

# نم هجوم يلع AntiVirus جم انرب نيوكت RV34x ةلسلسلا

## الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين برنامج AntiVirus على موجهات سلسلة RV34x.

## المقدمة

يحمي برنامج الحماية من الفيروسات مستخدمي الشبكة من حالات العدوى ومحتوى البرامج الضارة الذي يتم إستلامه في رسائل البريد الإلكتروني أو البيانات. تدعم ميزة مكافحة الفيروسات بروتوكولات بروتوكول نقل البريد البسيط (SMTP) وبروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل الملفات (FTP) وبروتوكول مكتب البريد الإصدار 3 (POP3) وبروتوكول الوصول إلى رسائل الإنترنت (IMAP).

يستخدم محرك الحماية من الفيروسات مكونين مهمين، هما مصنف يعرف أين يبحث، وقاعدة بيانات الفيروسات التي تعرف ما تبحث عنه. يقوم المحرك بتصنيف الملف حسب النوع بدلا من الاعتماد على الملحق. يقوم محرك الفيروسات بالبحث عن الفيروسات الموجودة في أجسام الرسائل التي تم تلقيها بواسطة النظام وملحقاتها، ويساعد نوع ملف المرفق في تحديد مسحتها ضوئيا.

لمعرفة ما هي البرامج الضارة، راجع هذا الارتباط: [ما هي البرامج الضارة؟](#).

لمعرفة كيفية تكوين Umbrella، انقر فوق الارتباط: [Cisco Umbrella RV34x تكوين](#).

**ملاحظة هامة:** إذا كان الموجه يخضع حاليا لحمل عمل كبير، فقد يؤدي ذلك إلى تفاقم المشكلة.

ويتضمن الجدول أدناه إحصاءات متوقعة للأداء في إطار عمليات تهيئة مختلفة. وينبغي إستخدام هذه القيم كدليل، لأن الأداء العالمي الحقيقي قد يختلف بسبب عدد من العوامل.

الاتصالات المتزامنة	معدل الاتصال	سعة معالجة HTTP	سعة معالجة FTP	
الإعدادات الافتراضية	3000	982 ميجابايت/ثانية	981 ميجابايت/ثانية	
تمكين التحكم في التطبيق	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية	
تمكين مكافحة الفيروسات	1500	982 ميجابايت/ثانية	981 ميجابايت/ثانية	
تمكين IPS	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية	
تمكين مكافحة الفيروسات و IPS للتحكم في التطبيقات	1000	982 ميجابايت/ثانية	981 ميجابايت/ثانية	

يتم تعريف الحقول التالية على أنها:

**الاتصالات المتزامنة** - إجمالي عدد الاتصالات المتزامنة، على سبيل المثال، إذا كنت تقوم بتنزيل ملف من موقع واحد، فهذا اتصال واحد، يتم الآن دفع الصوت من Spotify ويكون اتصالاً آخر، مما يجعله إتصالين متزامنين.

**معدل الاتصال** - عدد طلبات الاتصال في الثانية التي يمكن لهذا الاتصال معالجتها.

**سعة معالجة HTTP/FTP** - تعد سعة معالجة HTTP و FTP معدلات التنزيل بالميجابايت/الثانية.

تم تحديث تراخيص الأمان لتضمين برنامج الحماية من الفيروسات بالإضافة إلى التطبيق الحالي وتصفية الويب. يلزم وجود حساب ذكي للحصول على ترخيص أمان. إذا لم يكن لديك بالفعل حساب ذكي نشط، فسيُلزم القسم 1 من هذا المستند.

لمعرفة كيفية تكوين نظام منع التسلسل على RV34x، انقر [هنا](#).

## الأجهزة القابلة للتطبيق

• الطراز RV34x

## إصدار البرامج

1.0.03.5•

## جدول المحتويات

1. [بنية الترخيص](#)
2. [تكوين برنامج مكافحة الفيروسات](#)
3. [حالة التهديدات/IPS](#)
4. [تحديث تعريفات مكافحة الفيروسات](#)
5. [القرار](#)

## بنية الترخيص - إصدارات البرنامج الثابت 1.0.3.15 والإصدارات الأحدث

عند الانتقال إلى الأمام، سيتحمل AnyConnect رسوماً لتراخيص العملاء فقط.

