

نم VPN ةكبشل ةمدقتم لادادعإل انيوكت و RV160 لعل لشفلا زواجت و عقوم لادع قوم RV260

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين الإعدادات المتقدمة لشبكة VPN من موقع إلى موقع وتجاوز الأعطال على RV160 و RV260.

المقدمة

تعد الشبكة الخاصة الظاهرية (VPN) طريقة رائعة لربط العاملين عن بعد بشبكة آمنة. تسمح الشبكة الخاصة الظاهرية (VPN) للمضيف البعيد بالعمل كما لو كان متصلاً بالشبكة الآمنة في الموقع. في شبكة VPN من موقع إلى موقع، يتصل الموجه المحلي في موقع واحد بموجه بعيد من خلال نفق شبكة VPN. يقوم هذا النفق بتضمين البيانات بشكل آمن باستخدام تقنيات التشفير والمصادقة المتوافقة مع معايير الصناعة لتأمين البيانات المرسلة. يجب إجراء تكوين مطابق على كلا جانبي الاتصال لإنشاء اتصال شبكة VPN ناجح من موقع إلى موقع. توفر تهيئة الشبكة الخاصة الظاهرية (VPN) المتقدمة من موقع إلى موقع مرونة تكوين التكوينات الاختيارية لنفق الشبكة الخاصة الظاهرية (VPN).

بعد تجاوز الفشل ميزة قوية تضمن وجود اتصال دائم بين هذين الموقعين. ويكون ذلك مفيداً عندما يكون تجاوز الأخطاء مهماً. يحدث تجاوز الفشل عندما يكون الموجه الأساسي معطلاً. عند هذه النقطة، سيقوم الموجه الثانوي أو الموجه الاحتياطي بتولي الأمر وتوفير اتصال. وهذا من شأنه أن يساعد في منع نقطة واحدة من الفشل.

الأجهزة القابلة للتطبيق

RV160 .

RV260 .

إصدار البرامج

1.0.00.13•

المتطلبات الأساسية

قبل تكوين الإعدادات المتقدمة وتجاوز الفشل لشبكة VPN من موقع إلى موقع على RV160 و RV260، ستحتاج إلى تكوين ملف تعريف IPsec وشبكة VPN من موقع إلى موقع على الموجه المحلي والبعيد. فيما يلي قائمة بالمقالات التي يمكن أن تساعدك على تكوينها. لديك الخيار لاستخدام معالج إعدادات VPN الذي سيساعدك في تكوين كل من ملف تعريف IPsec وكذلك شبكة VPN من موقع إلى موقع أو يمكنك تكوينها بشكل منفصل ومتابعتها على طول المستندين الواردين أدناه.

1. [تكوين معالج إعدادات VPN على RV160 و RV260](#)

أو

1. [تكوين توصيفات IPsec \(وضع الكبلات التلقائية\) على RV160 و RV260](#) (إختياري)

تكوين الإعدادات المتقدمة لشبكة VPN من موقع إلى موقع

يجب تكوين الإعدادات المتقدمة بنفس الطريقة على كلا جانبي اتصال VPN.

الخطوة 1. قم بتسجيل الدخول إلى الأداة المساعدة لتكوين الويب.



