

# RV34xシリーズルータの侵入防御システムの設定

## 目的

このドキュメントの目的は、RV34xシリーズルータで侵入防御システム(IPS)を設定する方法を示すことです。

## 概要

侵入防御システム(IPS)はトラフィックをスキャンして、ブロックする既知の攻撃パターンを探します。ルータを通過するパケットとセッションを監視し、各パケットをスキャンして任意のCisco IPSシグニチャと一致させます。疑わしいアクティビティを検出すると、ログを記録またはブロックするように設計されています。IPSおよびウイルス対策データベースと定義を更新することが重要です。これらは手動または自動で更新できます。

Cisco Intrusion Prevention Systemの次のビデオをご覧ください。

ただし、IPSはルータのパフォーマンスに影響を与える可能性があります。一般に、ハイパーテキスト転送プロトコル(HTTP)トラフィックとファイル転送プロトコル(FTP)トラフィックの総スループットには影響しませんが、同時接続の最大数を大幅に減らすことができます。

**特記事項：**ルータの負荷が大きい場合は、問題が悪化する可能性があります。

次の表に、さまざまな設定でのパフォーマンスに関する予想される統計情報を示します。これらの値はガイドとして使用する必要があります。実際のパフォーマンスは多くの要因によって異なる場合があります。

	同時接続	接続レート	HTTPスループット	FTPスループット
デフォルト設定	40000	3,000	982 MB/秒	981 MB/秒
APP制御の有効化	15000-16000	1300	982 MB/秒	981 MB/秒
ウイルス対策を有効にする	16000	1,500	982 MB/秒	981 MB/秒
IPSの有効化	17000	1300	982 MB/秒	981 MB/秒
App Control Antivirus & IPSの有効化	15000-16000	1,000	982 MB/秒	981 MB/秒

次のフィールドは次のように定義されます。

**同時接続数**：同時接続数の合計。たとえば、あるサイトからファイルをダウンロードしている場合、つまり1つの接続であるSpotifyからオーディオをストリーミングして、別の接続を確立し、同時に2つの接続を確立します。

**Connection Rate**：処理できる接続要求の数/秒。

**HTTP/FTPスループット**:HTTPおよびFTPのスループットは、ダウンロード速度 ( MB/秒 ) です。

セキュリティライセンスが更新され、既存のアプリケーションやWebフィルタリングに加えてIPS保護が追加されました。セキュリティライセンスを取得するには、スマートアカウントが必要です。アクティブなスマートアカウントがない場合は、このドキュメントのセクション1が必要です。

RV34xでウイルス対策を設定する方法については、[ここをクリックしてください](#)。

## 該当するデバイス

RV34x

## [Software Version]

1.0.03.x

## 目次

1. [Smart Licensing](#)
2. [侵入防御システムの設定](#)  
を選択します。 [侵入防御システムシグニチャ](#)
4. [侵入防御システムのシグニチャテーブル](#)
5. [IPSステータス](#)
6. [IPS定義の更新](#)
7. [結論](#)

## Smart Licensing

アクティブなスマートアカウントがない場合は、次の手順に進む必要があります。

スマートライセンスアカウントの設定中に問題が発生した場合は、サポートチームが潜在的な問題を解決し、複数の方法で問題を解決できます。ご希望の方法で連絡してください。

ルータコミュニティ : [Cisco Small Business Support Community](#)

RV34xシリーズに関するFAQ: [RV34xシリーズルータに関するFAQ](#)

スマートライセンスの概要 : [スマート ソフトウェア ライセンシング](#)

スマートライセンスに関するFAQ: [パートナー、ディストリビュータ、およびお客様向けのスマートライセンスおよびスマートアカウントに関するFAQ](#)

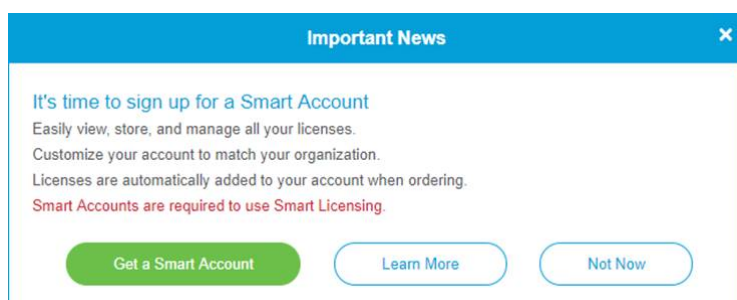
ケースを送信します。 [Support Case Manager](#)

