

Configurazione del sistema di prevenzione delle intrusioni sul router serie RV34x

Obiettivo

Lo scopo di questo documento è quello di mostrare come configurare il sistema di prevenzione delle intrusioni (IPS) sui router serie RV34x.

Introduzione

Il Sistema di Prevenzione delle Intrusioni analizza il traffico per cercare modelli di attacco noti da bloccare. Controlla i pacchetti e le sessioni mentre passano attraverso il router e analizza ciascun pacchetto in modo che corrisponda a una delle firme Cisco IPS. Quando rileva attività sospette, è progettato per registrarle o bloccarle. È importante aggiornare i database e le definizioni IPS e Antivirus. Queste impostazioni possono essere aggiornate manualmente o automaticamente.

Guarda questi video su Cisco Intrusion Prevention System:

Tuttavia, l'IPS può influire sulle prestazioni del router. In generale, non influisce sul throughput totale per il traffico HTTP (Hypertext Transfer Protocol) e FTP (File Transfer Protocol), ma può ridurre in modo significativo il numero massimo di connessioni simultanee.

Nota importante: Se il router è attualmente sottoposto a un carico di lavoro pesante, il problema potrebbe essere aggravato.

La tabella seguente fornisce le statistiche previste per le prestazioni nelle varie configurazioni. Questi valori devono essere utilizzati come guida, in quanto le prestazioni reali possono variare a causa di una serie di fattori.

	Connessioni simultanee	Velocità di connessione	Throughput HTTP	Throughput FTP
Impostazioni predefinite	40000	3000	982 MB/sec	981 MB/sec
Abilita controllo APP	15000-16000	1300	982 MB/sec	981 MB/sec
Abilita antivirus	16000	1500	982 MB/sec	981 MB/sec
Abilita IPS	17000	1300	982 MB/sec	981 MB/sec
Abilita Antivirus e IPS di App Control	15000-16000	1000	982 MB/sec	981 MB/sec

I campi seguenti sono definiti come:

Connessioni simultanee: il numero totale di connessioni simultanee. Ad esempio, se state scaricando un file da un sito, si tratta di una connessione, lo streaming audio da Spotify sarà un'altra connessione, rendendola due connessioni simultanee.

Velocità di connessione: numero di richieste di connessione al secondo che è possibile elaborare.

Throughput HTTP/FTP: il throughput HTTP e FTP corrisponde alla velocità di download in MB/sec.

Le licenze di sicurezza sono state aggiornate per includere la protezione IPS oltre alle applicazioni e ai filtri Web esistenti. Per ottenere una licenza di protezione, è necessario uno smart account. Se non si dispone di uno smart account attivo, sarà necessaria la sezione 1 di questo documento.

per informazioni su come configurare Antivirus su RV34x, fare clic [qui](#).

Dispositivi interessati

- RV34x

Versione del software

- 1.0.03.x

Sommario

1. [Licenze Smart](#)
2. [Configurazione del sistema di prevenzione delle intrusioni](#)
3. [Firme del sistema di prevenzione delle intrusioni](#)
4. [Tabella delle firme del sistema di prevenzione delle intrusioni](#)
5. [Stato IPS](#)
6. [Aggiornamento delle definizioni IPS](#)
7. [Conclusioni](#)

Licenze Smart

Se non si dispone di uno smart account attivo, è necessario procedere come segue.

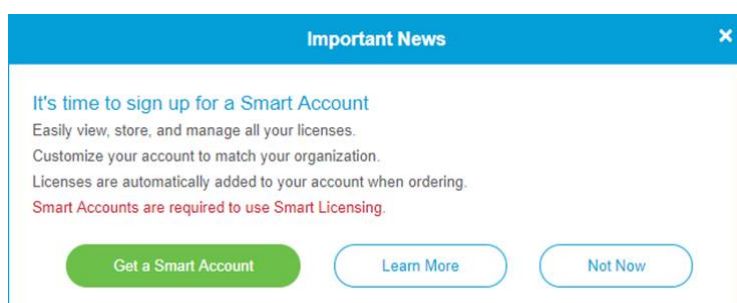
In caso di problemi durante la configurazione dell'account Smart License, il team di supporto Dell è in grado di individuare potenziali problemi e di raggiungere l'utente con diversi metodi.