Router

cisco

••••••••

English

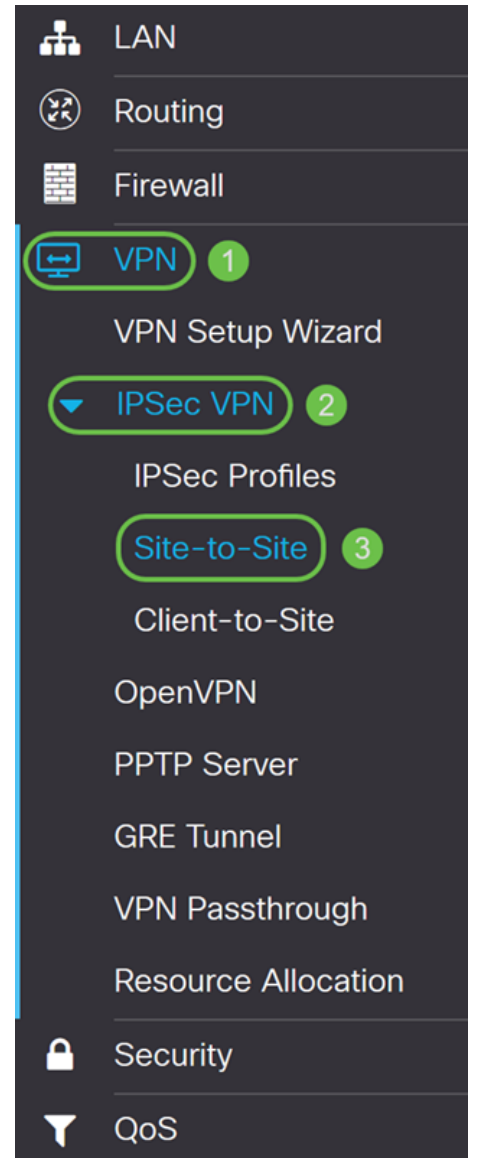


Login

©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 IPsec VPN < VPN > من موقع إلى موقع.



الخطوة 3. حدد خانة الاختيار الخاصة بالاتصال الذي تريد تحريره. ثم اضغط على أيقونة القلم والورق لتحرير الاتصال. في هذا المثال، يتم تحديد الاتصال المسمى HomeOffice.

Site-to-Site Apply Cancel

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

+ ✎ 🗑️

<input type="checkbox"/>	Connection Name	Remote Endpoint	Interface	IPsec Profiles	Local Traffic Selection	Remote Traffic Selection	Status	Actions
<input checked="" type="checkbox"/>	HomeOffice	140. [REDACTED]	WAN	VPNTTest	10.1.1.0/24	192.168.2.0/24	Connected	

الخطوة 4. انقر على علامة التبويب إعدادات متقدمة.

Add/Edit a New Connection

Apply

Cancel

Basic Settings

Advanced Settings

Failover

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

الخطوة 5. حدد خانة الاختيار **ضغط** (دعم بروتوكول ضغط حمولة IP (IPComp)) لتمكين الموجه من اقتراح الضغط عند بدء إتصاله. يقلل هذا البروتوكول من حجم مخططات بيانات IP. إذا رفض المستجيب هذا الاقتراح، فلن يقوم الموجه بتنفيذ الضغط. عندما يكون الموجه هو المستجيب، فإنه يقبل الضغط، حتى إذا لم يتم تمكين الضغط. إذا قمت بتمكين هذه الميزة لهذا الموجه، فستحتاج إلى تمكينها على الموجه البعيد (الطرف الآخر من النفق).

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

الخطوة 6. تستخدم رسائل البث لدقة الأسماء في شبكات Windows لتعريف الموارد مثل أجهزة الكمبيوتر والطابعات وخواص الملفات. يتم استخدام هذه الرسائل من قبل بعض تطبيقات البرامج وميزات Windows مثل حي الشبكة. لا تتم إعادة توجيه حركة مرور بث LAN عادة عبر نفق VPN. ومع ذلك، يمكنك تحديد هذا المربع للسماح بإعادة بث بث NetBIOS من أحد طرفي النفق إلى الطرف الآخر. حدد خانة الاختيار **بث NetBIOS** للتمكين.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

الخطوة 7. حدد خانة الاختيار الاحتفاظ بقيد الحياة لتمكين الموجه من محاولة إعادة إنشاء اتصال VPN في فواصل زمنية منتظمة. أدخل عدد الثواني لتعيين الفاصل الزمني للمراقبة قيد الحياة في حقل الفاصل الزمني للمراقبة قيد الحياة. المدى from 10-999 ثاني.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive **1**

2

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

الخطوة 8. تحقق من تمكين ميزة "اكتشاف النظير الميت (DPD)" لتمكين DPD. وهو يرسل رسائل HELLO/ACK دورية للتحقق من حالة نفق VPN. يجب تمكين خيار DPD على كلا طرفي نفق VPN. حدد الفاصل الزمني بين رسائل HELLO/ACK في حقل الفاصل الزمني بإدخال ما يلي:

• وقت التأخير - أدخل وقت التأخير بالثواني بين كل رسالة Hello. المدى from 10 - 300 ثاني والقيمة الافتراضية هي 10.

• مهلة الكشف - أدخل المهلة بالثواني للإعلان عن وفاة النظير. المدى from 30 - 1800 ثاني.