米国/カナダのサポート電話番号 : 1-866-606-1866または[Small Business TACの連絡先](#)

メール : [licensing@cisco.com](mailto:licensing@cisco.com)

ステップ1 : 最近Cisco.comアカウントを作成または閲覧した場合は、独自のスマートライセンスアカウントを作成するためのメッセージが表示されます。Smart Licenseアカウントの作成ページに[移動する](#)には、ここをクリックしてください。ログインが必要になる場合があります。

注 : スマートアカウントのリクエスト手順の詳細については、[ここをクリックしてください](#)。



ステップ2 : ルータのスマートライセンスを購入する際には、ベンダーが独自のライセンスIDをスマートライセンスアカウントに移動するプロセスを行う必要があります。次の表は、バンドルの購入時に必要な情報を示しています。

注 : IPSとアンチウイルスは、Webフィルタリングとアプリケーションフィルタリングに使用されるセキュリティライセンスの一部です。

必要な情報	情報の検索
Cisco.comユーザID	アカウントプロファイルに配置するか、 <a href="#">ここをクリックできます</a> 。
スマートライセンスアカウント名	ライセンスを購入する前にスマートアカウントを作成しておくことをお勧めします。これは、「 <a href="#">スマートライセンスアカウントの作成」の記事のステップ8</a> です。
スマートライセンスSKU	デバイスの製品識別コード。例 : RV340-K9-NA

注：ライセンスを購入していて、仮想アカウントに表示されない場合は、リセラーに連絡して転送を要求するか、または当社に連絡してください。

プロセスを適切に行うには、ライセンス請求書、シスコの販売注文番号、およびスマートアカウントライセンスページのスクリーンショットを用意する必要があります（チームと共有するため）。

ステップ3：トークンを生成するには、スマートソフトウェアライセンス [アカウントに移動](#) します。次に、[インベントリ] > [全般] タブをクリックします。[New Token...] ボタンをクリックします。

## Smart Software Licensing

[Feedback](#) [Support](#) [Help](#)

Alerts **Inventory** | [Convert to Smart Licensing](#) | [Reports](#) | [Preferences](#) | [Satellites](#) | [Activity](#) [Questions About Licensing?](#)  [Try our Virtual Assistant](#)

Virtual Account: [Redacted] 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- <span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	2019-Mar-08 19:07:30 (in 8 ...)		Allowed	Test token - rv340	<span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	<a href="#">Actions</a> ▾
MTiz- <span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	2019-Mar-08 17:41:45 (in 8 ...)		Allowed	Test Token 1-2019	<span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	<a href="#">Actions</a> ▾
ZDE- <span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	2020-Feb-06 17:18:54 (in 34...)	1 of 5	Allowed	<span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span> Token	<span style="background-color: #e0e0e0; padding: 0 5px;">[Redacted]</span>	<a href="#">Actions</a> ▾

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

Showing All 3 Records

ステップ4:[Create Registration Token] ウィンドウが開きます。[説明]、[期限切れ後]、[最大値]を入力します。使用回数。次に、[トークンの作成] ボタンを押します。