للحصول على معلومات إضافية حول ترخيص AnyConnect على موجهات سلسلة RV340، يرجى الاطلاع على المقالة المتعلقة [بترخيص AnyConnect لموجهات سلسلة RV340](#).

## تكوين برنامج مكافحة الفيروسات

الخطوة 1. إذا لم تكن قد قمت بتسجيل الدخول إلى الموجه، فسجل الدخول إلى صفحة تكوين الويب.



## Router

Username

Password

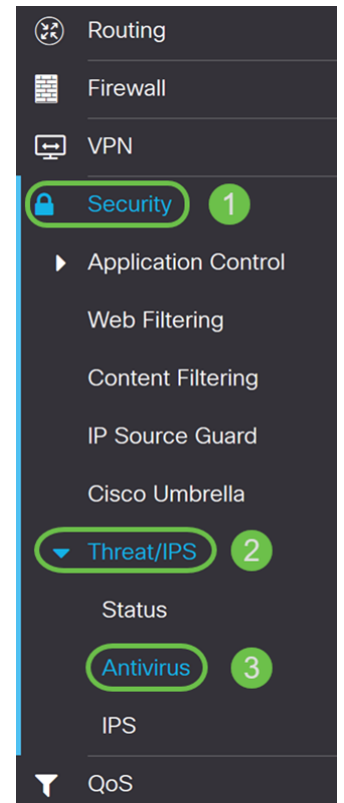
English

Login

©2017-2019 Cisco Systems, Inc. All rights reserved.

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

الخطوة 2. انتقل إلى الأمان < التهديد/IPS < مكافحة الفيروسات.



الخطوة 3. انقر فوق الزر تشغيل الراديو لتمكين ميزة مكافحة الفيروسات.

## Antivirus

Enable

On  Off

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input type="checkbox"/>	None
	FTP:	<input type="checkbox"/>	None
	SMTP Email Attachments:	<input type="checkbox"/>	None
	POP3 Email Attachments:	<input type="checkbox"/>	None
	IMAP Email Attachments:	<input type="checkbox"/>	None
	<input type="checkbox"/> Enable File Size Threshold		
	AV scan when file size is less than	<input type="text" value="1"/>	MB (Range: 1-100)

الخطوة 4. حدد خانة (خانات) **تمكين** لتمكين التطبيقات من المسح الضوئي على البروتوكولات. في هذا المثال، قمنا بتمكين جميع البروتوكولات (HTTP و FTP و SMTP و POP3 و IMAP). ثم حدد الإجراء المناسب له. يتم تعريف الخيارات التالية على أنها:

• **السجل** - حدد هذا الخيار لإنشاء السجل فقط (باستخدام معلومات العميل ومعرف التوقيع، وما إلى ذلك) عند تعريف التهديدات. لا يؤثر على الاتصال.

• **تدمير السجل** - حدد هذا الخيار لإسقاط الاتصال عند تحديد التهديدات وتسجيل الرسالة للحذف.

**ملاحظة:** في حالة وجود تهديد محدد في مرفق، سيتم اقتطاع الملف أثناء عملية التنزيل.

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input checked="" type="checkbox"/>	Log Destroy
	FTP:	<input checked="" type="checkbox"/>	Log
	SMTP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	POP3 Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	IMAP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy

الخطوة 5. إذا كنت تريد أن يحتوي برنامج الحماية من الفيروسات على حجم ملف مطلوب للمسح الضوئي، فتتحقق من **عتبة تمكين حجم الملف**. ثم قم بإدخال حجم الملف الذي يمكن أن يقوم برنامج مكافحة الفيروسات بمسحه. المدى 1-100 ميغابايت.

في هذا المثال، تم إدخال 50 ميغابايت.



Enable File Size Threshold

1

AV scan when file size is less than 50 MB (Range: 1-100)

2

الخطوة 6. في قسم قاعدة بيانات الفيروسات، يظهر التحديث الأخير تاريخ ووقت آخر توقيع تم تحديثه. يعرض إصدار الملف إصدار التوقيع الذي يتم استخدامه.