• إجراء DPD - الإجراء الذي يجب إتخاذ بعد مهلة DPD. حدد مسح أو إعادة التشغيل من القائمة المنسدلة.

Compress (Support IP Payload Compression Protocol (IPComp))

NetBIOS Broadcast

Keep-Alive

Keep-Alive Monitoring Interval: sec. (Range: 10 - 999, Default: 10)

DPD Enabled 1

Delay Time: 2 sec. (Range: 10 - 300)

Detection Timeout: 3 sec. (Range: 30 - 1800)

DPD Action: 4

Extended Authentication

User

User Name

الخطوة 9. تحقق من المصادقة الموسعة إذا أردت تمكين المصادقة الموسعة. وسيوفر ذلك مستوى إضافيا من المصادقة يتطلب من المستخدمين عن بعد المفتاح في بيانات الاعتماد الخاصة بهم قبل منحهم حق الوصول إلى شبكة VPN. للحصول على مصادقة موسعة للعمل، يجب أن يستخدم الموقع الرئيسي مصادقة المجموعة ويجب أن يستخدم الموقع البعيد مصادقة المستخدم. في الخطوات القليلة التالية، سنقوم بتكوين الموقع الرئيسي لاستخدام مصادقة المجموعة.

ملاحظة: يوصى بتكوين اتصال من عميل إلى موقع لمصادقة المستخدم بدلا من المصادقة الموسعة.

إذا لم تكن قد قمت بإنشاء مجموعة مستخدمين لموقعك الرئيسي، فانقر فوق الارتباط لمعرفة كيفية إنشاء مجموعة مستخدمين موجودة في هذه المقالة: [إنشاء مجموعة مستخدمين للمصادقة الموسعة](#).

إذا كنت تريد معرفة كيفية إنشاء حسابات مستخدمين، انقر فوق الارتباط لإعادة توجيهه إلى القسم: [إنشاء حساب مستخدم للمصادقة الموسعة](#).

Delay Time: sec. (Range: 10 - 300)

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:



Group Name

الخطوة 10. حدد مجموعة كمصادقة موسعة واضغط على أيقونة زائد لإضافة مجموعة جديدة. من القائمة المنسدلة، اختر المجموعة التي تريد استخدامها للمصادقة. تأكد من وجود المستخدمين الذين تريد في تلك المجموعة.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

1 Group: 2 3

Group Name

الخطوة 11. في الخطوات القليلة التالية، سنقوم بتكوين الموجه البعيد لاستخدام مصادقة المستخدم. في الموجه البعيد، حدد خانة الاختيار **مصادقة موسعة** لتمكين المصادقة الموسعة.

Detection Timeout: sec. (Range: 30 - 1800)

DPD Action:

Extended Authentication

User

User Name

Password

Show Password: Enable

Group:

Group Name

الخطوة 12. حدد **المستخدم** كمصادقة موسعة. أدخل اسم المستخدم وكلمة المرور للمستخدم في المجموعة التي تم تحديدها في الموجه الرئيسي. في هذا مثال، VPNUser و CiscoTest123! دخلت.

Extended Authentication

1 User

User Name

2 VPNUser

Password

3

Show Password:

Enable

Group:



Group Name

الخطوة 13. تحقق من تقسيم DNS للتمكين. يقوم هذا بتقسيم خادم نظام اسم المجال (DNS) وطلبات DNS الأخرى إلى خادم DNS آخر، استنادا إلى أسماء المجالات المحددة. عندما يستقبل الموجه طلب تحليل العنوان، فإنه يفحص اسم المجال. إذا طابقت اسم المجال اسم المجال في إعدادات DNS المقسمة، فإنه يقوم بتمرير الطلب إلى خادم DNS المحدد داخل شبكة خادم VPN. وإلا، يتم تمرير الطلب إلى خادم DNS المحدد في إعدادات واجهة WAN (أي خادم DNS لـ ISP).

يتم فصل DNS المقسم إلى منطقتين لنفس المجال. واحد لاستخدامه من قبل الشبكة الداخلية والآخر المستخدم من قبل الشبكة الخارجية. يوجه تقسيم DNS المضيفين الداخليين إلى DNS داخلي لدقة الاسم ويتم توجيه المضيفين الخارجيين إلى DNS خارجي لدقة الاسم.