注：30日間の有効期限が推奨されます。

## 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

ステップ5: トークンが生成されたら、最近作成したトークンの右側にある[Token]リンク (白い矢印の付いた青いボックス) ボタンをクリックします。

### Product Instance Registration Tokens

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

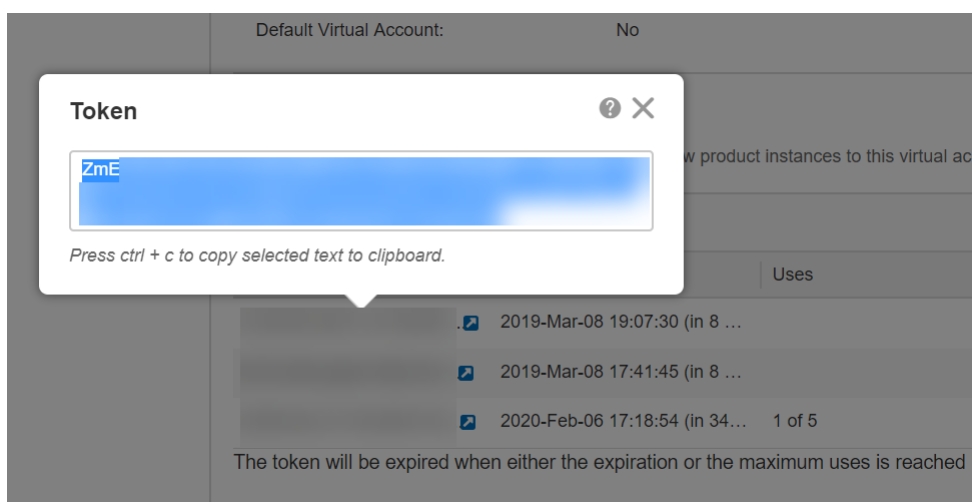
New Token...

Token	Expiration Date	Uses	Export-Controlled	Description	Created By	Actions
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

ステップ6: コピーする完全なトークンが含まれた[Token]ウィンドウが表示されます。トークンを強調表示し、トークンを右クリックして[Copy]をクリックするか、キーボードのctrlボタンを押したままcを同時にクリックしてテキストをコピーします。



ステップ7: トークンをコピーしたら、デバイスにログインし、トークンキーをアップロードする必要があります。ルータのWeb設定ページにログインします。



# Router

cisco

●●●●●●●●|

English

Login

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

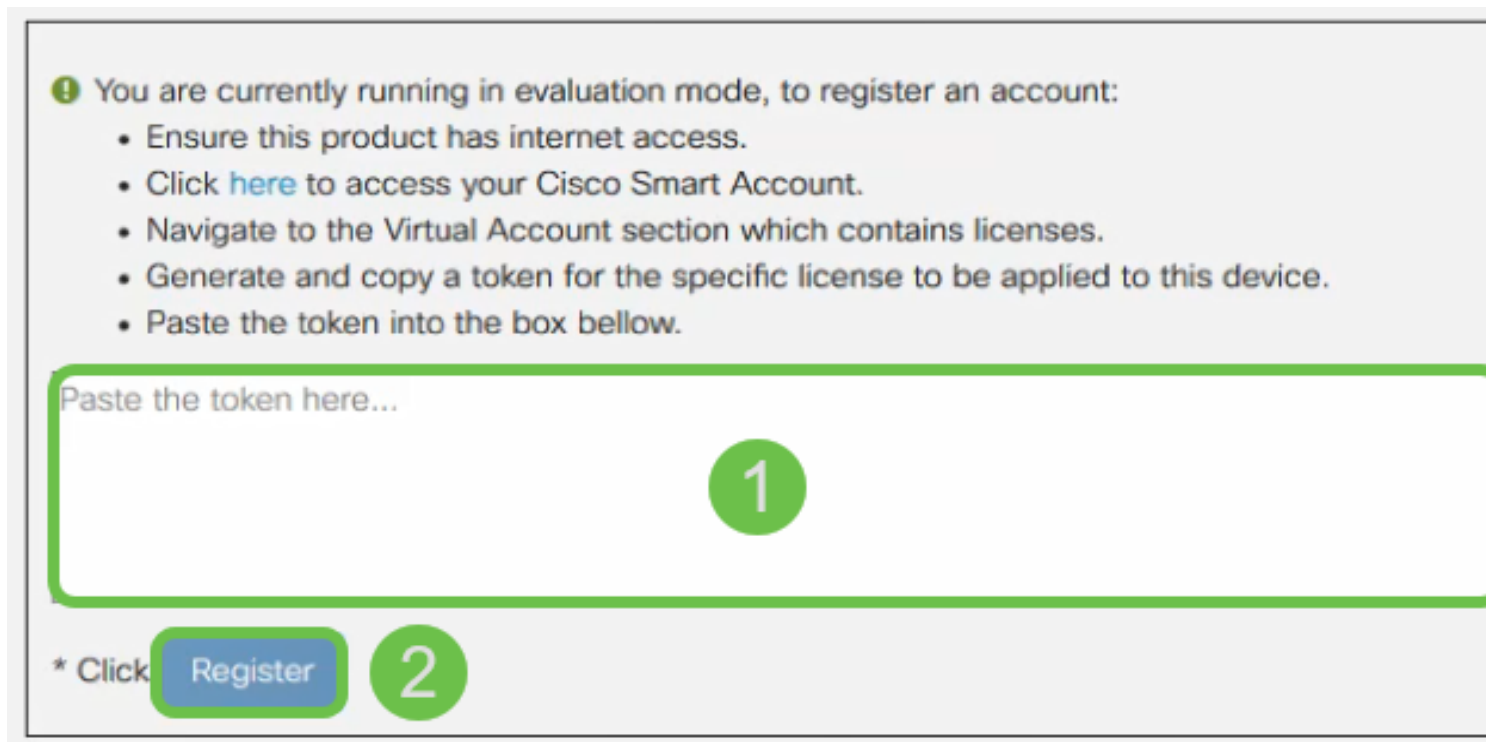
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

