

نم هجوم يلع ماحتق اال ع نم ماظن نيوكت RV34x ةلسلسلا

الهدف

الهدف من هذا المستند هو توضيح كيفية تكوين نظام منع التسلسل (IPS) على موجهات من السلسلة RV34x.

المقدمة

يقوم "نظام منع التسلسل" بفحص حركة المرور للبحث عن أنماط الهجمات المعروفة التي يتم منعها. يراقب هو ربط وجلسات بينما هم يتدفق من خلال المسحاج تخديد ويمسح كل ربط أن تلاءم any of the cisco ips توقيع. وعندما يكتشف أي نشاط مريب، فإنه مصمم لتسجيل أو منع حدوثه. من المهم تحديث قواعد بيانات وتعريفات IPS ومكافحة الفيروسات. يمكن تحديث هذه الملفات يدويا أو تلقائيا.

اطلع على مقاطع الفيديو هذه على نظام Cisco لمنع الاقتحام:

ومع ذلك، يمكن أن يؤثر بروتوكول IPS على أداء الموجه. بشكل عام، لا يؤثر هذا على سعة المعالجة الإجمالية لحركة مرور بروتوكول نقل النص التشعبي (HTTP) وبروتوكول نقل الملفات (FTP)، ولكن يمكنه إسقاط الحد الأقصى لعدد الاتصالات المترامنة بشكل كبير إلى حد ما.

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 استخدام هذه القيم كدليل، لأن الأداء العالمي الحقيقي قد يختلف بسبب عدد من العوامل.

الاتصالات المترامنة	معدل الاتصال	سعة معالجة HTTP	سعة معالجة FTP	
40000	3000	982 ميجابايت/ثانية	981 ميجابايت/ثانية	الإعدادات الافتراضية
15000-16000	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية	تمكين التحكم في التطبيق
16000	1500	982 ميجابايت/ثانية	981 ميجابايت/ثانية	تمكين مكافحة الفيروسات
17000	1300	982 ميجابايت/ثانية	981 ميجابايت/ثانية	تمكين IPS
15000-16000	1000	982 ميجابايت/ثانية	981 ميجابايت/ثانية	تمكين مكافحة الفيروسات و IPS للتحكم في التطبيقات

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، سيتم دفع الصوت من Spotify وسيكون اتصال آخر، مما يجعله إتصالين متزامنين.

معدل الاتصال - عدد طلبات الاتصالات/الثانية التي يمكن معالجتها.

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

تم تحديث تراخيص الأمان لتضمن حماية نظام منع الاختراقات (IPS) 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 برنامج AntiVirus على RV34x، انقر [هنا](#).

الأجهزة القابلة للتطبيق

• RV34x

إصدار البرامج

• x.1.0.03

جدول المحتويات

1. [الترخيص الذكي](#)
2. [تهيئة نظام منع الاقتحام](#)
3. [توقيعات نظام منع التسلسل](#)
4. [جدول توقيع نظام منع الاقتحام](#)
5. [حالة IPS](#)
6. [تحديث تعريفات IPS](#)
7. [القرار](#)

الترخيص الذكي

إذا لم يكن لديك حساب ذكي نشط، فستحتاج إلى متابعة الخطوات أدناه.

إذا صادفتك أية مشكلات أو مشكلات أثناء تكوين حساب "الترخيص الذكي"، فسيقوم فريق الدعم التابع لنا بالمساعدة في حل المشكلات المحتملة ويمكن الوصول إليها من خلال طرق متعددة. لا تتردد في استخدام طريقتك المفضلة للوصول إلى الآخرين.

