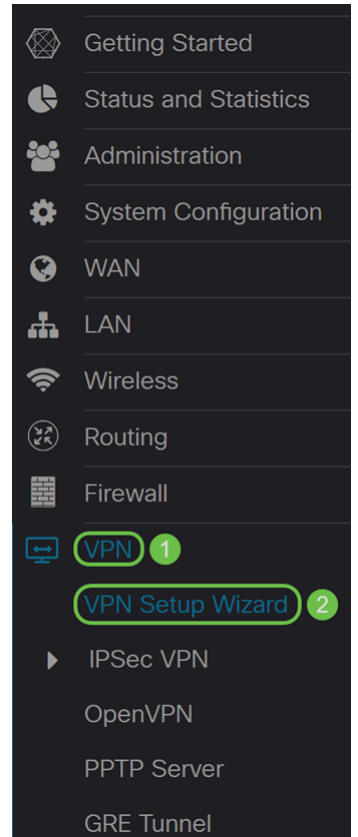
English

Login

©2018 Cisco Systems, Inc. All Rights Reserved.

Cisco, the Cisco Logo, and the Cisco Systems are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

الخطوة 2. انتقل إلى معالج إعداد VPN > VPN.



الخطوة 3. في قسم يحصل يبدأ ، أدخل اسم اتصال في الحقل أدخل اسم اتصال. لقد أدخلنا في HomeOffice كاسم اتصال لنا.

## VPN Setup Wizard (Site-to-Site)

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name:

### 4. Profile

Interface: WAN

### 5. Summary

Next

Cancel

الخطوة 4. في حقل الواجهة، حدد واجهة من القائمة المنسدلة إذا كنت تستخدم RV260. يحتوي RV160 على إرتباط WAN فقط لذلك لن تتمكن من تحديد واجهة من القائمة المنسدلة. انقر على التالي للمتابعة إلى قسم إعدادات الموجه البعيد.

## VPN Setup Wizard (Site-to-Site)

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name:

### 4. Profile

Interface: WAN

### 5. Summary

Next

Cancel

الخطوة 5. حدد نوع اتصال عن بعد من القائمة المنسدلة. حدد إما IP الثابت أو FQDN (اسم المجال المؤهل بالكامل) ثم أدخل إما عنوان IP الخاص بشبكة WAN أو FQDN الخاص بالبوابة التي ترغب في الاتصال بها

في حقل العنوان البعيد. في هذا المثال، تم تحديد IP ساكن إستاتيكي وتم إدخال عنوان IP للموجه البعيد WAN (الموجه B). ثم انقر فوق التالي للانتقال إلى المقطع التالي.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

Remote Connection Type :

Static IP

1

2. Remote Router Settings

Remote Address :

145.

2

3. Local and Remote Networks

4. Profile

5. Summary

3

Back

Next

Cancel

الخطوة 6. في قسم الشبكة المحلية والبعيدة، ضمن تحديد حركة المرور المحلية، حدد IP المحلي (الشبكة الفرعية، أو المفرد، أو أي) من القائمة المنسدلة. إذا قمت بتحديد الشبكة الفرعية، فأدخل عنوان IP للشبكة الفرعية وقناع الشبكة الفرعية. إذا قمت بتحديد أحادي، فأدخل عنوان IP. في حالة تحديد أي، انتقل إلى الخطوة التالية لتكوين تحديد حركة مرور البيانات عن بعد.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Local Traffic Selection:

Any

Remote Traffic Selection:

Subnet

IP Address:

Subnet Mask:

Back

Next

Cancel

الخطوة 7. في تحديد حركة المرور عن بعد، حدد IP عن بعد (الشبكة الفرعية أو أحادي أو أي) من القائمة المنسدلة. إذا قمت بتحديد الشبكة الفرعية، فأدخل عنوان IP الشبكة الفرعية وقناع الشبكة الفرعية للموجه البعيد (الموجه B). إذا قمت بتحديد أحادي، فأدخل عنوان IP. ثم انقر على التالي لتكوين قسم التوصيف.