Sentitevi liberi di utilizzare il vostro metodo preferito per raggiungere fuori.

- **Community router:** [Community di supporto Cisco Small Business](#)
- **Domande frequenti sulla serie RV34x:** [Serie RV34x Router: domande frequenti](#)
- **Panoramica delle licenze Smart:** [Licenze software Smart](#)
- **Domande frequenti sulle licenze Smart:** [Domande frequenti su Smart Licensing e Smart Account per partner, distributori e clienti](#)
- **Invia una richiesta:** [Support Case Manager](#)
- **Numero di telefono dell'assistenza USA/Canada:** 1-866-606-1866 o [Contatti TAC per piccole imprese](#)
- **E-mail sulle licenze:** licensing@cisco.com

Passaggio 1. Se l'account Cisco.com è stato creato o visitato di recente, viene visualizzato un messaggio per creare un account Smart License personalizzato. In caso contrario, fare clic [qui](#) per accedere alla pagina di creazione dell'account Smart License. Potrebbe essere necessario eseguire l'accesso.

Nota: Per ulteriori informazioni sui passaggi da seguire per richiedere lo Smart Account, fare clic [qui](#).



Passaggio 2. Quando si acquista una licenza smart per un router, il fornitore deve eseguire un processo che sposta l'ID licenza univoco nell'account Smart License. Di seguito è riportata una tabella con le informazioni necessarie da richiedere al momento dell'acquisto dei pacchetti.

Nota: IPS e Antivirus fanno parte della licenza di protezione utilizzata per Filtro Web e Filtro applicazioni.

Informazioni richieste	Individuazione delle informazioni
Cisco.com ID utente	Si trova nel profilo dell'account o puoi fare clic qui .
Nome dello Smart License Account	E meglio aver creato lo smart account prima di acquistare la licenza. Questa operazione deve essere effettuata al punto 8 dell'articolo sulla creazione dello Smart

	License Account.
SKU Smart License	Codice di identificazione del prodotto per il dispositivo. Es. RV340-K9-NA

Nota: Se la licenza è stata acquistata e non è visualizzata nell'account virtuale, è necessario contattare il rivenditore per richiedere il trasferimento o contattarci.

Per rendere il processo il più rapido possibile, è necessario disporre della fattura di licenza, del numero dell'ordine di vendita Cisco e di uno screenshot della pagina della licenza dello Smart Account (da condividere con il team).

Passaggio 3. Per generare un token, passare all'account della [licenza Smart Software](#). Quindi fare clic su **Inventario > scheda Generale**. Fare clic sul pulsante **New Token...**

Smart Software Licensing

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

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

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

Passaggio 4. Viene visualizzata la finestra *Crea token di registrazione*. Immettere una *descrizione*, *Scadenza dopo* e *Max. Numero di utilizzi*. Quindi premi il pulsante **Create Token**.

Nota: Si consiglia 30 giorni per *Scadenza dopo*.

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

Passaggio 5. Una volta generato il token, è possibile fare clic sul **collegamento Token** (casella blu con freccia bianca) a destra del token creato di recente.

