

在RV34x系列路由器上配置入侵防禦系統

目標

本文檔旨在向您展示如何在RV34x系列路由器上配置入侵防禦系統(IPS)。

簡介

入侵防禦系統掃描流量以查詢要阻止的已知攻擊模式。它會監視資料包和會話在路由器中的流動，並掃描每個資料包以匹配任何Cisco IPS簽名。當檢測到可疑活動時，會將其記錄或阻止。更新IPS和防病毒資料庫和定義非常重要。可以手動或自動更新它們。

檢視思科入侵防禦系統上的以下影片：

但是，IPS可能會影響路由器的效能。一般情況下，它不會影響超文字傳輸通訊協定(HTTP)和檔案傳輸通訊協定(FTP)流量的總輸送量，但可能會略微降低最大併發連線數。

重要附註：如果路由器當前工作負荷過重，可能會使問題惡化。

下表給出了不同配置下的預期效能統計資訊。這些值應作為指導，因為實際績效可能因多種因素而不同。

| | 併發連線 | 連線速率 | HTTP吞吐量 | FTP吞吐量 |
|----------------------|--------------|-------------|----------------|----------------|
| 預設設定 | 40000 | 3000 | 982MB/秒 | 981MB/秒 |
| 啟用APP控制 | 15000-16000 | 1300 | 982MB/秒 | 981MB/秒 |
| 啟用防病毒 | 16000 | 1500 | 982MB/秒 | 981MB/秒 |
| 啟用IPS | 17000 | 1300 | 982MB/秒 | 981MB/秒 |
| 啟用App Control防病毒和IPS | 15000-16000 | 1000 | 982MB/秒 | 981MB/秒 |

以下欄位定義為：

併發連接 — 併發連線總數。例如，如果您從一個站點下載檔案，即一個連線，從Spotify流式傳輸音訊即另一個連線，從而使它成為兩個併發連線。

連線速率 — 每秒可處理的連線請求數。

HTTP/FTP吞吐量- HTTP和FTP吞吐量是下載速率 (MB/秒)。

安全許可證已更新，除了現有應用和網路過濾之外，還包含IPS保護。需要智慧帳戶才能獲得安全許可證。如果您尚未擁有活動的智慧帳戶，則需要本文檔的第1部分。

要瞭解如何在RV34x上配置防病毒，請按一下[此處](#)。

適用裝置

- RV34x

軟體版本

- 1.0.03.x

目錄

1. [智慧型授權](#)
2. [配置入侵防禦系統](#)
3. [入侵防禦系統簽名](#)
4. [入侵防禦系統簽名錶](#)
5. [IPS狀態](#)
6. [更新IPS定義](#)
7. [結論](#)

智慧型授權

如果您沒有活動的智慧帳戶，您需要繼續執行以下步驟。

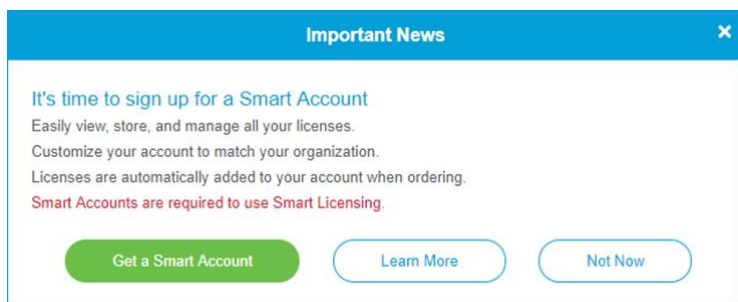
如果在配置智慧許可證帳戶時遇到任何問題或問題，我們的支援團隊將幫助解決潛在問題，並且可以通過多種方法聯絡到他們。隨時使用您首選的方法進行聯絡。

- 路由器社群：[思科小型企業支援社群](#)
- RV34x系列常見問題：[RV34x系列路由器常見問題](#)
- 智慧許可證概述：[智慧軟體授權](#)
- 智慧許可證常見問題：[面向合作夥伴、總代理商和客戶的智慧許可和智慧帳戶常見問題解答](#)
- 提交案例：[支援個案管理器](#)
- 美國/加拿大支援電話號碼：1-866-606-1866或小型企業[TAC聯絡人](#)
- 許可電子郵件：licensing@cisco.com