**ملاحظة:** إذا كنت قد حددت أي لتحديد حركة المرور المحلية، فيجب عليك تحديد إما الشبكة الفرعية أو Single لتحديد حركة مرور البيانات عن بعد.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

**3. Local and Remote Networks**

4. Profile

5. Summary

Local Traffic Selection: Any

Remote Traffic Selection: Subnet 1

IP Address: 10.1.1.0 2

Subnet Mask: 255.255.255.0 3

4

Back Next Cancel

الخطوة 8. في قسم ملف التعريف، حدد اسم لملف تعريف IPsec من القائمة المنسدلة. لهذا العرض التوضيحي، تم تحديد ملف تعريف جديد كملف تعريف IPsec.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started	IPSec Profile:	<input type="text" value="new-profile"/>
✓ 2. Remote Router Settings	IKE Version:	<input type="text" value="new-profile"/>
✓ 3. Local and Remote Networks	Phase I Options	<input type="text" value="Default"/>
<b>4. Profile</b>	DH Group:	<input type="text" value="Group2 - 1024 bit"/>
5. Summary	Encryption:	<input type="text" value="3DES"/>
	Authentication:	<input type="text" value="MD5"/>
	SA Lifetime (sec.): ?	<input type="text" value="28800"/>
	Pre-shared Key:	<input type="text"/>
	Show Pre-shared Key:	<input type="checkbox"/> Enable
	Phase II Options	

Back

Next

Cancel

الخطوة 9. أختار 1 (Internet Key Exchange version 1 أو IKEv1) أو (Internet Key Exchange version 2 أو IKEv2) إصدار IKE الخاص بك. IKE هو بروتوكول هجين يقوم بتنفيذ تبادل مفاتيح Oakley وتبادل مفاتيح Skeme داخل إطار عمل رابطة أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP). يوفر IKE مصادقة أقران IPsec، وبتفاوض مفاتيح IPsec، وبتفاوض على اقتارات أمان IPsec. يعد IKEv2 أكثر فعالية لأنه يستغرق حزم أقل لإجراء تبادل المفاتيح وبدعم المزيد من خيارات المصادقة، بينما يقوم IKEv1 فقط بالمصادقة القائمة على المفاتيح المشتركة والشهادات. في هذا المثال، تم تحديد IKEv1 كإصدار IKE.

**ملاحظة:** إذا كان جهازك يدعم IKEv2، يوصى باستخدام IKEv2. إذا كانت أجهزتك لا تدعم IKEv2، فاستخدم IKEv1. يحتاج كلا الموجهين (المحلي والبعيد) إلى استخدام نفس إصدار IKE وإعدادات الأمان.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

الخطوة 10. في قسم خيارات المرحلة الأولى، حدد مجموعة Diffie-hellman (DH) (المجموعة 2 - 1024 بت أو المجموعة 5 - 1536 بت) من القائمة المنسدلة. DH هو بروتوكول تبادل مفاتيح، مع مجموعتين من أطوال المفاتيح الأساسية المختلفة: تحتوي المجموعة 2 على ما يصل إلى 1024 وحدة بت، والمجموعة 5 على ما يصل إلى 1536 وحدة بت. سوف نستخدم المجموعة 2 - 1024 بت لهذا العرض التوضيحي.

**ملاحظة:** للحصول على سرعة أكبر وأمان أقل، اختر المجموعة 2. من أجل سرعة أبطأ وأمان أعلى، اختر مجموعة 5. يتم تحديد المجموعة 2 بشكل افتراضي.



## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back Next Cancel

الخطوة 11. حدد خيار تشفير (3DES أو AES-128 أو AES-192 أو AES-256) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم حمولة الأمان (ESP)/اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) أو فك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن عبارة عن خوارزمية قديمة. وهذا يعني أنه يجب استخدامه فقط عندما لا يكون هناك بدائل أفضل لأنه يوفر مستوى أمنيا هامشيا ومقبولا في الوقت نفسه. يجب على المستخدمين استخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". معيار التشفير المتقدم (AES) هو خوارزمية تشفير تم تصميمها لتكون أكثر أمانا من DES. يستخدم معيار التشفير المتطور (AES) حجما أكبر للمفتاح مما يضمن أن النهج الوحيد المعروف لفك تشفير الرسالة هو أن يقوم الدخيل بتجريب كل مفتاح ممكن. يوصى باستخدام AES بدلا من 3DES. في هذا المثال، سنستخدم AES-192 كخيار تشفير خاص بنا.