## Virus Database

Last Update: 2019-Mar-06, 18:44:31 GMT

File Version: 2.5.0.1003

الخطوة 7. انقر فوق الزر تطبيق لحفظ التغييرات.

## Antivirus

Apply

Cancel

Enable  On  Off

Applications To Scan:	Protocol	Enable	Action
	HTTP:	<input checked="" type="checkbox"/>	Log Destroy
	FTP:	<input checked="" type="checkbox"/>	Log
	SMTP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	POP3 Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	IMAP Email Attachments:	<input checked="" type="checkbox"/>	Log Destroy
	<input checked="" type="checkbox"/> Enable File Size Threshold		
	AV scan when file size is less than	50	MB (Range: 1-100)

يؤدي الضغط على تطبيق فقط إلى حفظ التكوين الخاص بك في التكوين الجاري تشغيله. ستحتاج إلى نسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل إذا كنت ترغب في الاحتفاظ بالتكوين الخاص بك بين عمليات إعادة التشغيل.

الخطوة 8. انقر أيقونة القرص المرن (حفظ) في أعلى الصفحة. وهذا سيقوم بإعادة توجيهك إلى إدارة التكوين لنسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.



cisco (admin)

English



الخطوة 9. في إدارة التكوين، قم بالتمرير إلى قسم نسخ/حفظ التكوين. تأكد من أن المصدر يشغل التكوين والوجهة هي بدء التشغيل. طقطقة يطبق. سيؤدي هذا إلى نسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل للاحتفاظ بالتكوين بين عمليات إعادة التمهيد.

## Configuration Management

3

Apply

Cancel

Disable Save Icon Blinking

### CONFIGURATION FILE NAME

Last Change Time

Running Configuration: ⓘ 2019-Feb-28, 17:20:54 GMT

Startup Configuration: ⓘ 2019-Feb-25, 20:28:52 GMT

Mirror Configuration: ⓘ 2019-Feb-24, 00:00:04 GMT

Backup Configuration: ⓘ N/A

### Copy/Save Configuration

All configurations that the router is currently using are in the Running Configuration file which is volatile and is not retained between reboots. To retain the configuration between reboots, make sure you copy the running configuration file to the startup configuration file after you have completed all your changes.

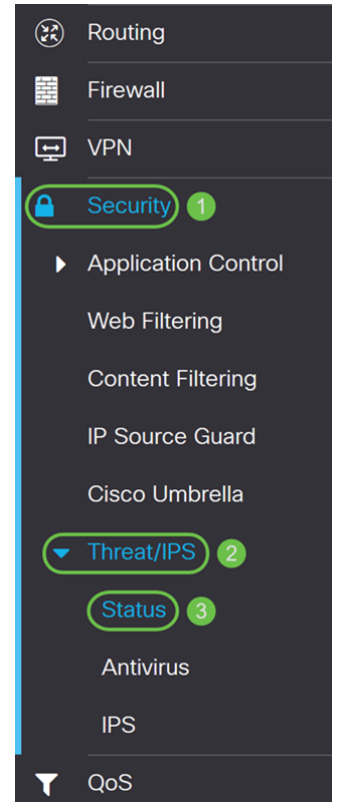
Source: ① Running Configuration

Destination: ② Startup Configuration

Save Icon Blinking: Enable

## حالة التهديد/IPS

الخطوة 1. انتقل إلى الأمان < التهديد/IPS < الحالة.



الخطوة 2. في صفحة الحالة، يمكنك رؤية تاريخ ووقت النظام، والتهديدات التي تم مسحها ضوئياً أو كشفها، والهجمات من علامة التبويب المحددة. بشكل افتراضي، يمكنك أن ترى حالة علامة التبويب "إجمالي".

## Status

System Date & Time: 2019-Mar-06, 22:44:55 GMT

Total Last 30 Days: Scanned 0 Detected 0

Total Last 7 Days: Scanned 0 Detected 0

Total Last 24 Hours: Scanned 0 Detected 0

Virus/IPS status since: 2019-Mar-06, 18:41:53 GMT [↻](#)

Total

Virus

IPS

Last 24 Hours

Events over time



الخطوة 3. في القائمة المنسدلة تحت علامة التبويب إجمالي ، يمكنك تحديد آخر 24 ساعة أو أسبوع أو شهر لعرض الأحداث.