ステップ8:[License]に移動します。

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

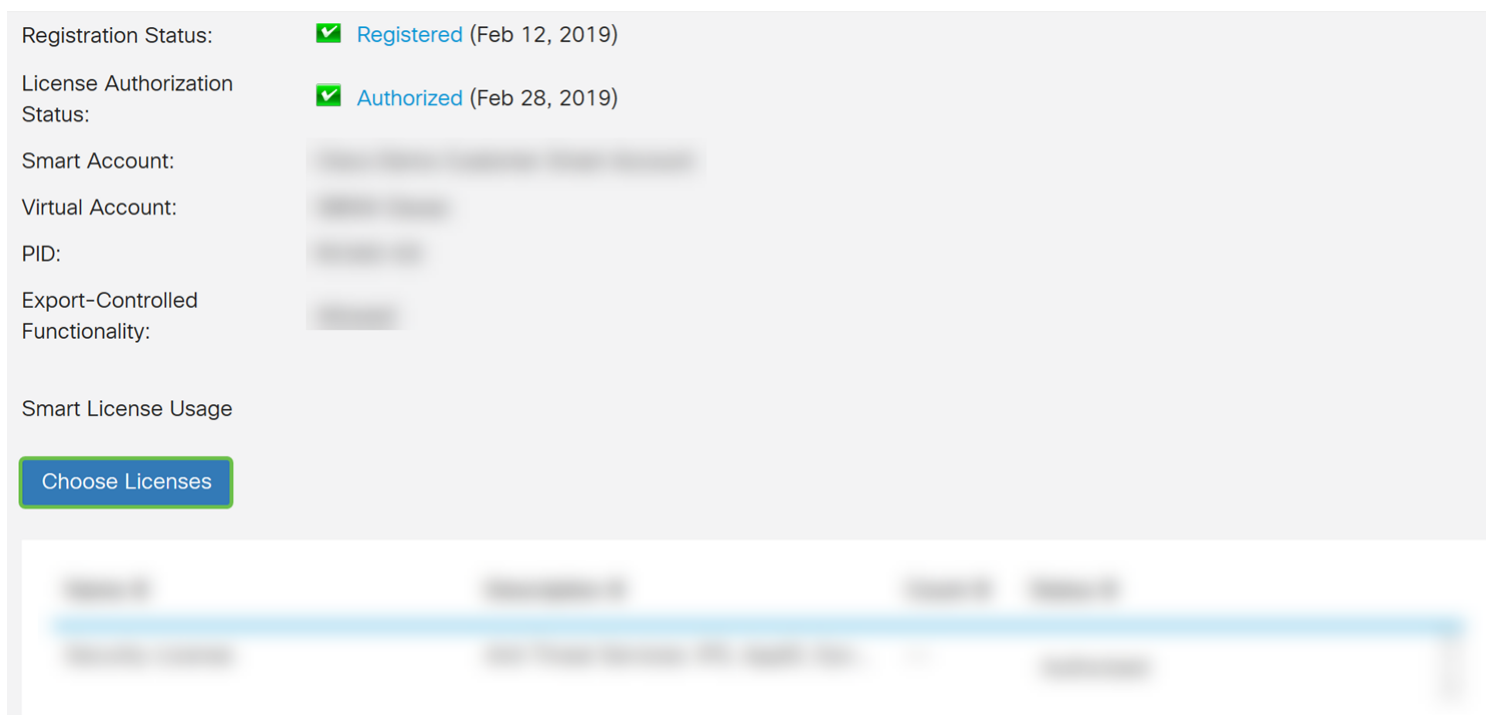
ステップ9：デバイスが登録解除されると、ライセンス認証ステータスが評価モードとして表示されます。[Smart Licensing Manager]ページから生成したトークン(このセクションのステップ6)を貼り付けます。次に、[登録]をクリックします。