إذا قمت بتمكين تقسيم DNS، فأدخل عنوان IP الخاص بخادم DNS لاستخدامه للمجالات المحددة. إختياريا، حدد خادم DNS ثانوي في حقل DNS Server 2. في اسم المجال 1-6، أدخل أسماء المجالات لخوادم DNS. يتم تمرير طلبات المجالات إلى خادم DNS المحدد.

Split DNS 1

DNS Server 1:

2 192.168.1.80

DNS Server 2:

(Optional)

Domain Name 1:

3 www.cisco.com

Domain Name 2:

(Optional)

Domain Name 3:

(Optional)

Domain Name 4:

(Optional)

Domain Name 5:

(Optional)

Domain Name 6:

(Optional)

الخطوة 14. طقطقة يطبق.

Add/Edit a New Connection

Apply

Cancel

Group Name

Split DNS

DNS Server 1:

DNS Server 2: (Optional)

Domain Name 1:

Domain Name 2: (Optional)

Domain Name 3: (Optional)

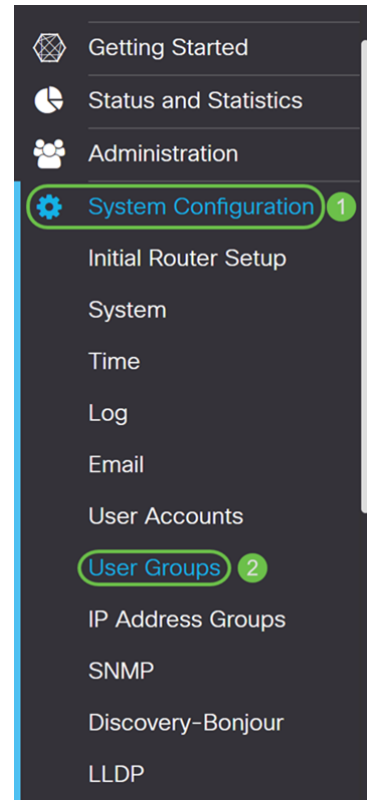
Domain Name 4: (Optional)

Domain Name 5: (Optional)

Domain Name 6: (Optional)

إنشاء مجموعة مستخدمين للمصادقة الموسعة

الخطوة 1. انتقل إلى تكوين النظام < مجموعات المستخدمين.



الخطوة 2. انقر فوق أيقونة زائد لإضافة مجموعة مستخدمين جديدة.

User Groups

Apply

Cancel



<input type="checkbox"/>	Group	Web Login /NETCONF /RESTCONF	802.1x	S2S IPSec VPN	C2S IPSec VPN	OpenVPN	PPTP
<input type="checkbox"/>	admin	Admin	Enable	Enable	Enable	Enable	Enable
<input type="checkbox"/>	guest	Disable	Disable	Disable	Disable	Disable	Disable

الخطوة 3. أدخل اسما في حقل اسم المجموعة ثم اضغط على تطبيق. في هذا المثال، تم إدخال SiteGroupTest كاسم للمجموعة.

User Groups

2

Apply

Cancel

Group Name:

1

Local User Membership List



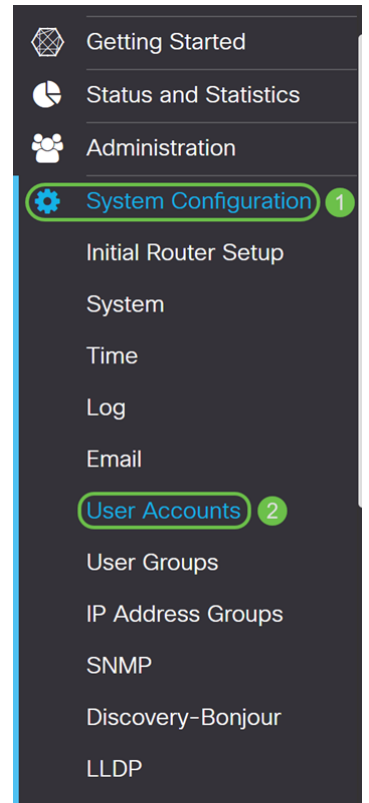
User

* Should have at least one account in the 'admin' group.