步驟1。如果您最近建立或訪問了Cisco.com帳戶，系統將顯示一條消息提示您建立自己的智慧許可證帳戶。如果尚未建立，可以點選此處[轉到](#)智慧許可證帳戶建立頁面。您可能需要登入

。

附註：有關請求智慧帳戶所涉及步驟的其他詳細資訊，請點選此處。



步驟2.為路由器購買智慧許可證時，供應商需要執行將唯一許可證ID移動到您的智慧許可證帳戶的流程。下表列出了購買捆綁包時需要瞭解的必要資訊。

附註：IPS和防病毒是用於Web過濾和應用程式過濾的安全許可證的一部分。

| 所需資訊 | 查詢資訊 |
|----------------|---|
| Cisco.com使用者ID | 位於您的帳戶配置檔案中，或者您可以按一下 此處 。 |
| 智慧許可證帳戶名稱 | 最好在購買許可證之前建立您的智慧帳戶。這應該是 智慧許可證帳戶建立 文章的第8步。 |
| 智慧許可證SKU | 裝置的產品標識代碼。 例如RV340-K9-NA |

附註：如果您購買了許可證，但是該許可證不會顯示在您的虛擬帳戶中，則您應該與經銷商聯絡，請求他們進行轉讓，或者聯絡我們。

為了儘可能加快該流程，您應該擁有您的許可證發票、思科銷售訂單編號和智慧帳戶許可證頁面的螢幕截圖（以便與我們的團隊分享）。

步驟3.若要產生權杖，請導航到您的[智慧軟體授權](#)帳戶。然後按一下Inventory > General頁籤。按一下New Token...按鈕。

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- | 2019-Mar-08 19:07:30 (in 8 ...) | | Allowed | Test token - rv340 | | Actions ▾ |
| MTIz- | 2019-Mar-08 17:41:45 (in 8 ...) | | Allowed | Test Token 1-2019 | | Actions ▾ |
| ZDE- | 2020-Feb-06 17:18:54 (in 34...) | 1 of 5 | Allowed | Token | | Actions ▾ |

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

Showing All 3 Records

步驟4.開啟建立註冊令牌視窗。輸入Description、Expire After和Max。使用次數。然後按下Create Token按鈕。

附註：建議在30天後使用Expire After。

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

* Expire After:

2

Days

Between 1 - 365, 30 days recommended

Max. Number of Uses:

3

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

步驟5.產生權杖後，您可以按一下最近建立的權杖右側的Token連結(藍框搭配白色箭頭)按鈕

o

Product Instance Registration Tokens

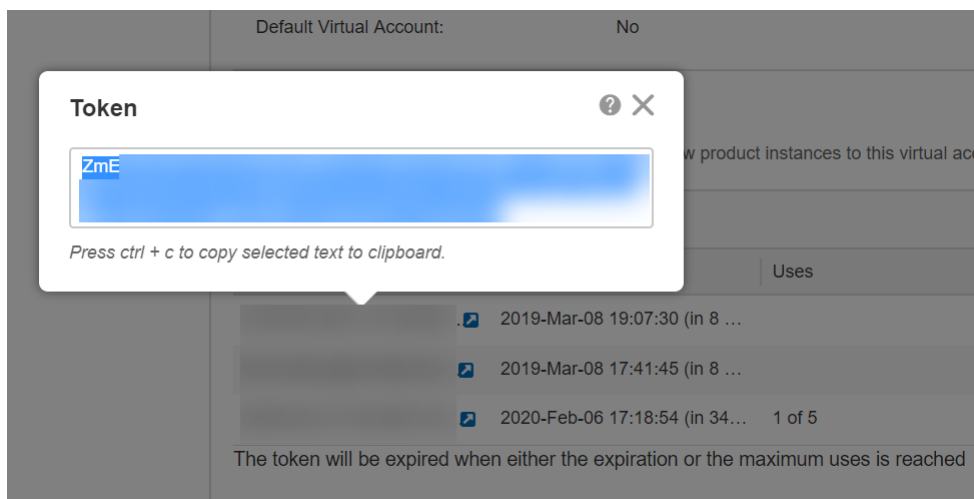
The registration tokens below can be used to register new product instances to this virtual account.

| 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

步驟6. 權杖視窗應顯示完整的權杖，以便您進行複製。突出顯示標籤，按一下右鍵該標籤並按一下**Copy**，或者可以按住鍵盤上的**ctrl**按鈕並同時按一下**c**複製文本。