注：登録プロセスに時間がかかる可能性があります。完了するまでお待ちください。



The screenshot shows a registration interface. At the top, there is a green information icon followed by the text: "You are currently running in evaluation mode, to register an account:". Below this, there is a bulleted list of instructions: "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.", and "Paste the token into the box below.". Below the list is a large text input field with the placeholder text "Paste the token here...". A green circle with the number "1" is positioned to the right of the input field. Below the input field, there is a blue button labeled "Register" with a green circle and the number "2" next to it. To the left of the button, the text "\* Click" is visible.

ステップ10：トークンを登録したら、ライセンスを割り当てる必要があります。[ライセンスの選択]ボタンをクリックします。



The screenshot shows a page with registration and license authorization status. The "Registration Status:" is "Registered (Feb 12, 2019)" with a green checkmark. The "License Authorization Status:" is "Authorized (Feb 28, 2019)" with a green checkmark. Below these are fields for "Smart Account:", "Virtual Account:", "PID:", and "Export-Controlled Functionality:", all of which are blurred. At the bottom, there is a section for "Smart License Usage" with a blue button labeled "Choose Licenses". Below the button, there is a table with columns for "License", "Status", "Action", and "Date", but the content is blurred.

ステップ11:[スマートライセンスの選択]ウィンドウが表示されます。Security-Licenseを確認し、Save and Authorizeを押します。

## 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

ステップ12：セキュリティライセンスのステータスは、今すぐ承認されます。

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

これで、侵入防御システムの設定に進むことができます。

## 侵入防御システムの設定

ステップ1：まだルータにログインしていない場合は、ルータのWeb設定ページにログインします。





# 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.

ステップ2:[Security] > [Threat/IPS] > [IPS]に移動します。

- Firewall
- VPN
- Security** 1
  - ▶ Application Control
  - Web Filtering
  - Content Filtering
  - IP Source Guard
  - Cisco Umbrella
  - Threat/IPS** 2
    - Status
    - Antivirus
    - IPS** 3
- QoS
- Configuration Wizards

ステップ3：侵入防御システム(IPS)機能を有効にするには、[オン(On)]を選択します。オフにするには、[オフ]を選択します。

この例ではOnを選択します。

## IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS):  On  Off

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

IPS Security Level:  Connectivity ⓘ  
 Balanced ⓘ  
 Security ⓘ

ステップ4:[Block Attacks (Prevention)]または[Log Only]を選択します。この例では、[Block Attacks (Prevention)]を選択します。次のオプションを定義します。

**Block Attacks (Prevention)** -すべての攻撃をブロックします。また、異常も記録されます。

**Log Only**△接続には影響しません。

## IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS):  On  Off

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

IPS Security Level:  Connectivity ⓘ  
 Balanced ⓘ  
 Security ⓘ

ステップ5：使用するIPSセキュリティレベルを選択します。次のオプションを定義します。

**Connectivity**これにより、保護が最小限になります。(重大度が高い)リスク攻撃だけが検出されます。これは最もセキュアでないオプションです。

**Balanced** – 選択したモードは、重大な攻撃と同時に重大な攻撃を検出します。これは中程度の保護を提供します。(重大度の高+中)は、低リスクのシグニチャを渡すことによって検査されます。これは、IPSの中間レベルのセキュリティです。

**セキュリティ**：セキュリティモードは、重大および重大な攻撃とともに通常の攻撃を検出します。これにより、最も保護が強化されます。すべてのルール(高+中+低)が検査されます。これは、IPSの最高のセキュリティレベルです。

注：選択するセキュリティレベルが高いほど、モニタされる攻撃が多くなるため、システムパフォーマンスへの影響が大きくなります。

このデモンストレーションでは[Balanced]を選択します。

Intrusion Prevention System (IPS):  On  Off

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

IPS Security Level:  Connectivity ⓘ  
 Balanced ⓘ  
 Security ⓘ

## 侵入防御システムシグニチャ

ステップ6:[Last Update]フィールドに、最後に更新された署名の日時が表示されます。

### Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID:

ステップ7:[ファイルのバージョン(File Version)]に、使用されている署名のバージョンが表示されます。

### Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID:

ステップ8：シグニチャIDを検索するには、[Search by IPS Signature ID]フィールドにシグニチャIDを入力し、[Search]をクリックしてシグニチャがサポートされているかどうかを確認します。シグニチャIDがサポートされている場合、テーブルは次のような結果で更新されます。

注：シグニチャIDがサポートされていない場合、テーブルには何も表示されません。

# 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:

8005394 2

Search

## IPS Signature Table

Name	ID	Severity	Category
<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">3</span> TROJAN Keylogger connection	8005394	high	successful-recon-limited

Navigation: 1 | 50 lines per page | Showing 1 - 1 of 1

## 侵入防御システムのシグニチャテーブル

ステップ9:[IPS Signature Table]で、次のフィールドを次のように定義します。

### Name

**ID** : シグニチャの一意的識別子。IDをクリックすると、ウィンドウが開き、選択した署名の詳細が表示されます。

**Severity** : 重大度はセキュリティへの影響を示します。

### Category

## IPS Signature Table

<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">1</span> Name	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">2</span> ID	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">3</span> Severity	<span style="border: 1px solid green; border-radius: 50%; padding: 2px;">4</span> 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

Navigation: 1 | 2 | 3 | ... | 58 | 50 lines per page | Showing 1 - 50 of 2864

ステップ10: ( オプション ) IPSシグニチャテーブルでシグニチャIDをクリックした場合は、選択したシグニチャの完全な詳細を示すウィンドウが表示されます。

## 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

ステップ11:IPSシグニチャテーブルの下部で、矢印と番号を選択して、テーブルを前後に移動します。[ページあたりの行数(Lines per page)]ドロップダウンリストで、ページあたりの行数(50、100、または150)を選択することもできます。

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 [Navigation icons: Home, Left, 1, 2, 3, ..., 58, Right, End]

② [Dropdown menu: 50, 100, 150]

50 lines per page

Showing 1 - 5

ステップ12:[Apply]をクリックして、実行コンフィギュレーションファイルに変更を保存します。

# 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

^

注：ルータが使用しているすべての設定は、現在実行コンフィギュレーションファイルに含まれています。このファイルは揮発性であり、リブートの間は保持されません。リブートの間も設定を保持するには、実行コンフィギュレーションファイルをスタートアップコンフィギュレーションファイルにコピーします。

次のいくつかの手順では、実行コンフィギュレーションをスタートアップコンフィギュレーションにコピーする方法を示します。

ステップ13： ページ上部のフッピーディスク(保存)アイコンをクリックします。これにより、[構成管理]にリダイレクトされ、実行構成をスタートアップコンフィギュレーションに保存します。



cisco (admin)

English



ステップ14:[Configuration Management]で、[Copy/Save Configuration]セクションまで下にスクロールします。[Source]が[Running Configuration]、[Destination]が[Startup Configuration]であることを確認してください。[Apply] をクリックします。これにより、実行コンフィギュレーションファイルがスタートアップコンフィギュレーションファイルにコピーされ、リブート間も設定が保持されます。