تكوين حسابات المستخدمين للمصادقة الموسعة






ملاحظة هامة: الرجاء ترك حساب المسؤول الافتراضي في مجموعة الإدارة وإنشاء حساب مستخدم جديد ومجموعة مستخدمي ل Show Soft. إذا قمت بنقل حساب المسؤول الخاص بك إلى مجموعة مختلفة، فستمنع نفسك من تسجيل الدخول إلى الموجه.

الخطوة 1. انتقل إلى تكوين النظام < حسابات المستخدمين.



الخطوة 2. قم بالتمرير لأسفل إلى المستخدمين المحليين. انقر فوق رمز الإضافة لإضافة مستخدم محلي جديد.

Local Users ^


    

<input type="checkbox"/> Username	Group
<input type="checkbox"/> cisco	admin
<input type="checkbox"/> guest	guest

* Should have at least one account in the 'admin' group.

الخطوة 3. يتم فتح صفحة إضافة حساب مستخدم. أدخل اسم مستخدم في حقل اسم المستخدم. في هذا المثال، تم إدخال VPNuser كاسم مستخدم.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter:

Group:


Apply

Cancel

الخطوة 4. أدخل كلمة مرور في حقل كلمة المرور الجديدة وتأكد كلمة المرور. في هذا المثال، تم إدخال CiscoTest123.

ملاحظة: تم استخدام كلمة المرور هذه كمثال، ومع ذلك يوصى باستخدام كلمة مرور أكثر تعقيدا.

Add user account

 The current minimum requirements are as follows

* Minimal Password Length: 8

* Minimal Number of Character Classes: 3

Username:

New Password:

1

Confirm Password:

2

Password Strength meter:




Group:

Apply

Cancel

الخطوة 5. حدد مجموعة ثم اضغط على تطبيق لإنشاء حساب المستخدم الجديد. في هذا المثال، تم تحديد SiteGroupTest كمجموعة.

Add user account

 The current minimum requirements are as follows

- * Minimal Password Length: 8
- * Minimal Number of Character Classes: 3

Username:

New Password:

Confirm Password:

Password Strength meter:

Group: 1

2

Apply

Cancel

تهيئة تجاوز الفشل

لتمكين التغلب على الأعطال من موقع إلى موقع، يجب تمكين "المحافظة على الحياة" في علامة التبويب إعدادات متقدمة.

الخطوة 1. انقر فوق علامة التبويب تجاوز الفشل لتكوين تجاوز الفشل.

Add/Edit a New Connection

Basic Settings Advanced Settings Failover

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

الخطوة 2. تحقق من النسخ الاحتياطي للنفق للتمكين. عندما يكون النفق الرئيسي معطلا، تعمل هذه الميزة على تمكين الموجه من إعادة إنشاء نفق VPN باستخدام عنوان IP بديل للنظير البعيد أو شبكة WAN محلية بديلة. تكون هذه الميزة متاحة فقط في حالة تمكين DPD.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

الخطوة 3. في حقل عنوان IP للنسخ الاحتياطي البعيد، أدخل عنوان IP للنظير البعيد، أو أعد إدخال عنوان IP لشبكة WAN الذي تم تعيينه بالفعل للعبارة البعيدة. ثم حدد الواجهة المحلية (WAN1 أو WAN2 أو USB1 أو USB2) من القائمة المنسدلة.

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address) **1**

Local Interface: **2**

الخطوة 4. طقطقة يطبق.

Add/Edit a New Connection Apply Cancel

Basic Settings Advanced Settings **Failover**

Tunnel Backup

Remote Backup IP Address: (Name or IPv4 Address)

Local Interface:

القرار

يجب أن تكون قد انتهت الآن من تكوين الإعدادات المتقدمة وتجاوز الفشل بنجاح للشبكة الخاصة الظاهرية (VPN) من موقع إلى موقع على شبكتي RV160 و RV260. يجب أن تظل شبكة VPN الخاصة بك من موقع إلى موقع متصلة.

[عرض فيديو متعلق بهذه المقالة...](#)

[انقر هنا لعرض المحادثات التقنية الأخرى من Cisco](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقदन ةتيلوئسم Cisco
Systems (رفوتم طبارل) يلصلأل يزىلچنل دن تسمل