**ملاحظة:** فيما يلي بعض الموارد الإضافية التي قد تساعد: [تكوين الأمان للشبكات الخاصة الظاهرية \(VPNs\) باستخدام IPSec وتشفير الجيل التالي.](#)

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): ? 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

الخطوة 12. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). يعتبر MD5 خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 128 بت. إن SHA1 عبارة عن خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 160 بت بينما ينتج SHA2-256 خلاصة 256 بت. يوصى بإجراء SHA2-256 لأنه أكثر أمانا. تأكد من أن كلا طرفي نفق VPN يستخدمان نفس طريقة المصادقة. حدد مصادقة (MD5 أو SHA1 أو SHA2-256). تم تحديد SHA2-256 لهذا المثال.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 28800

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

الخطوة 13. تخبرك مدة صلاحية (SA) مقدار الوقت، بالثواني، يكون IKE SA نشطا في هذه المرحلة. يتم التفاوض على افتراض أمان جديد (SA) قبل انتهاء صلاحية مدة البقاء لضمان أن وكيل خدمة (SA) جديد جاهز للاستخدام عند انتهاء صلاحية الملحق القديم. الافتراضي هو 28800 والنطاق هو من 120 إلى 86400. سنستخدم القيمة الافتراضية لـ 28800 ثانية كعمر SA الخاص بنا للمرحلة الأولى.

**ملاحظة:** يوصى بأن تكون مدة البقاء للمساعد الخاص بك في المرحلة الأولى أطول من فترة بقائك على قيد الحياة للمرحلة الثانية. إذا جعلت المرحلة الأولى أقصر من المرحلة الثانية، ثم سيكون عليك إعادة التفاوض النفق ذهابا وإيابا بشكل متكرر مقارنة بنفق البيانات. إن نفق البيانات هو ما يحتاج إلى مزيد من الأمان ومن الأفضل أن تكون مدة البقاء في المرحلة الثانية أقصر من المرحلة الأولى.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.):

Pre-shared Key:

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

الخطوة 14. أدخل المفتاح المشترك مسبقا لاستخدامه لمصادقة نظير IKE البعيد. يمكنك إدخال حتى 30 حرف من لوحة المفاتيح أو قيم سداسية عشرية، مثل My\_@123 أو 4d795f40313233. يجب أن يستخدم كلا طرفي نفق VPN نفس المفتاح المشترك مسبقا.

ملاحظة: نوصي بتغيير المفتاح المشترك مسبقا بشكل دوري لزيادة أمان VPN إلى الحد الأقصى.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile: new-profile

IKE Version:  IKEv1  IKEv2

Phase I Options

DH Group: Group2 - 1024 bit

Encryption: AES-192

Authentication: SHA2-256

SA Lifetime (sec.): 28800

Pre-shared Key: ●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Back

Next

Cancel

الخطوة 15. في قسم خيارات المرحلة الثانية، حدد بروتوكول من القائمة المنسدلة.

• ESP - حدد ESP لتشغيل البيانات وأدخل التشفير.

• آه - حدد هذا الخيار لسلامة البيانات في الحالات التي تكون فيها البيانات غير سرية ولكن يجب مصادقتها.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: ESP

Encryption: 3DES

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back Next Cancel

الخطوة 16. حدد خيار تشفير (3DES أو AES-128 أو AES-192 أو AES-256) من القائمة المنسدلة. تحدد هذه الطريقة الخوارزمية المستخدمة لتشفير حزم حمولة الأمان (ESP)/اقتران أمان الإنترنت وبروتوكول إدارة المفاتيح (ISAKMP) أو فك تشفيرها. يستخدم المعيار الثلاثي لتشفير البيانات (3DES) تشفير DES ثلاث مرات ولكنه الآن عبارة عن خوارزمية قديمة. وهذا يعني أنه يجب استخدامه فقط عندما لا يكون هناك بدائل أفضل لأنه يوفر مستوى أمنيا هامشيا ومقبولا في الوقت نفسه. يجب على المستخدمين استخدامها فقط إذا كانت مطلوبة للتوافق مع الإصدارات السابقة لأنها عرضة لبعض هجمات "التصادم الكلي". معيار التشفير المتقدم (AES) هو خوارزمية تشفير تم تصميمها لتكون أكثر أمانا من DES. يستخدم معيار التشفير المتطور (AES) حجما أكبر للمفتاح مما يضمن أن النهج الوحيد المعروف لفك تشفير الرسالة هو أن يقوم الدخيل بتجريب كل مفتاح ممكن. يوصى باستخدام AES بدلا من 3DES. في هذا المثال، سنستخدم AES-192 كخيار تشفير خاص بنا.