## 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.

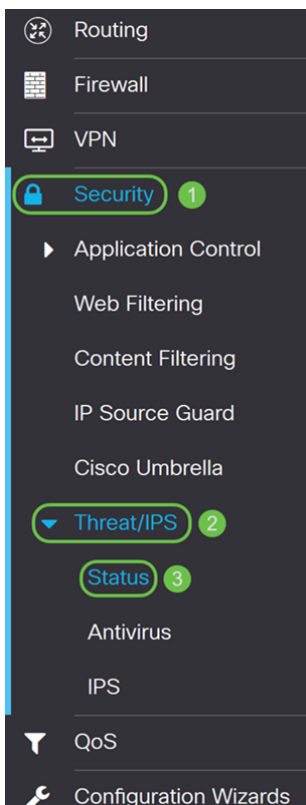
Source: 1 Running Configuration

Destination: 2 Startup Configuration

Save Icon Blinking: Enable

## IPSステータス

ステップ1:[Security] > [Threat/IPS] > [Status]に移動します。



ステップ2:[Status] ページに、脅威と攻撃に対する対策およびIPS機能が設定されている場合の詳細情報が表示されます。ダッシュボードには、イベント全体の概要と、選択した日、週、月ごとに検出された脅威と攻撃の詳細情報が表示されます。

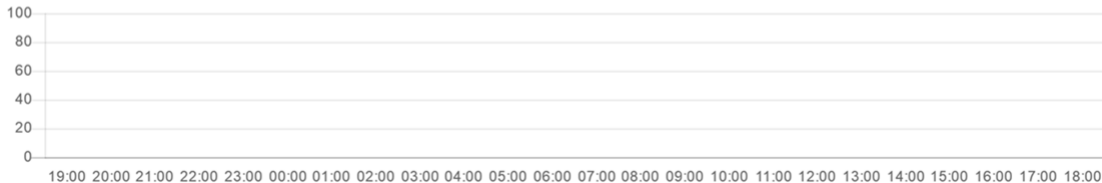
## Status

System Date & Time: 2019-Feb-28, 17:44:12 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-Feb-26, 19:04:33 GMT ↻

Total Virus IPS

Last 24 Hours ▾

Events over time



ステップ3:[IPS]タブをクリックします。これにより、攻撃を受けたクライアントのトップ10とIPS攻撃のトップ10が表示されます。

## Status

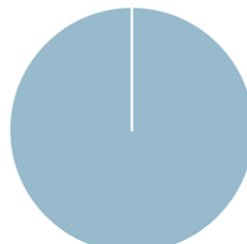
System Date & Time: 2019-Feb-28, 17:45:47 GMT  
Total Since Activated: Scanned 0 Detected 0  
Total Last 7 Days: Scanned 0 Detected 0  
Total Last 24 Hours: Scanned 0 Detected 0  
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT ↻

Total Virus IPS

Top 10 Attacked Clients



Top 10 IPS Attacks



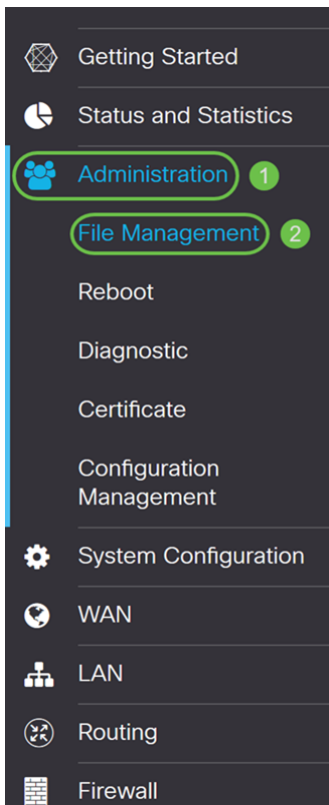
## IPS定義の更新

IPS定義は、手動または自動で更新できます。ステップ1～2ではIPS定義を手動で更新する方法を示し、ステップ3～6ではIPS定義を自動的に更新する方法を示します。