• [مجتمع الموجه: مجتمع دعم الأعمال الصغيرة من Cisco](#)

• [أسئلة متداولة حول السلسلة RV34x: الأسئلة المتداولة حول الموجه RV34x Series](#)

• نظرة عامة على الترخيص Smart: [ترخيص البرامج الذكية](#)

• الأسئلة المتداولة حول التراخيص الذكية: [الأسئلة المتداولة حول الترخيص الذكي والحسابات الذكية للشركاء والموزعين والعملاء](#)

• إرسال حالة: [Support Case Manager \(مدير حالة الدعم\)](#)

• رقم هاتف الدعم الخاص بالولايات المتحدة/كندا: جهات اتصال TAC للأنشطة التجارية [الصغيرة](#) 1-866-606-1866

• البريد الإلكتروني للترخيص: licensing@cisco.com

الخطوة 1. إذا كنت قد قمت بإنشاء حساب Cisco.com الخاص بك أو قمت بزيارته مؤخرا، فسيتم الترحيب بك برسالة لإنشاء حساب الترخيص الذكي الخاص بك. إذا لم تقم بذلك، يمكنك النقر [هنا](#) لاخذك إلى صفحة إنشاء حساب الترخيص الذكي. قد تحتاج إلى تسجيل الدخول.

ملاحظة: للحصول على تفاصيل إضافية حول الخطوات المتعلقة بطلب حسابك الذكي، انقر [هنا](#).



الخطوة 2. عند شراء ترخيص ذكي لمسحاج تخديد، يحتاج المورد إلى إجراء عملية ينقل معرف الترخيص الفريد إلى حساب الترخيص الذكي الخاص بك. في ما يلي جدول بالمعلومات الضرورية التي سيطلب منها عند شراء الحزم.

ملاحظة: يعد كل من IPS و AntiVirus جزءا من ترخيص الأمان المستخدم لتصفية الويب وتصفية التطبيقات.

المعلومات المطلوبة	تحديد موقع المعلومات
Cisco.com معرف المستخدم	موجود في ملف تعريف حسابك، أو يمكنك النقر هنا .
اسم حساب الترخيص الذكي	من الأفضل إنشاء حسابك الذكي قبل شراء الترخيص. يجب أن تكون هذه الخطوة 8 من مقال إنشاء حساب الترخيص الذكي .
وحدة الاحتفاظ بالمخزون (SKU) للترخيص الذكي	كود تعريف المنتج للجهاز. مثال: RV340-K9-NA

ملاحظة: إذا كنت قد اشترت ترخيصا ولم يظهر في حسابك الظاهري، فعليك إما المتابعة مع بائع التجزئة لطلب التحويل أو التواصل معنا.

لجعل العملية مناسبة قدر الإمكان، يجب أن يكون لديك فاتورة الترخيص ورقم أمر المبيعات من Cisco ولقطة شاشة لصفحة ترخيص الحساب الذكي (للمشاركة مع فريقنا).

الخطوة 3. لإنشاء رمز مميز، انتقل إلى حساب [ترخيص برنامج Smart](#) الخاص بك. ثم انقر فوق [المخزون < علامة التبويب العامة](#). انقر فوق الزر رمز مميز جديد...

Virtual Account:

Hide Alerts

General

Licenses

Product Instances

Event Log

Virtual Account

Description:

Default Virtual Account: No

Product Instance Registration Tokens

The registration tokens below can be used to register new product instances to this virtual account.

New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
ZmE2- [redacted]	2019-Mar-08 19:07:30 (in 8 ...)		Allowed	Test token - rv340	[redacted]	Actions ▾
MTIz- [redacted]	2019-Mar-08 17:41:45 (in 8 ...)		Allowed	Test Token 1-2019	[redacted]	Actions ▾
ZDE- [redacted]	2020-Feb-06 17:18:54 (in 34...)	1 of 5	Allowed	[redacted] Token	[redacted]	Actions ▾

The token will be expired when either the expiration or the maximum uses is reached

Showing All 3 Records

الخطوة 4. يتم فتح نافذة إنشاء رمز تسجيل مميز. أدخل الوصف، وتنتهي الصلاحية بعد، والحد الأقصى. عدد الاستخدامات. ثم اضغط على الزر إنشاء رمز مميز.

ملاحظة: 30 يوما لانتها الصلاحية بعد التوصية بها.

Create Registration Token

This will create a token that is used to register product instances, so that they can use licenses from this virtual account. Once it's created, go to the Smart Licensing configuration for your products and enter the token, to register them with this virtual account.