Product Instance Registration Tokens

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

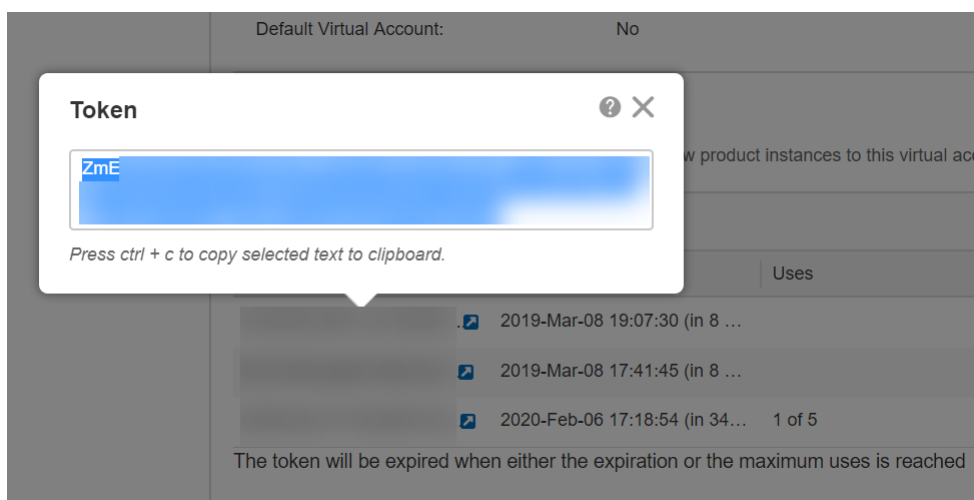
New Token...

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

Passaggio 6. Dovrebbe essere visualizzata una finestra *Token* con il token completo da copiare. Evidenziare il token, fare clic con il pulsante destro del mouse sul token e scegliere **Copia** oppure tenere premuto il pulsante **ctrl** sulla tastiera e fare clic **c** contemporaneamente per copiare il testo.



Passaggio 7. Dopo aver copiato il token, sarà necessario accedere al dispositivo e caricare la chiave del token. Accedere alla pagina di configurazione Web del router.



Router

cisco

●●●●●●●●|

English ▼

Login

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

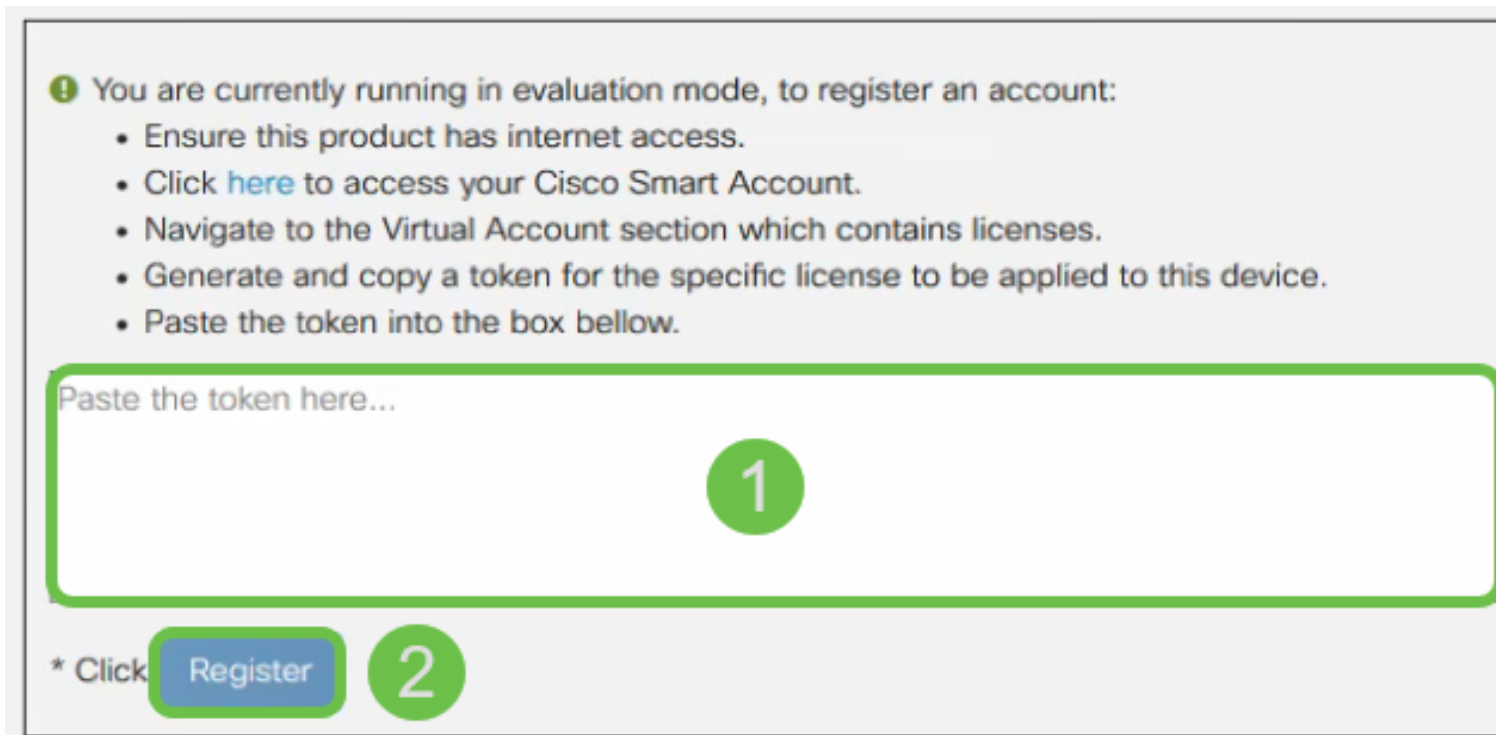
Cisco, the Cisco logo, and Cisco Systems are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