步驟7. 複製權杖後，您需要登入裝置並上傳權杖金鑰。登入路由器的Web組態頁面。



Router

cisco

●●●●●●●●|

English ▼

Login

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

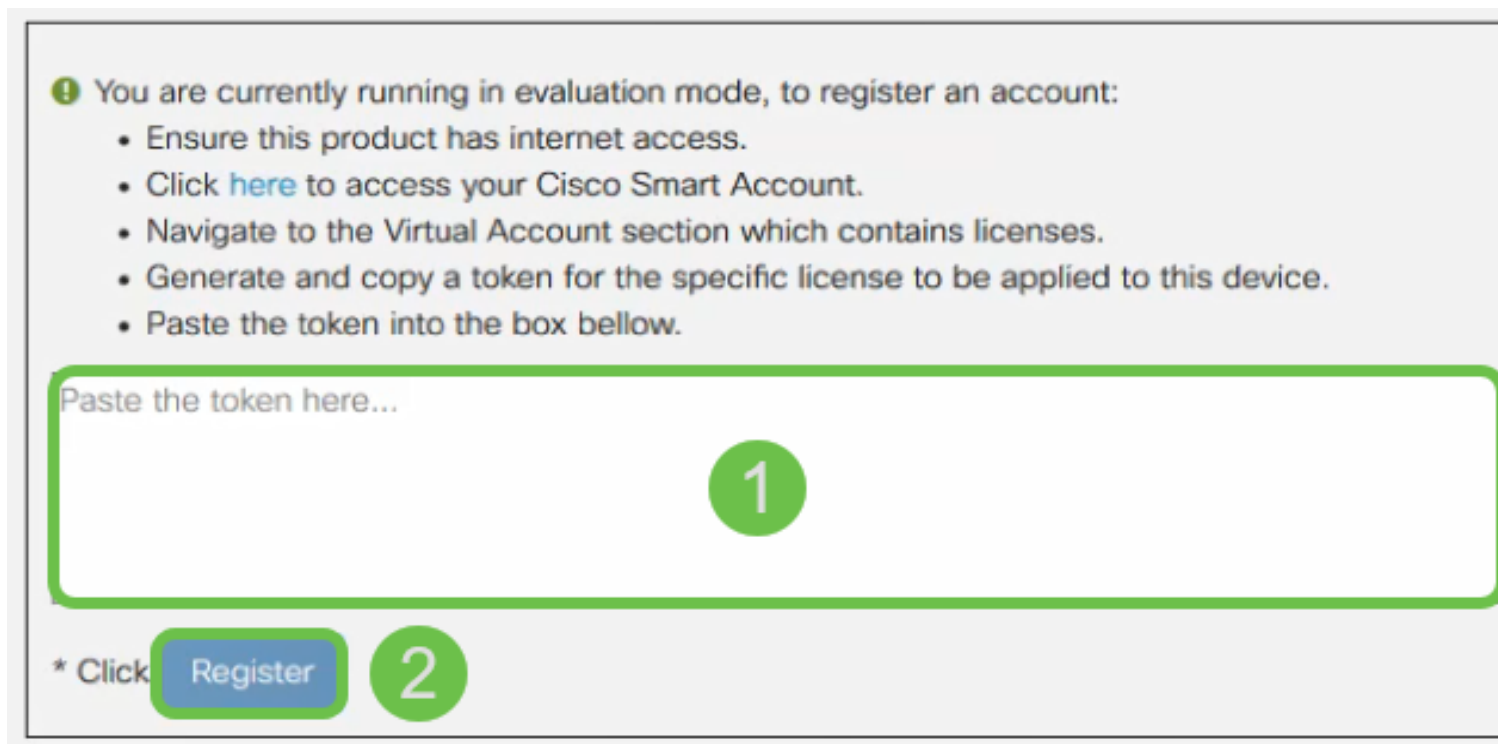
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

步驟8.導覽至License。

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

步驟9.如果您的裝置未註冊，您的許可證授權狀態將列為評估模式。貼上您從Smart Licensing Manager頁面生成的令牌(本節的第6步)。然後按一下「Register」。

附註：註冊過程可能需要一些時間，請等待其完成。



① You are currently running in evaluation mode, to register an account:

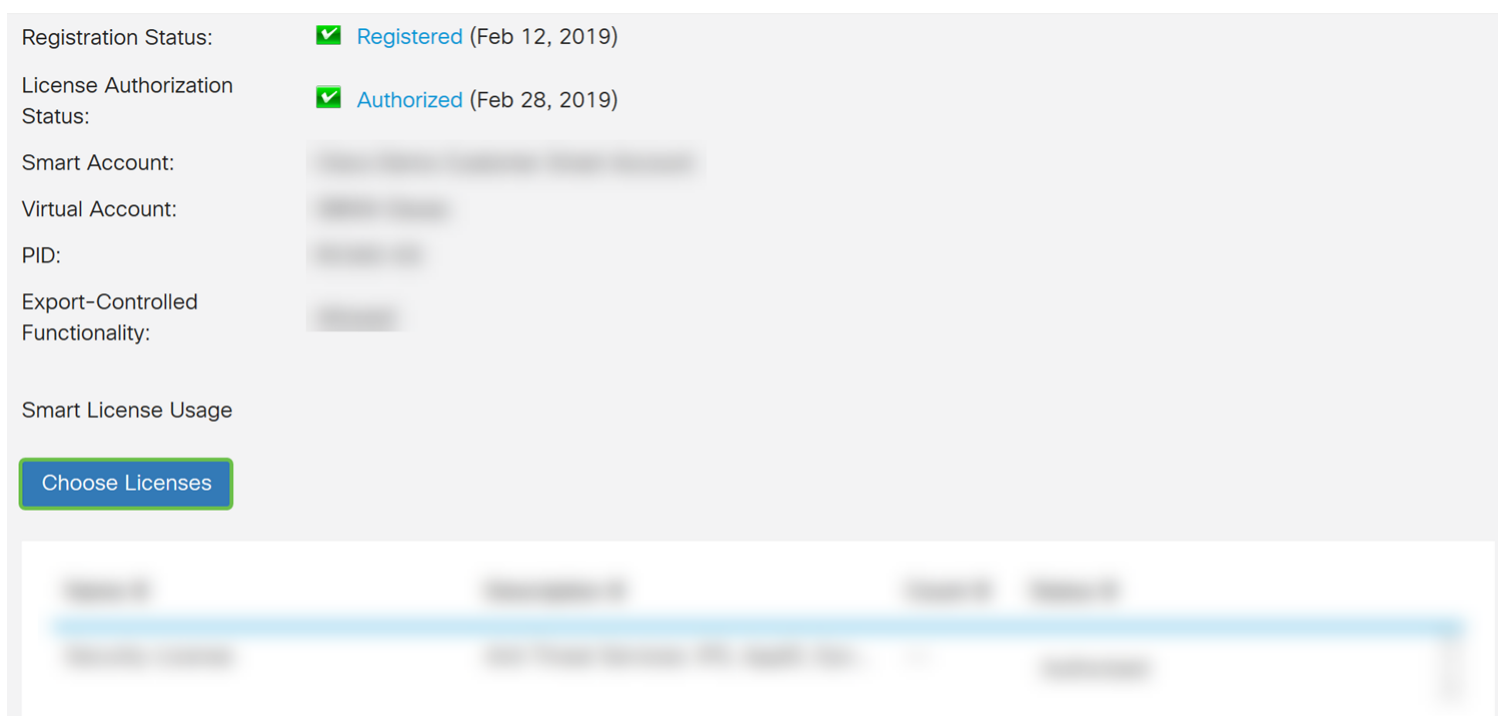
- Ensure this product has internet access.
- Click [here](#) to access your Cisco Smart Account.
- Navigate to the Virtual Account section which contains licenses.
- Generate and copy a token for the specific license to be applied to this device.
- Paste the token into the box below.

Paste the token here...

1

* Click [Register](#) 2

步驟10.註冊令牌後，您需要分配許可證。按一下Choose Licenses按鈕。



Registration Status: Registered (Feb 12, 2019)

License Authorization Status: Authorized (Feb 28, 2019)

Smart Account: [blurred]

Virtual Account: [blurred]

PID: [blurred]

Export-Controlled Functionality: [blurred]

Smart License Usage

[Choose Licenses](#)

步驟11.應該會顯示Choose Smart Licenses視窗。選中Security-License，然後按Save and Authorize。

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 ... | -- |

2

Save and Authorize Cancel

步驟12.您的 *Security-License* 的狀態現在應是 *Authorized*。

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

現在，您應該能夠繼續配置入侵防禦系統。

配置入侵防禦系統

步驟1。如果您尚未登入路由器，請登入路由器的Web組態頁面。



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.