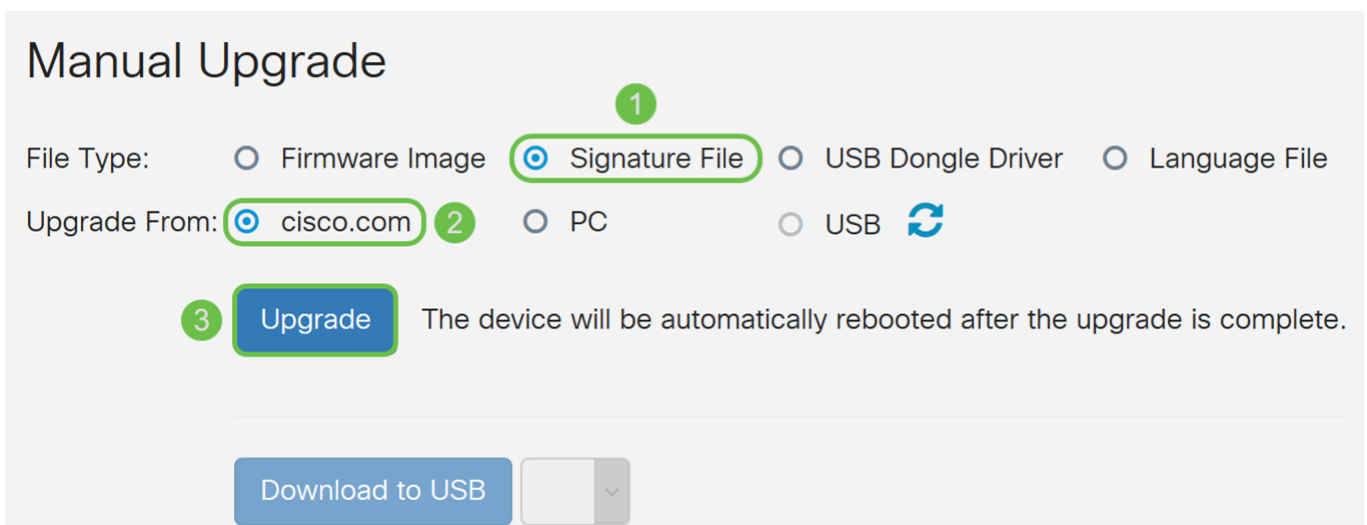
ベストプラクティス:セキュリティシグニチャを毎週自動的に更新することをお勧めします。

ステップ1:IPS定義を手動で更新するには、[Administration] > [File Management]に移動します。

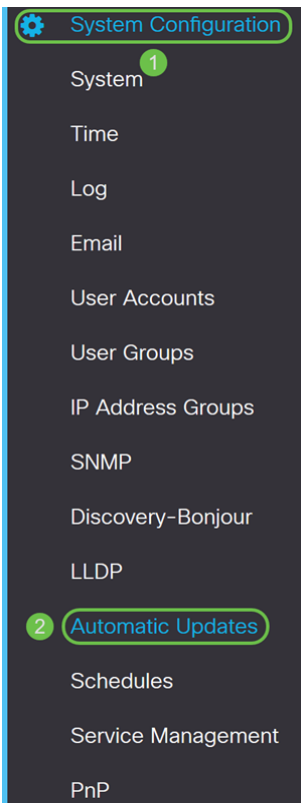




ステップ2:[File Management]ページの[Manual Upgrade]セクションまで下にスクロールします。[File Type] に[Signature File] を、[Upgrade From] に[cisco.com]を選択します。次に、[アップグレード]を押します。これにより、最新のセキュリティ署名がダウンロードされ、インストールされます。



ステップ3:IPS定義を自動的に更新するには、[システムの構成] > [自動更新]に移動します。



ステップ4:[自動更新]ページが開きます。更新を週ごとまたは月ごとに確認できます。ルータに電子メールまたはWeb UIで通知させることができます。この例では、毎週チェックを選択します。

注：セキュリティシグニチャを毎週自動的に更新することをお勧めします。

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.

ステップ5:[Automatic Update]セクションまで下にスクロールし、[Security Signature]フィールドを探します。[セキュリティ署名の更新]ドロップダウンリストで、自動更新する時刻を選択します。この例では、[Immediately]を選択します。

#### 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, ...

ステップ6:[Apply]をクリックして、実行コンフィギュレーションファイルに変更を保存します。

注：上の[フロッピーディスク]アイコンをクリックして、[構成管理]ページに移動し、実行コンフィギュレーションファイルをスタートアップコンフィギュレーションファイルにコピーしてください。これにより、リブート間の設定が維持されます。

Automatic Updates Apply Cancel

Check Every: Week Check Now

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

## 結論

これで、RV34xシリーズルータで侵入防御システム(IPS)が正しく設定されたはずですが。