Passaggio 8. Passare a Licenza.

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

Passaggio 9. Se la registrazione del dispositivo viene annullata, *lo stato di autorizzazione della licenza* verrà elencato come *modalità di valutazione*. Incollare il token ([passo 6 di questa sezione](#)) generato dalla pagina *Smart Licensing Manager*. Quindi fare clic su **Register** (Registra).

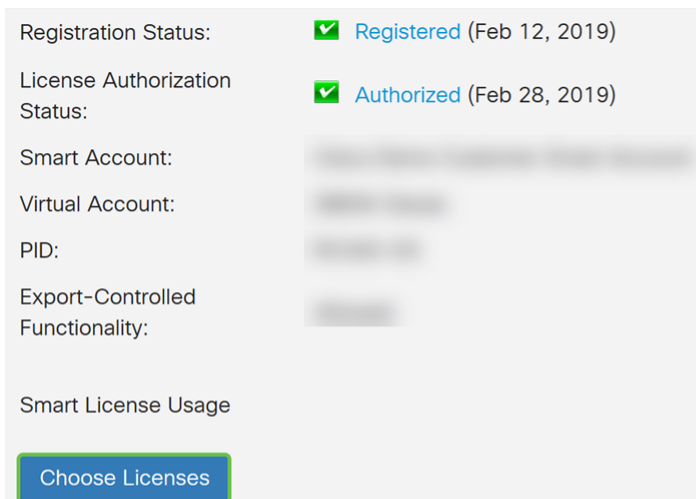
Nota: Il processo di registrazione potrebbe richiedere del tempo. Attendere il completamento.



The screenshot shows a registration interface with the following elements:

- An information icon (i) followed by the text: "You are currently running in evaluation mode, to register an account:"
- 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.
 - Paste the token into the box below.
- 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 field.
- A blue button labeled "Register" with a green circle and the number "2" to its right.
- The text "* Click" is positioned to the left of the "Register" button.

Passaggio 10. Dopo aver registrato il token, sarà necessario allocare la licenza. Fare clic sul pulsante **Scegli licenze**.



The screenshot shows the registration status page with the following information:

- 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
- A blue button labeled "Choose Licenses" is highlighted with a green border.

Passaggio 11. Viene visualizzata la finestra *Scegli licenze Smart*. Controllare la **Security-License**, quindi premere **Save and Authorize** (Salva e autorizzazione).

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

Passaggio 12. Lo *stato* della licenza di protezione deve essere *autorizzato* ora.

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

A questo punto dovrebbe essere possibile procedere con la configurazione del sistema di prevenzione delle intrusioni.

Configurazione del sistema di prevenzione delle intrusioni

Passaggio 1. Se non è stato ancora eseguito il login al router, accedere alla pagina di configurazione Web del router.



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.

Passaggio 2. Passare a **Sicurezza > Minaccia/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

Passaggio 3. Selezionare **On** per abilitare la funzione Intrusion Prevention System. Per disattivarlo, selezionare **Disattivato**.

In questo esempio verrà selezionato **Attivo**.

IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS): On Off

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

IPS Security Level: Connectivity ⓘ
 Balanced ⓘ
 Security ⓘ

Passaggio 4. Selezionare **Blocca attacchi (Prevenzione)** o **Registra solo**. In questo esempio, selezioneremo **Blocca attacchi (Prevenzione)**. Le opzioni seguenti sono definite di seguito.

- **Blocca attacchi (prevenzione)**: selezionare questa opzione per bloccare tutti gli attacchi. Registra anche l'anomalia.
- **Solo registro** - Questa opzione genera il registro solo (con informazioni sul client, ID firma, ecc.) quando vengono identificate le anomalie. Non influisce sulla connessione.

IPS (Intrusion Prevention System)

Intrusion Prevention System (IPS): On Off

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

IPS Security Level: Connectivity ⓘ
 Balanced ⓘ
 Security ⓘ

Passaggio 5. Selezionare il livello di protezione IPS che si desidera utilizzare. Le opzioni seguenti sono definite come:

- **Connettività** - Questa modalità rileva gli attacchi più critici. Ciò garantisce la protezione minima: vengono rilevati solo attacchi a rischio (alta gravità). Questa è l'opzione meno sicura.
- **Bilanciato** - La modalità selezionata rileva gli attacchi gravi insieme agli attacchi critici. Ciò fornisce una protezione media: (alta + media gravità) sono ispezionati, passando firme a basso rischio. Si tratta della protezione di livello intermedio per IPS.
- **Sicurezza**: la modalità di sicurezza rileva gli attacchi normali e quelli gravi e critici. Ciò

garantisce la massima protezione: Tutte le regole (alta + media + bassa severità) sono ispezionate. Questo è il livello di protezione più alto per IPS.

Nota: Maggiore è il livello di protezione scelto, maggiore è il numero di attacchi monitorati, maggiore sarà l'impatto sulle prestazioni del sistema.

Per questa dimostrazione verrà selezionato **Bilanciato**.

Intrusion Prevention System (IPS): On Off

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

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

Firme del sistema di prevenzione delle intrusioni

Passaggio 6. Nel campo *Ultimo aggiornamento* viene visualizzata la data e l'ora dell'ultima firma aggiornata.

Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID:

Passaggio 7. Nella casella *Versione file* viene visualizzata la versione della firma in uso.

Intrusion Prevention System Signatures

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

File Version: 2.4.0.0010

Search By IPS Signature ID:

Passaggio 8. Per cercare un ID firma, immettere il **Signature ID** nel campo *Cerca per Signature ID IPS* e fare clic su **Cerca** per verificare se la firma è supportata o meno. Se l'ID firma è supportato, la tabella verrà aggiornata con il risultato illustrato di seguito.

Nota: Se l'ID della firma non è supportato, nella tabella non verrà visualizzato nulla.

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
3 TROJAN Keylogger connection	8005394	high	successful-recon-limited

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

Tabella delle firme del sistema di prevenzione delle intrusioni

Passaggio 9. Nella *tabella Firma IPS* sono definiti i campi seguenti:

- **Nome** - Nome della firma.
- **ID**: identificatore univoco della firma. Facendo clic sull'ID verrà visualizzata una finestra che consente di visualizzare i dettagli completi della firma selezionata.
- **Gravità**: η ληπελλο δι γραπιτὸ ινδιχα λειμαπαττο συλλα σιχυρεζζα.
- **Category** - Χατεγορια α χυι απαρτιενε λα φηρμα.

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

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

Passaggio 10. (Facoltativo) Se si è fatto clic sull'ID della firma nella *tabella delle firme IPS*, verrà visualizzata una finestra che mostra i dettagli completi della firma selezionata.

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

Passaggio 11. Nella parte inferiore della *tabella delle firme IPS*, selezionare le frecce e i numeri per spostarsi avanti e indietro nella tabella. È inoltre possibile selezionare la quantità di righe (50, 100 o 150) per pagina nell'elenco a discesa *Righe per pagina*.

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

50 lines per page

Showing 1 - 5

Passaggio 12. Fare clic su **Apply** (Applica) per salvare le modifiche nel file di configurazione in esecuzione.

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

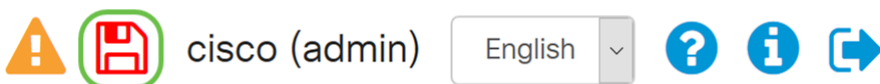
IPS Signature Table



Nota: Tutte le configurazioni utilizzate dal router sono attualmente incluse nel file di configurazione in esecuzione, che è volatile e non viene conservato tra un riavvio e l'altro. Per conservare la configurazione tra un riavvio e l'altro, copiare il file della configurazione in esecuzione nel file della configurazione di avvio.

Nei passaggi successivi verrà illustrato come copiare la configurazione in esecuzione nella configurazione di avvio.

Passaggio 13. Fare clic sull'icona **Disco floppy (Salva)** nella parte superiore della pagina. In questo modo, si verrà reindirizzati alla *Gestione configurazione* per salvare la configurazione in esecuzione nella configurazione di avvio.



Passaggio 14. In *Gestione configurazione*, scorrere verso il basso fino alla sezione *Copia/Salva configurazione*. Verificare che l'*origine* stia **eseguendo la configurazione** e che la *destinazione* sia la **configurazione di avvio**. Fare clic su **Apply** (Applica). Il file della configurazione in esecuzione verrà copiato nel file della configurazione di avvio per conservare la configurazione tra un riavvio e l'altro.

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.

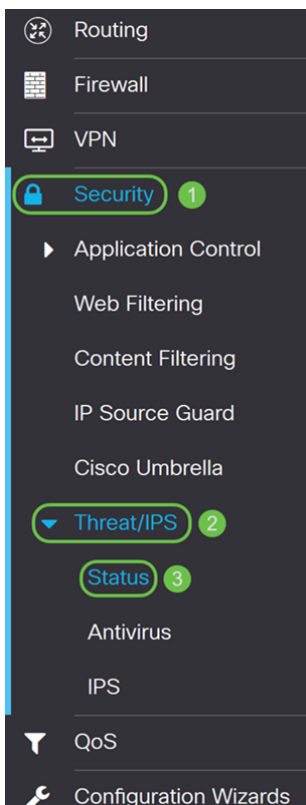
Source: 1 Running Configuration

Destination: 2 Startup Configuration

Save Icon Blinking: Enable

Stato IPS

Passaggio 1. Passare a **Sicurezza > Minaccia/IPS > Stato**.



Passaggio 2. La pagina *Status* (Stato) visualizza i dettagli delle minacce e degli attacchi quando vengono configurate le funzionalità Anti Threat e IPS. Il dashboard offre una visualizzazione del riepilogo completo degli eventi e informazioni dettagliate sulle minacce e gli attacchi rilevati in base alla selezione, ad esempio giorno, settimana e mese.

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 ↻

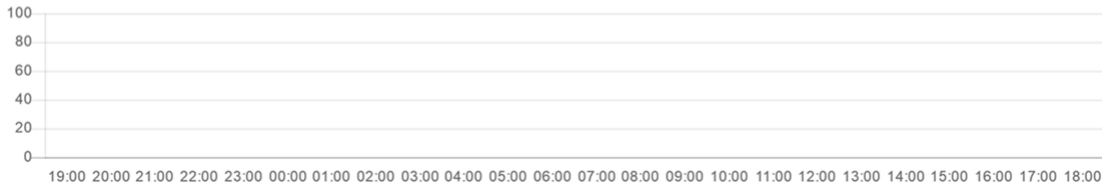
Total

Virus

IPS

Last 24 Hours ▾

Events over time



Passaggio 3. Fare clic sulla scheda **IPS**. Verranno visualizzati i primi 10 client attaccati e i primi 10 attacchi IPS.

Status

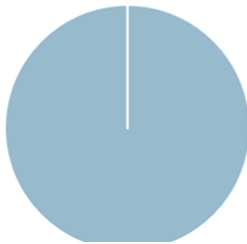
System Date & Time: 2019-Feb-28, 17:45:47 GMT
Total Since Activated: Scanned 0 Detected 0
Total Last 7 Days: Scanned 0 Detected 0
Total Last 24 Hours: Scanned 0 Detected 0
Virus/IPS status since: 2019-Feb-26, 19:04:33 GMT ↻

Total

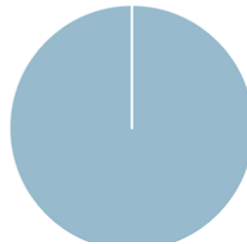
Virus

IPS

Top 10 Attacked Clients



Top 10 IPS Attacks

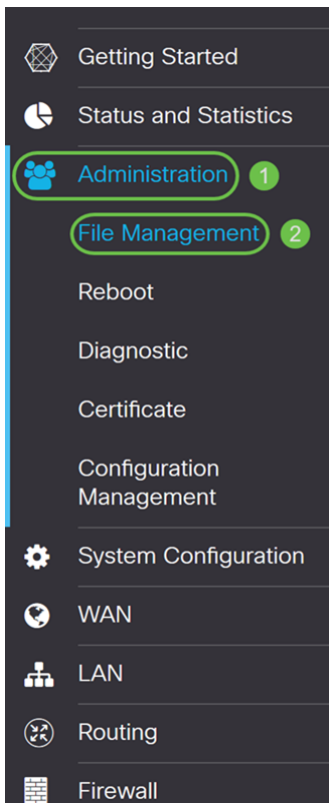


Aggiornamento delle definizioni IPS

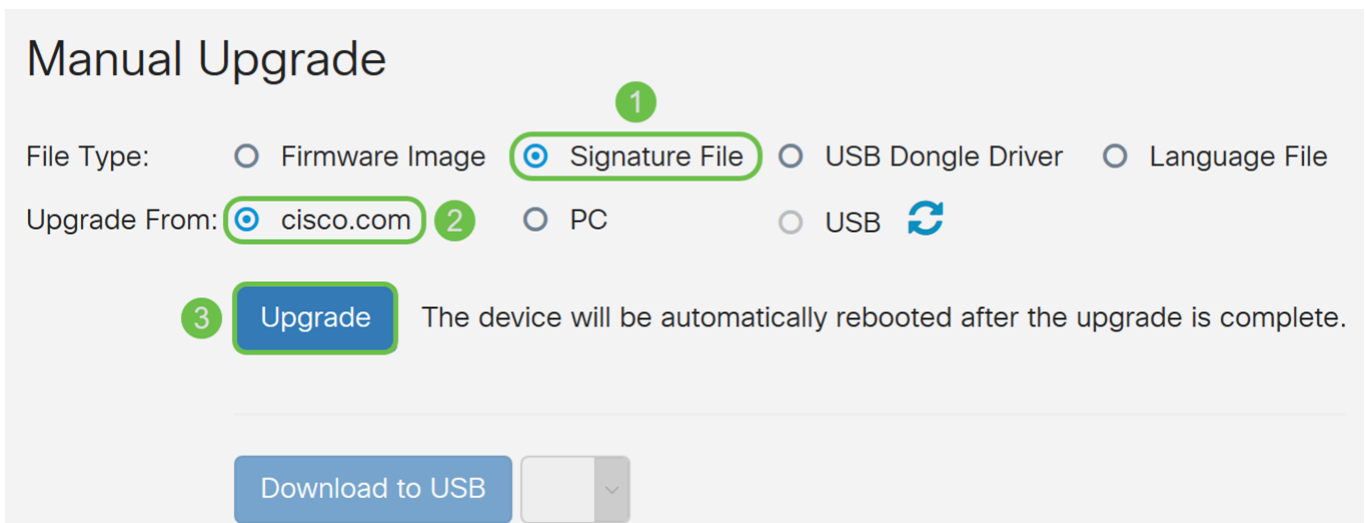
È possibile aggiornare la definizione IPS manualmente o automaticamente. Le fasi 1-2 mostrano come aggiornare la definizione IPS manualmente, mentre le fasi 3-6 mostrano come aggiornare la definizione IPS automaticamente.