步驟2.導覽至Security > Threat/IPS > IPS。

- 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

步驟3.選擇On以啟用入侵防禦系統功能。如果要關閉它，請選擇關閉。

在本例中，我們將選擇On。

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**

步驟4.選擇Block Attacks(Prevention)或Log Only。在本例中，我們將選擇Block Attacks(Prevention)。以下選項定義如下。

- **Block Attacks(Prevention)** — 選擇以阻止所有攻擊。它還會記錄異常。
·**僅日誌** **i**不會影響連線。

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**

步驟5.選擇要使用的IPS安全級別。以下選項定義為：

- **Connectivity** 這樣提供的保護最少：僅檢測到（高嚴重性）風險攻擊。這是最不安全的選項。
- **Balanced** 這樣可提供中等程度的保護：通過低風險特徵碼來檢查（高+中嚴重度）。這是IPS的中級安全性。
- **安全** — 安全模式將檢測正常攻擊以及嚴重和關鍵的攻擊。這樣可提供最大的保護：檢查所有規則（高+中+低嚴重性）。這是IPS的最高安全級別。

附註：您選擇的安全級別越高，所監控的攻擊越多，可能會對系統效能造成的影響就越大。

我們將為此演示選擇Balanced。

Intrusion Prevention System (IPS): On Off

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

IPS Security Level: Connectivity ⓘ
 Balanced ⓘ
 Security ⓘ

入侵防禦系統簽名

步驟6. 在上次更新欄位中，將顯示上次更新簽名的日期和時間。

Intrusion Prevention System Signatures

Last Update:

File Version: 2.4.0.0010

Search By IPS Signature ID:

步驟7. 檔案版本顯示正在使用的簽名版本。

Intrusion Prevention System Signatures

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

File Version:

Search By IPS Signature ID:

步驟8. 要搜尋特徵碼ID，請在 *Search by IPS Signature ID* 欄位中輸入 **Signature ID**，然後按一下 **Search** 以檢查是否支援該特徵碼。如果支援簽名ID，則表將使用如下所示的結果進行更新。

附註： 如果不支援該簽名ID，則表中不會顯示任何內容。

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

Search ²

IPS Signature Table

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

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

入侵防禦系統簽名錶

步驟9.在IPS簽名錶中，以下欄位定義為：

Name

- ID — 簽名的唯一識別符號。按一下ID將開啟一個視窗，供您檢視所選簽名的完整詳細資訊。

嚴重性

Category

IPS Signature Table

| Name | ID | Severity | 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

步驟10。(可選) 如果按一下IPS特徵碼表中的特徵碼ID，則會出現一個視窗，顯示所選特徵碼的完整詳細資訊。

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.


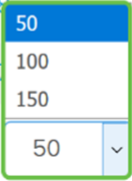
Category: attempted-recon

Severity: high

Cancel

步驟11.在IPS簽名錶的底部，選擇箭頭以及要在表中來回導航的編號。您還可以在「每頁行數」下拉選單中，選擇每頁行數(50、100或150)。

| | | | |
|------------------------------------|---------|------|-----------------|
| 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  58  50 lines per page Showing 1 - 5

步驟12.按一下Apply，將變更儲存到執行組態檔中。

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

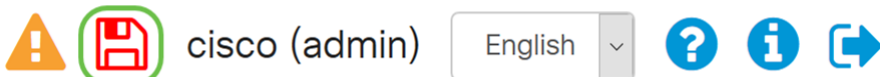
IPS Signature Table



附註：路由器使用的所有配置當前都位於運行配置檔案中，該檔案是易失性配置，在重新啟動後不會保留。為了在重新啟動之間保留您的配置，請將運行配置檔案複製到啟動配置檔案。

在接下來的幾個步驟中，我們將向您展示如何將運行配置複製到啟動配置。

步驟13.按一下頁面頂部的**Floppy Disk(Save)**圖示。這會將您重新導向至**組態管理**，以將您的執行組態儲存到啟動組態。



步驟14.在**組態管理**中，向下滾動到**複製/儲存組態**一節。請確認**Source**是**Running Configuration**，而**Destination**是**Startup Configuration**。按一下「**Apply**」。此操作會將運行配置檔案複製到啟動配置檔案中，以便在重新啟動之間保留配置。

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.