Virtual Account:

Description :

1

Test

* Expire After:

2

30

Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

3

1

The token will be expired when either the expiration or the maximum uses is reached

 Allow export-controlled functionality on the products registered with this token

4

Create Token

Cancel

الخطوة 5. بمجرد إنشاء الرمز المميز، يمكنك النقر فوق ارتباط الرمز المميز (مربع أزرق بسهم أبيض) زر الموجود على يمين الرمز المميز الذي تم إنشاؤه مؤخرا.

Product Instance Registration Tokens

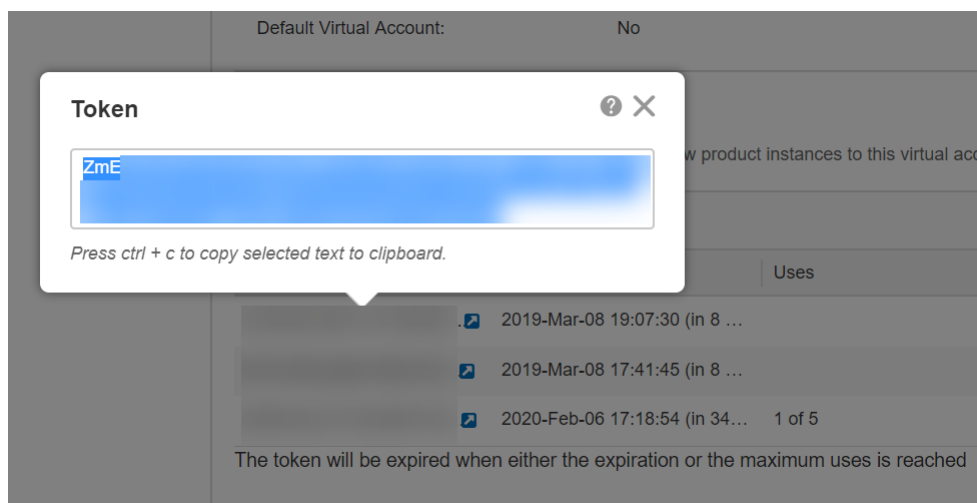
The registration tokens below can be used to register new product instances to this virtual account.

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
Zm	2019-Mar-08 19:07:30 (in 8 ...)		Allowed	Test token - rv340		Actions
MT	2019-Mar-08 17:41:45 (in 8 ...)		Allowed	Test Token 1-2019		Actions
ZD	2020-Feb-06 17:18:54 (in 34...)	1 of 5	Allowed			Actions

The token will be expired when either the expiration or the maximum uses is reached

Showing All 3 Records

الخطوة 6. يجب أن تظهر نافذة الرمز المميز مع الرمز المميز الكامل للنسخ. ركزت الرمز المميز، انقر بزر الماوس الأيمن فوق الرمز المميز وانقر فوق نسخ أو يمكنك الضغط مع الاستمرار على زر **ctrl** على لوحة المفاتيح وانقر فوق **C** في نفس الوقت لنسخ النص.



الخطوة 7. بمجرد نسخ الرمز المميز، ستحتاج إلى تسجيل الدخول إلى الجهاز وتحميل مفتاح الرمز المميز. قم بتسجيل الدخول إلى صفحة تكوين الويب للموجه.



Router

cisco

●●●●●●●●|

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 8. انتقل إلى الترخيص.

- Getting Started
- Status and Statistics
- Administration
- System Configuration
- WAN
- LAN
- Routing
- Firewall
- VPN
- Security
- QoS
- Configuration Wizards
- License**

الخطوة 9. إذا كان جهازك غير مسجل، فسيتم إدراج حالة تحويل الترخيص الخاصة بك كوضع تقييم. الصق الرمز المميز (الخطوة 6 من هذا القسم) الذي قمت بتكوينه من صفحة مدير الترخيص الذكي. ثم انقر فوق تسجيل.

ملاحظة: قد تستغرق عملية التسجيل بعض الوقت، يرجى الانتظار حتى تنتهي.