Procedure ottimali: Si consiglia di aggiornare automaticamente le firme di protezione ogni settimana.

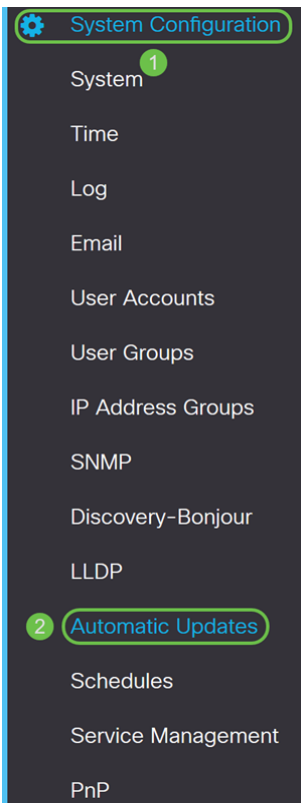
Passaggio 1. Per aggiornare manualmente le definizioni IPS, passare ad **Amministrazione > Gestione file**.



Passaggio 2. Scorrere fino alla sezione *Aggiornamento manuale* della pagina *Gestione file*. Selezionare **Signature File** per *File Type* (Tipo file) e **cisco.com** per *Upgrade da* (*Aggiorna da*). Quindi premere **Aggiorna**. Verrà scaricata la firma di protezione più recente e installata.



Passaggio 3. Per aggiornare automaticamente le definizioni IPS, selezionare **Configurazione di sistema > Aggiornamenti automatici**.



Passaggio 4. Viene visualizzata la pagina *Aggiornamenti automatici*. È possibile verificare la disponibilità di aggiornamenti su base settimanale o mensile. È possibile impostare la notifica del router tramite posta elettronica o interfaccia utente Web. In questo esempio verrà selezionato un controllo ogni settimana.

Nota: Si consiglia di aggiornare automaticamente le firme di protezione ogni settimana.

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.

Passaggio 5. Scorrere verso il basso fino alla sezione *Aggiornamento automatico* e cercare il campo *Firma di sicurezza*. Nell'elenco a discesa *Aggiornamento firma di sicurezza*, selezionare l'ora che si desidera aggiornare automaticamente. In questo esempio, la selezione verrà eseguita **immediatamente**.

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, ...

Passaggio 6. Fare clic su **Apply** (Applica) per salvare le modifiche nel file di configurazione in esecuzione.

Nota: Ricordarsi di fare clic sull'icona **Disco floppy** nella parte superiore per accedere alla pagina *Gestione configurazione* e copiare il file di configurazione in esecuzione nel file della configurazione di avvio. In questo modo, le configurazioni verranno mantenute tra un riavvio e l'altro.

Automatic Updates Apply

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, ...

Conclusioni

A questo punto, è necessario configurare correttamente il sistema di prevenzione delle intrusioni sul router serie RV34x.