## Status

System Date & Time: 2019-Mar-06, 22:44:55 GMT

Total Last 30 Days: Scanned 0 Detected 0

Total Last 7 Days: Scanned 0 Detected 0

Total Last 24 Hours: Scanned 0 Detected 0

Virus/IPS status since: 2019-Mar-06, 18:41:53 GMT [↻](#)

Total

Virus

IPS

Last 24 Hours

Events over time



الخطوة 4. انقر فوق علامة التبويب فيروس. في علامة التبويب فيروس، سيعرض ما يلي:

• أفضل 10 عملاء متأثرين - قائمة عناوين MAC المتضررين.

• أكثر 10 فيروسات تم اكتشافها - قائمة التهديدات التي تم الكشف عنها.

ملاحظة: يمكنك تمرير الماوس عبر المخطط الدائري للحصول على مزيد من التفاصيل.

## Status

System Date & Time: 2019-Mar-06, 22:35:48 GMT  
Total Since Activated: Scanned 0 Detected 0  
Total Last 7 Days: Scanned 0 Detected 0  
Total Last 24 Hours: Scanned 0 Detected 0  
Virus/IPS status since: 2019-Mar-06, 18:41:53 GMT [↻](#)

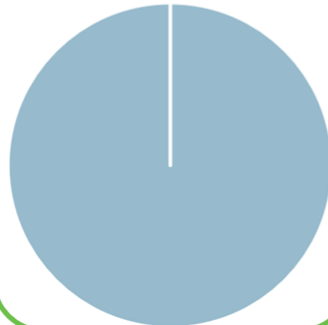
Total

Virus

IPS

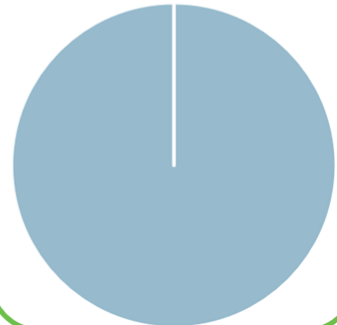
1

Top 10 Clients Affected



2

Top 10 Viruses Detected



3

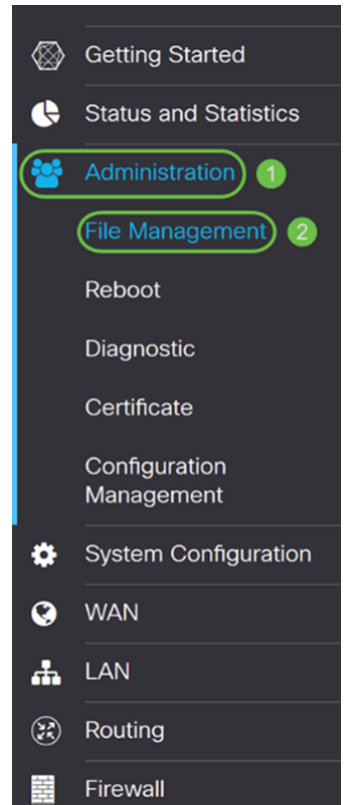
## تحديث تعريفات مكافحة الفيروسات

يمكنك تحديث قاعدة بيانات الحماية من الفيروسات يدويا أو تلقائيا. تظهر لك الخطوات من 1 إلى 2 كيفية تحديث قاعدة بيانات الحماية من الفيروسات يدويا بينما تظهر لك الخطوات من 3 إلى 6 كيفية تحديث قاعدة بيانات الحماية من الفيروسات تلقائيا.

**أفضل ممارسة:** يوصى بتحديث توقيعات الأمان تلقائيا على أساس أسبوعي.

الخطوة 1. لتحديث قاعدة بيانات مكافحة الفيروسات يدويا، انتقل إلى إدارة < إدارة الملفات.





الخطوة 2. قم بالتمرير لأسفل إلى قسم الترقية اليدوية في صفحة إدارة الملفات. اختر ملف توقيع ل نوع الملف و Cisco.com ل الترقية من. ثم اضغط على ترقية. سيقوم هذا بتنزيل أحدث توقيع أمان وتثبيته.

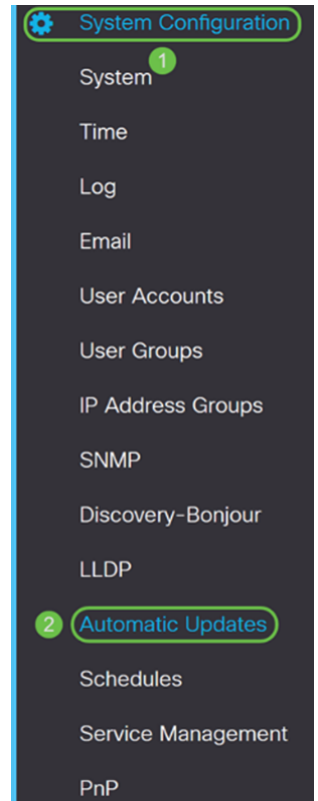
## Manual Upgrade

File Type:  Firmware Image  Signature File  USB Dongle Driver  Language File

Upgrade From:  cisco.com  PC  USB

Upgrade The device will be automatically rebooted after the upgrade is complete.

الخطوة 3. لتحديث قاعدة بيانات مكافحة الفيروسات تلقائياً، انتقل إلى تكوين النظام < تحديثات تلقائية.



الخطوة 4. يتم فتح صفحة التحديثات التلقائية. لديك خيار التحقق من وجود تحديثات إما بشكل أسبوعي أو شهري. يمكنك أن تقوم بإخطار الموجه عبر البريد الإلكتروني أو واجهة مستخدم ويب. في هذا المثال، سنختار التحقق كل أسبوع.

ملاحظة: يوصى بتحديث توقيعات التأمين تلقائياً على أساس أسبوعي.

Check Every:

Notify via:  Admin GUI

Email to  Notifications will not be sent unless an email server is configured.  
Click [here](#) to manage email server settings.

الخطوة 5. قم بالتمرير إلى قسم التحديث التلقائي وابحث عن حقل توقيع الأمان. في القائمة المنسدلة تحديث توقيع الأمان، حدد الوقت الذي تريد تحديثه تلقائياً. في هذا المثال، سنختار فوراً.

Automatic Update ^

	Notify ⇅	Update (hh:mm) ⇅	Status ⇅
System Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	<input checked="" type="checkbox"/>	<input type="text" value="Immediately"/>	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

الخطوة 6. انقر فوق تطبيق لحفظ التغييرات في ملف التكوين الجاري تشغيله.

ملاحظة: تذكر النقر فوق رمز القرص المرن الموجود بالأعلى للتنقل إلى صفحة إدارة التكوين لنسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل. سيساعد ذلك في الاحتفاظ بالتكوينات الخاصة بك بين عمليات إعادة التمهيد.

## Automatic Updates

Apply

Cancel

Check Every:

Notify via:  Admin GUI

Email to

Notifications will not be sent unless an email server is configured.  
Click [here](#) to manage email server settings.

### Automatic Update

	Notify ↕	Update (hh:mm) ↕	Status ↕
System Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	<input checked="" type="checkbox"/>	<input type="text" value="Never"/>	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	<input checked="" type="checkbox"/>	<input type="text" value="Immediately"/>	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

## القرار

يجب أن تكون قد انتهيت الآن من تكوين برنامج AntiVirus على موجه من السلسلة RV34x لديك.

للحصول على معلومات إضافية، راجع الموارد التالية.

- [مجتمع الموجه: مجتمع دعم الأعمال الصغيرة من Cisco](#)
- [أسئلة متداولة حول السلسلة RV34x: الأسئلة المتداولة حول الموجه RV34x Series](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة م ادخت ساب دن تسمل اذة Cisco ت مچرت  
ملاعلاء انء مچ م ف ن م دخت تسمل معد و ت م م دقت ل ة يرش ب ل و  
امك ة ق ق د ن و ك ت ن ل ة ل آل ة مچرت ل ض ف أن ة ظ حال م چ ر ة . ة ص ا خ ل م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت م م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا م ل ا ح ل ا و ه  
ل ا ا م ا د ا د و چ ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه 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 أ ل ا ي ز ي ل چ ن ا ل ا دن تسمل ا