! You are currently running in evaluation mode, to register an account:

- Ensure this product has internet access.
- Click [here](#) to access your Cisco Smart Account.
- Navigate to the Virtual Account section which contains licenses.
- Generate and copy a token for the specific license to be applied to this device.
- Paste the token into the box below.

Paste the token here...

1

* Click [Register](#) 2

الخطوة 10. بمجرد تسجيل الرمز المميز، ستحتاج إلى تخصيص الترخيص. انقر فوق الزر إختيار التراخيص.

Registration Status: Registered (Feb 12, 2019)

License Authorization Status: Authorized (Feb 28, 2019)

Smart Account: [Redacted]

Virtual Account: [Redacted]

PID: [Redacted]

Export-Controlled Functionality: [Redacted]

Smart License Usage

[Choose Licenses](#)

[Redacted Table]

الخطوة 11. يجب أن يظهر إطار إختيار التراخيص الذكية. تحقق من ترخيص الأمان ثم اضغط على حفظ والتحويل.

Choose Smart Licenses

Choose Smart Licenses to be used by this product. Ensure you have a sufficient number of licenses in the Virtual Account associated with this product, otherwise it will be out of compliance.

Enable	Name (Version)	Description	Count
<input checked="" type="checkbox"/>	Security-License	Anti Threat Services: IPS, AppID, Dynamic ...	--

Save and Authorize

Cancel

الخطوة 12. يجب اعتماد حالة ترخيص الأمان الآن.

Name	Description	Count	Status
Security-License	Anti Threat Services: IPS, AppID, Dyn...	--	Authorized

يجب أن تكون الآن قادرا على المضي قدما في تكوين نظام منع الاقتحام.

تهيئة نظام منع الاقتحام

الخطوة 1. إذا لم تسجل دخولك إلى الموجه بعد، فسجل الدخول إلى صفحة تكوين الويب الخاصة بالموجه.



Router

cisco

●●●●●●●●|

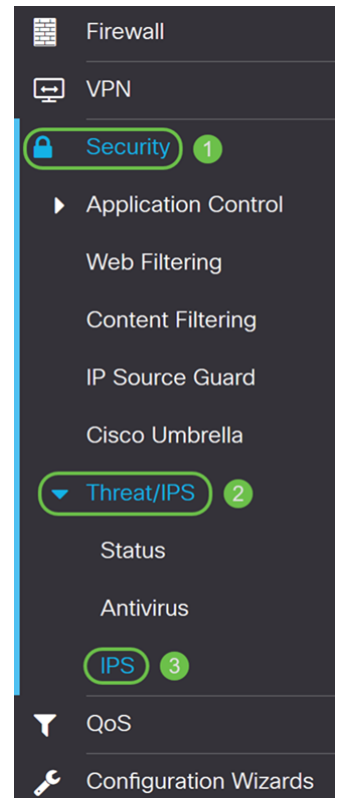
English ▾

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 > IPS.



الخطوة 3. حدد تشغيل لتمكين ميزة نظام منع التسلسل. إذا كنت تريد إيقاف تشغيله، حدد إيقاف التشغيل.

سنقوم باختيار تشغيل في هذا المثال.

IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS): On Off

Mode: Block Attacks (Prevention)
 Log Only (Detection)

IPS Security Level: Connectivity **i**
 Balanced **i**
 Security **i**

الخطوة 4. حدد إما حظر الهجمات (منع) أو السجل فقط. في هذا المثال، سنختار منع الهجمات (منع). يتم تحديد الخيارات التالية أدناه.

- منع الهجمات (منع) - حدد لحظر كافة الهجمات. ويسجل أيضا حالة الشذوذ.
- السجل فقط - سيقوم هذا الخيار بإنشاء السجل فقط (باستخدام معلومات العميل، ومعرف التوقيع، وما إلى ذلك) عند تحديد الحالات الشاذة. لا يؤثر على الاتصال.

IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS): On Off

Mode: Block Attacks (Prevention)
 Log Only (Detection)

IPS Security Level: Connectivity **i**
 Balanced **i**
 Security **i**

الخطوة 5. حدد مستوى أمان IPS الذي تريد استخدامه. يتم تعريف الخيارات التالية على أنها:

- الاتصال - سيقوم هذا الوضع باكتشاف الهجمات الأكثر خطورة. وهذا يوفر أقل قدر من الحماية: يتم اكتشاف هجمات المخاطر (عالية الخطورة) فقط. هذا هو الخيار الأقل أمانا.
- متوازن - وهذا يوفر حماية متوسطة: (عالية + متوسطة الخطورة) يتم فحصها عن طريق تمرير توقيعات منخفضة المخاطر. هذا هو مستوى الأمان المتوسط ل IPS.
- الأمان - سيكتشف وضع الأمان الهجمات العادية بالإضافة إلى الهجمات الشديدة والخطيرة. يوفر ذلك أقصى حماية: يتم فحص جميع القواعد (عالية + متوسطة + منخفضة الخطورة). هذا هو أعلى مستوى أمان ل IPS.

ملاحظة: كلما ارتفع مستوى الأمان الذي تختاره، كلما زاد عدد الهجمات التي يتم رصدها، كلما زاد التأثير على أداء النظام الذي قد يحدث.

سنختار متوازن لهذا العرض التوضيحي.

Intrusion Prevention System (IPS): On Off

Mode: Block Attacks (Prevention)
 Log Only (Detection)

IPS Security Level: Connectivity **i**
 Balanced **i**
 Security **i**

توقيعات نظام منع التسلسل

الخطوة 6. في حقل آخر تحديث، سيعرض تاريخ ووقت آخر توقيع تم تحديثه.

Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010

Search By IPS Signature ID:

الخطوة 7. يعرض إصدار الملف إصدار التوقيع الذي يتم استخدامه.

Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010

Search By IPS Signature ID:

الخطوة 8. للبحث عن معرف توقيع، أدخل معرف التوقيع في حقل البحث بواسطة معرف توقيع IPS وانقر فوق بحث للتحقق مما إذا كان التوقيع مدعوما أم لا. إذا كان معرف التوقيع مدعوما، سيتم تحديث الجدول بالنتيجة كما هو موضح أدناه.

ملاحظة: إذا لم يكن معرف التوقيع مدعوما، فلن يظهر أي شيء في الجدول.

Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010 ¹

Search By IPS Signature ID:

² Search

IPS Signature Table

Name	ID	Severity	Category
³ TROJAN Keylogger connection	8005394	high	successful-recon-limited

Showing 1 - 1 of 1

جدول توقيع نظام منع الاقتحام

الخطوة 9. في جدول توقيع IPS، يتم تعريف الحقول التالية على أنها:

• الاسم - اسم التوقيع.

• المعرف - المعرف الفريد للتوقيع. سيؤدي النقر فوق المعرف إلى فتح نافذة لعرض التفاصيل الكاملة للتوقيع المحدد.

• الخطورة -

• الفئة -

IPS Signature Table

¹ Name	² ID	³ Severity	⁴ Category
SERVER /etc/passwd misc attack	8000135	high	attempted-recon
OTHER Scan ident version requ...	8004101	high	attempted-recon
OTHER Scan Webtrends Scann...	8004120	high	attempted-recon
PROTOCOL TELNET resolv_ho...	8004195	high	attempted-admin

Showing 1 - 50 of 2864

الخطوة 10. (إختياري) إذا قمت بالنقر فوق معرف التوقيع في جدول توقيع IPS، ستظهر نافذة لتظهر لك التفاصيل الكاملة للتوقيع المحدد.

Selected Signature

ID:	8000135
Name:	SERVER /etc/passwd misc attack
Impact:	Information Gathering.
Description:	This event is generated when an attempt is made to retrieve a protected system file on a host via a web request.
Recommendation:	Webservers should not be allowed to view or execute files and binaries outside of it's designated web root or cgi-bin. This file may also be requested on a command line should the attacker gain access to the machine. Making the file read only by the superuser on the system will disallow viewing of the file by other users.
Category:	attempted-recon
Severity:	high

Cancel

الخطوة 11. في أسفل جدول توقيع IPS، حدد الأسهم وكذلك الأرقام التي تريد الانتقال بها إلى الأمام والخلف على الجدول. يمكنك أيضا تحديد مقدار الخطوط (50، 100، أو 150) لكل صفحة في السطور لكل صفحة في القائمة المنسدلة.