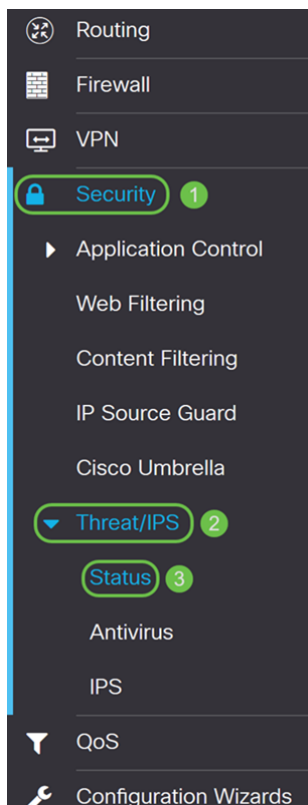
Source: 1 Running Configuration

Destination: 2 Startup Configuration

Save Icon Blinking: Enable

IPS狀態

步驟1. 導覽至 **Security > Threat/IPS > Status**。



步驟2. *Status* 頁面會在設定防威脅和IPS功能時顯示威脅和攻擊的詳細資訊。控制面板可讓您檢視整個事件摘要，以及按選擇（如天、周和月）檢測到的威脅和攻擊的詳細資訊。

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 ↻

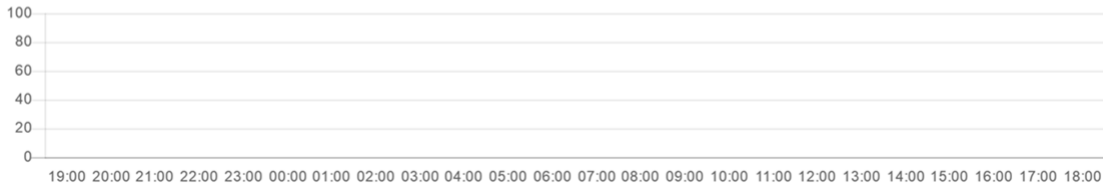
Total

Virus

IPS

Last 24 Hours ▾

Events over time



步驟3.按一下IPS頁籤。這將顯示前10個受攻擊客戶端以及前10個IPS攻擊。

Status

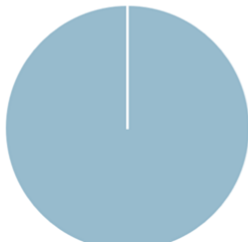
System Date & Time: 2019-Feb-28, 17:45:47 GMT
Total Since Activated: Scanned 0 Detected 0
Total Last 7 Days: Scanned 0 Detected 0
Total Last 24 Hours: Scanned 0 Detected 0
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT ↻