**ملاحظة:** فيما يلي بعض الموارد الإضافية التي قد تساعد: [تكوين الأمان للشبكات الخاصة الظاهرية \(VPNs\) باستخدام IPsec وتشفير الجيل التالي.](#)

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

SA Lifetime (sec.): 3600

Pre-shared Key: ●●●●●●●●

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: ESP

Encryption: AES-192

Authentication: MD5

SA Lifetime (sec.): 3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back Next Cancel

الخطوة 17. يحدد أسلوب المصادقة كيفية التحقق من صحة حزم رؤوس بروتوكول حمولة الأمان التضمين (ESP). يعتبر MD5 خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 128 بت. إن SHA1 عبارة عن خوارزمية تجزئة أحادية الإتجاه ينتج عنها ملخص 160 بت بينما ينتج SHA2-256 خلاصة 256 بت. يوصى بإجراء SHA2-256 لأنه أكثر أمانا. تأكد من أن كلا طرفي نفق VPN يستخدمان نفس طريقة المصادقة. حدد مصادقة (MD5 أو SHA1 أو SHA2-256). تم تحديد SHA2-256 لهذا المثال.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.):

20000

Pre-shared Key:

●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.):

3600

Perfect Forward Secrecy:  Enable

Save as a new profile

Back

Next

Cancel

الخطوة 18. أدخل في مدة بقاء SA (في الثانية) وهو مقدار الوقت، بالثواني، الذي يكون فيه نفق VPN نشطاً في هذه المرحلة. القيمة الافتراضية للمرحلة 2 هي 3600 ثانية.



## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

SA Lifetime (sec.):

28800

Pre-shared Key:

●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.):

3600

Perfect Forward Secrecy:

Enable

Save as a new profile

Back

Next

Cancel

الخطوة 19. عند تمكين سرية إعادة التوجيه المثالية (PFS)، تعمل مفاوضات المرحلة 2 من IKE على إنشاء مادة أساسية جديدة لتشفير حركة مرور IPsec والمصادقة. يتم استخدام سرية إعادة التوجيه المثالية لتحسين أمان الاتصالات المرسله عبر الإنترنت باستخدام تشفير المفتاح العام. حدد المربع لتمكين هذه الميزة، أو قم بإلغاء تحديد المربع لتعطيل هذه الميزة. يوصى بهذه الميزة. في حالة تحديده، حدد مجموعة DH. في هذا المثال يتم استخدام مجموعة 2 - 1024 بت.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

••••••••

Show Pre-shared Key:

Enable

### Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.):

3600

Perfect Forward Secrecy:

Enable

1

DH Group:

2

Group2 - 1024 bit

Save as a new profile

Back

Next

Cancel

الخطوة 20. في حفظ كملف تخصيص جديد، أدخل اسم لملف التخصيص الجديد الذي أنشأته للتو. طقطقت بعد ذلك أن يرى خلاصة من ك VPN تشكيل.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

4. Profile

5. Summary

Pre-shared Key:

••••••

Show Pre-shared Key:

Enable

### Phase II Options

Protocol Selection:

ESP

Encryption:

AES-192

Authentication:

SHA2-256

SA Lifetime (sec.): ?

3600

Perfect Forward Secrecy:  Enable

DH Group:

Group2 - 1024 bit

Save as a new profile <sup>1</sup>

HomeOffice

Back

<sup>2</sup> Next

Cancel

الخطوة 21. تحقق من المعلومات ثم انقر فوق إرسال.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started	(sec.):	-----	
✓ 2. Remote Router Settings	Pre-shared Key:	Test123	
✓ 3. Local and Remote Networks	Phase II Options		Remote Group
✓ 4. Profile	Protocol Selection:	ESP	Remote IP Type: Subnet
5. Summary	Encryption:	AES-192	IP Address: 10.1.1.0
	Authentication:	SHA2-256	Subnet: 255.255.255.0
	SA Lifetime (sec.):	3600	
	Perfect Forward Secrecy:	Enable	
	DH Group:	Group2 - 1024 bit	

Back

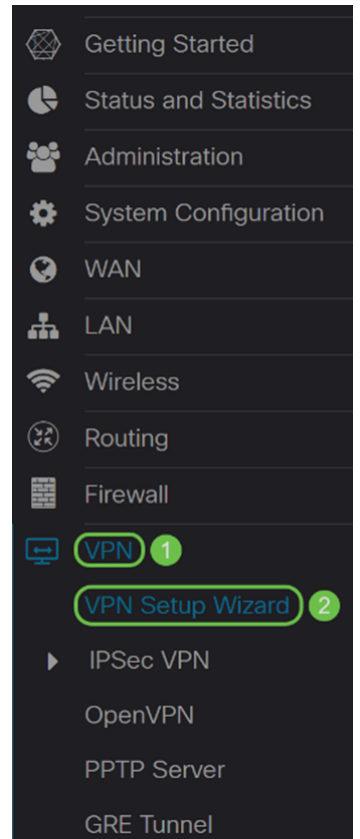
Submit

Cancel

VPN

على الموجه البعيد، ستحتاج إلى تكوين إعدادات الأمان نفسها الخاصة بالموجه المحلي لديك ولكن استخدم عنوان IP للموجه المحلي كحركة المرور عن بعد.

الخطوة 1. قم بتسجيل الدخول إلى صفحة تكوين الويب على الموجه عن بعد (Router B) وانتقل إلى معالج إعدادات VPN > VPN.



الخطوة 2. دخلت توصيل إسم واخترت القارن أن يكون استعملت ل ال VPN إن أنت تستعمل RV260. يحتوي RV160 على إرتباط WAN فقط لذلك لن تتمكن من تحديد واجهة من القائمة المنسدلة. ثم انقر فوق التالي للمتابعة.

## VPN Setup Wizard (Site-to-Site)

### 1. Getting Started

This Setup Wizard helps you to configure a secure connection between two routers that are physically separated over the IPsec VPN tunnel.

### 2. Remote Router Settings

Before you begin, you need to know the local network address and subnet mask, and the digital certificates for authentication between two peers if needed.

### 3. Local and Remote Networks

Enter a connection name:

### 4. Profile

Interface: WAN

### 5. Summary

2

Next

Cancel

الخطوة 3. في إعدادات الموجه البعيد، حدد نوع الاتصال عن بعد ثم أدخل عنوان IP لشبكة WAN للموجه A. ثم انقر فوق التالي للمتابعة إلى القسم التالي.

## VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

4. Profile

5. Summary

Remote Connection Type :

Static IP

1

Remote Address : ?

140.

2

3

Back

Next

Cancel

الخطوة 4. حدد حركة المرور المحلية والبعيدة. إذا كنت قد حددت الشبكة الفرعية في حقل تحديد حركة مرور البيانات عن بعد، فأدخل في الشبكة الفرعية لعنوان IP الخاص من الموجه A. ثم انقر على التالي لتكوين قسم التوصيف.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

**3. Local and Remote Networks**

4. Profile

5. Summary

Local Traffic Selection: Any 1

Remote Traffic Selection: Subnet 2

IP Address: 192.168.2.0 3

Subnet Mask: 255.255.255.0 4

5

Back Next Cancel

الخطوة 5. في قسم ملف التعريف، حدد نفس إعدادات التأمين الخاصة بالوجه A. لقد أدخلنا أيضا نفس المفتاح المشترك مسبقا مثل الوجه A. ثم انقر فوق التالي للانتقال إلى صفحة الملخص.

خيارات المرحلة الأولى:

# VPN Setup Wizard (Site-to-Site)

✓ 1. Getting Started

✓ 2. Remote Router Settings

✓ 3. Local and Remote Networks

**4. Profile**

5. Summary

IPSec Profile:

1 new-profile

IKE Version:

2  IKEv1  IKEv2

Phase I Options

DH Group:

3 Group2 - 1024 bit

Encryption:

4 AES-192

Authentication:

5 SHA2-256

SA Lifetime (sec.):

6 28800

Pre-shared Key:

7 ●●●●●●

Show Pre-shared Key:

Enable

Phase II Options

Back

Next

Cancel

خيارات المرحلة الثانية:



## VPN Setup Wizard (Site-to-Site)

1. Getting Started

2. Remote Router Settings

3. Local and Remote Networks

**4. Profile**

5. Summary

Pre-shared key:

Show Pre-shared Key:  Enable

Phase II Options

Protocol Selection: 1 ESP

Encryption: 2 AES-192

Authentication: 3 SHA2-256

SA Lifetime (sec.): ? 4 3600

Perfect Forward Secrecy:  Enable 5

DH Group: 6 Group2 - 1024 bit

Save as a new profile 7 RemoteOffice

8

Back Next Cancel

الخطوة 6. في صفحة الملخص، تحقق من صحة المعلومات التي قمت بتكوينها للتو. ثم انقر فوق إرسال لإنشاء شبكة VPN من موقع إلى موقع.

## VPN Setup Wizard (Site-to-Site)

1. Getting Started (sec.): -----

2. Remote Router Settings  
Pre-shared Key: Test123

3. Local and Remote Networks

4. Profile

5. Summary

Phase II Options

Remote Group

Protocol Selection: ESP  
Encryption: AES-192  
Authentication: SHA2-256  
SA Lifetime (sec.): 3600  
Perfect Forward Secrecy: Enable  
DH Group: Group2 - 1024 bit

Remote IP Type: Subnet  
IP Address: 192.168.2.0  
Subnet: 255.255.255.0

Back

Submit

Cancel

**ملاحظة:** توجد جميع التكوينات التي يستخدمها الموجه حاليا في ملف التكوين الجاري تشغيله والذي يكون متطابرا ولا يتم الاحتفاظ به بين عمليات إعادة التمهيدي. للحفاظ على التكوين بين عمليات إعادة التمهيدي، تأكد من نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل بعد إكمال جميع التغييرات التي قمت بها. للقيام بذلك، انقر فوق الزر حفظ الذي يظهر في أعلى الصفحة أو انتقل إلى إدارة < إدارة التكوين. بعد ذلك، تأكد من أن المصدر يشغل التكوين والوجهة هي تكوين بدء التشغيل. طقسطة يطبق.

يجب أن تكون قد انتهيت بنجاح من تكوين شبكة VPN من موقع إلى موقع باستخدام معالج إعداد VPN. اتبع الخطوات التالية للتحقق من توصيل شبكة VPN من موقع إلى موقع.

الخطوة 1. للتحقق من تأسيس الاتصال، يجب أن ترى حالة اتصال عند التنقل إلى VPN > VPN < موقع إلى موقع.

Site-to-Site

Apply Cancel

Number of Connections: 1 connected, 1 configured, maximum 10 supported.

Connection Name	Remote Endpoint	Interface	IPSec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
<input type="checkbox"/> RemoteOffice	140.	WAN	VPNTTest	0.0.0.0/0	192.168.2.0/24	Connected	

الخطوة 2. انتقل إلى الحالة والإحصاءات < حالة الشبكة الخاصة الظاهرية (VPN) وتأكد من تمكين نفق الموقع إلى الموقع وUP.

# VPN Status

## Site-to-Site Tunnel Status

1 Tunnel(s) Used    9 Tunnel(s) Available  
1 Tunnel(s) Enabled    1 Tunnel(s) Defined

### Connection Table



Column Display Selection

<input type="checkbox"/>	No.	Name	Enable	Status	Phase2 Enc/Auth/Grp	Local Group	Remote Group	Remote Gateway	Action
<input type="checkbox"/>	1	RemoteOffice	Enable	UP	aes192-sha256	0.0.0.0/0	192.168.2.0/24	140. [redacted]	

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن تسم ل ا ذه Cisco ت مچرت  
م ل ا ل اء ان ا ع مچ ي ف ن م دخت س م ل ل م عد و ت ح م م ي دقت ل ة ي ر ش ب ل و  
امك ة ق ي ق د ن و ك ت ن ل ة ي ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ال م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ال ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ى ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا هذه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
Systems (ر ف و ت م ط ب ا ر ل ا) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا دن ت س م ل ا