FILE FLAC libFLAC VORBIS buf...	8009043	high	attempted-user
FILE FLAC libFLAC picture buff...	8009044	high	attempted-user
FILE Microsoft Media Player asf...	8009047	high	attempted-user
FILE Microsoft Media Player int...	8009048	high	attempted-user
FILE Microsoft Media Player int...	8009049	high	attempted-user
FILE Microsoft Media Player int...	8009050	high	attempted-user
OS Windows SMB misc attack	8009053	high	attempted-admin
OS Windows SMB misc attack	8009054	high	attempted-admin
FILE Adobe Flash Player embe...	8009068	high	attempted-admin
SERVER Outlook VEVENT overfl...	8009071	high	attempted-user

1 2 3 ... 58 50 lines per page Showing 1 - 5

الخطوة 12. انقر فوق تطبيق لحفظ التغييرات التي أجريتها على ملف التكوين الجاري تشغيله.

IPS (Intrusion Prevention System)


Apply

Cancel


Intrusion Prevention System (IPS): On Off

Mode: Block Attacks (Prevention)

Log Only (Detection)

IPS Security Level: Connectivity 

Balanced 

Security 

Intrusion Prevention System Signatures

Last Update: 2019-Feb-26, 19:07:20 GMT

File Version: 2.4.0.0010

Search By IPS Signature ID:

Search

IPS Signature Table

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 الخاص بك بين عمليات إعادة التمهيدي، انسخ ملف التكوين الجاري تشغيله إلى ملف تكوين بدء التشغيل.

في الخطوات القليلة التالية، سنعرض لك كيفية نسخ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.

الخطوة 13. انقر أيقونة القرص المرن (حفظ) في أعلى الصفحة. وهذا سيقوم بإعادة توجيهك إلى إدارة التكوين لحفظ التكوين الجاري تشغيله إلى تكوين بدء التشغيل.



cisco (admin)

English



الخطوة 14. 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 التمهيدي.

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.