Total

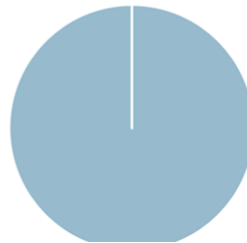
Virus

IPS

Top 10 Attacked Clients



Top 10 IPS Attacks

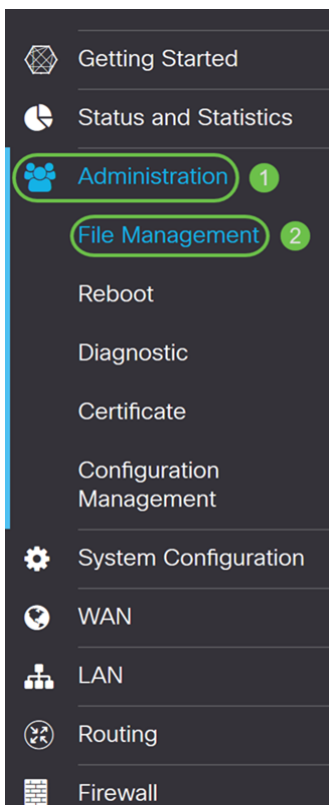


更新IPS定義

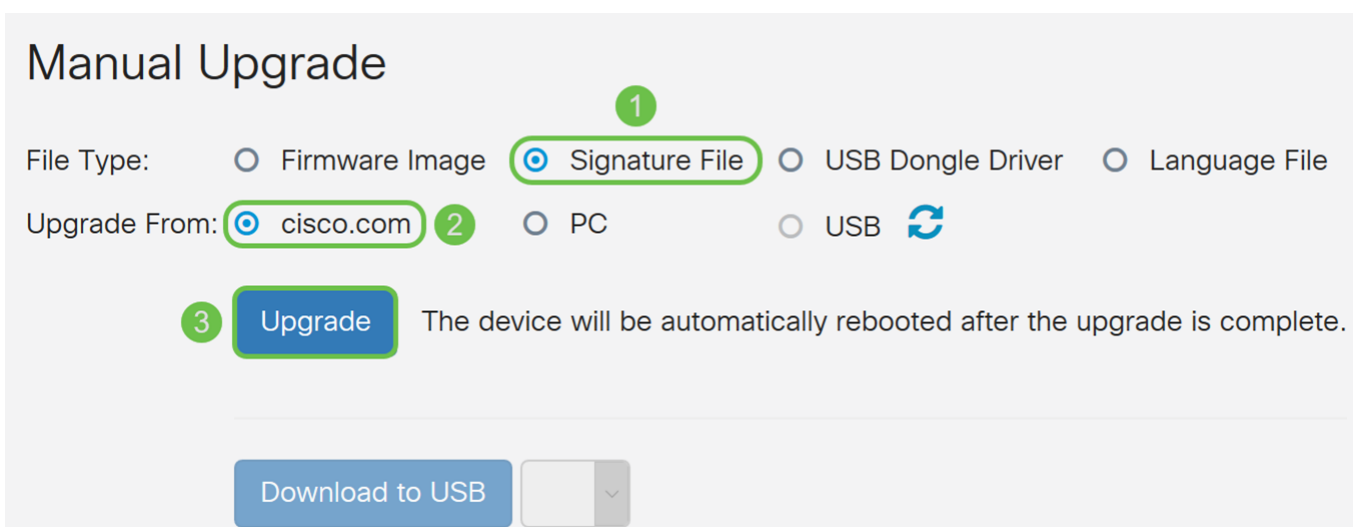
您可以手動或自動更新IPS定義。第1-2步將介紹如何手動更新IPS定義，第3-6步將介紹如何自動更新IPS定義。

最佳實踐：建議每週自動更新安全簽名。

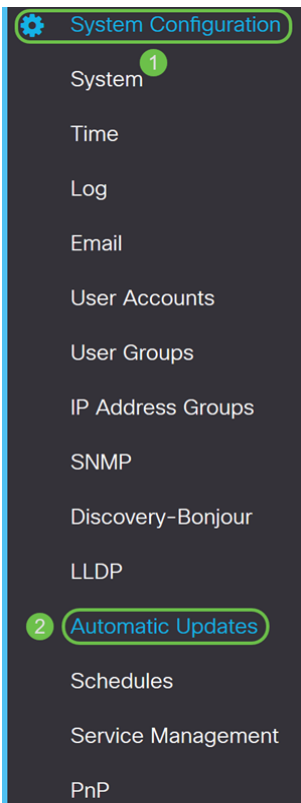
步驟1.要手動更新IPS定義，請導航到**管理>檔案管理**。



步驟2. 向下滾動到 *File Management* 頁面的 *Manual Upgrade* 部分。為 *File Type* 選擇 **Signature File**，為 *Upgrade From* 選擇 **cisco.com**。然後按升級。這將下載並安裝最新的安全簽名。



步驟3. 要自動更新IPS定義，請導航至系統配置>自動更新。



步驟4. *Automatic Updates* 頁面隨即開啟。您可以選擇每週或每月檢查更新。您可以通過電子郵件或Web UI通知路由器。在此示例中，我們將選擇每週進行檢查。

附註：建議每週自動更新安全簽名。

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.

步驟5. 向下滾動到 *Automatic Update* 部分，並查詢 *Security Signature* 欄位。在「*Security Signature Update*」下拉選單中，選擇要自動更新的時間。在本例中，我們將選擇 **Immediate**。

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, ... |

步驟6. 按一下 **Apply**，將變更儲存到執行組態檔中。

附註：請記得按一下頂部的 **Floppy Disk** 圖示，導航到 *Configuration Management* 頁面，將運行配置檔案複製到啟動配置檔案。這將有助於在重新啟動後保留您的配置。

Automatic Updates

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, ... |

結論

現在，您應該已經在RV34x系列路由器上成功配置了入侵防禦系統。