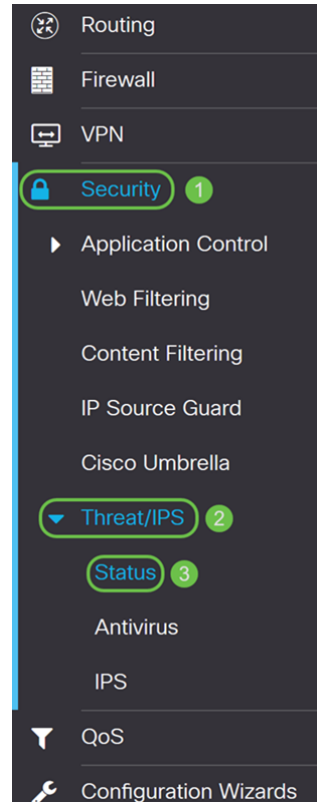
Source: 1 Running Configuration

Destination: 2 Startup Configuration

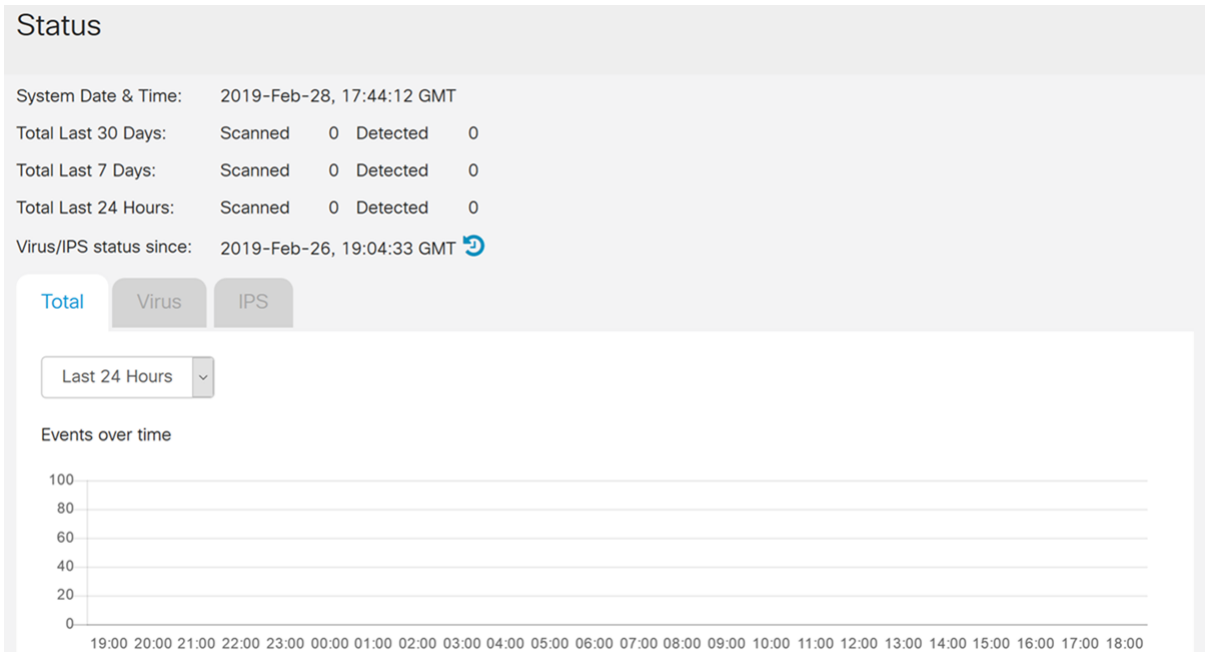
Save Icon Blinking: Enable

حالة IPS

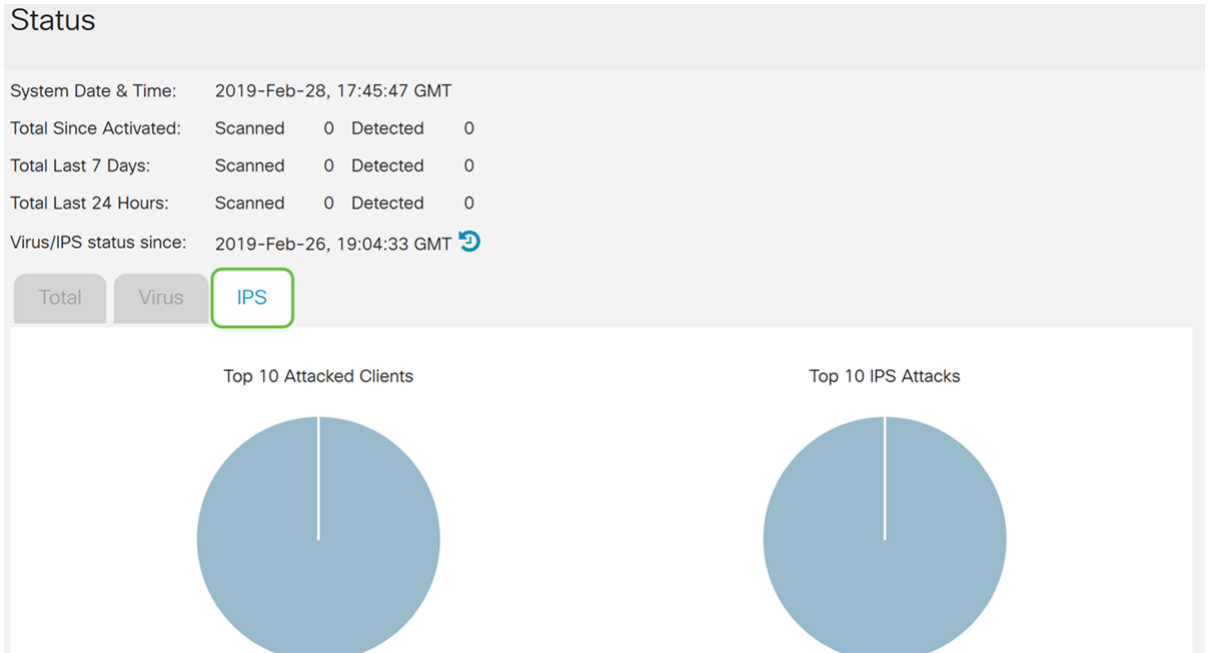
الخطوة 1. انتقل إلى الأمان < التهديد/IPS < الحالة.



الخطوة 2. تعرض صفحة الحالة تفاصيل التهديدات والهجمات عند تكوين ميزات الحماية من التهديد وبروتوكول الإنترنت (IPS). توفر لك لوحة المعلومات عرضاً لمُلخَص الأحداث بالكامل ومعلومات مفصلة عن التهديدات والهجمات التي تم الكشف عنها وفقاً للتحديد مثل اليوم والأسبوع والشهر.



الخطوة 3. انقر فوق علامة التبويب **IPS**. وسيعرض هذا أفضل 10 عملاء مهاجمين بالإضافة إلى أكبر 10 هجمات ضمن خطة الحماية الدولية.

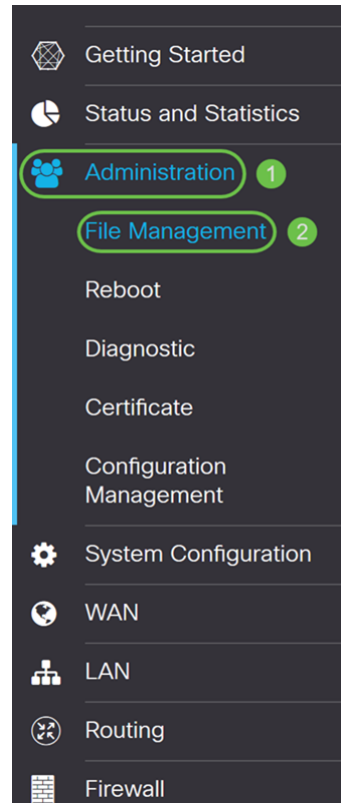


تحديث تعريفات IPS

يمكنك تحديث تعريف IPS يدويا أو تلقائيا. توضح الخطوات من 1 إلى 2 كيفية تحديث تعريف IPS يدويا بينما تظهر لك الخطوات 3-6 كيفية تحديث تعريف IPS تلقائيا.

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

الخطوة 1. لتحديث تعريفات IPS 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.

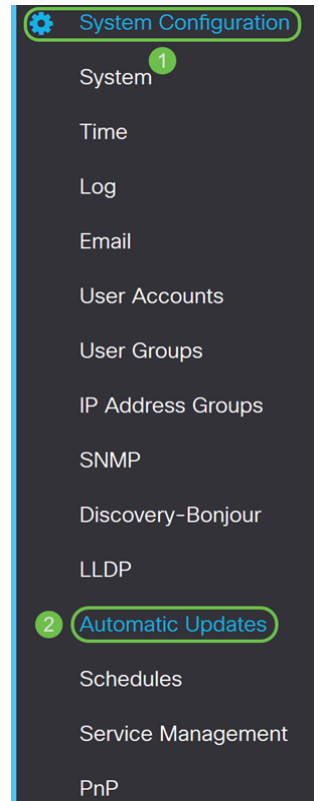
Manual Upgrade

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 تعريفات IPS تلقائياً، انتقل إلى تكوين النظام < التحديثات التلقائية.



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: Week

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"/>	Never	Version 0.0.0.1, Version 1.0.02.16 is available on Cisco.com.
USB Modem Firmware	<input checked="" type="checkbox"/>	Never	Version 1.0.00.01, Version 0.0.00.01 is available on Cisco.com.
Security Signature	<input checked="" type="checkbox"/>	Immediately	Version 2.0.0.0006 was applied on 2019-Feb-26, 19:07:20 GMT, ...

القرار

يجب أن تكون قد انتهت الآن من تكوين نظام منع الاقتحام بنجاح على موجه من السلسلة RV34x.

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل