

Configurazione del controllo dell'applicazione sul router serie RV34x

Obiettivo

Application Control è una funzione di sicurezza aggiuntiva sul router che può migliorare una rete già protetta, promuovere la produttività sul posto di lavoro e massimizzare la larghezza di banda. Il controllo dell'applicazione può essere utile per smartphone e altre applicazioni basate su browser. Se si collega un punto di accesso wireless (WAP) a un router, quest'ultimo sarà in grado di autorizzare o bloccare il traffico verso qualsiasi host connesso al WAP. In questo modo gli utenti non possono accedere ad alcune applicazioni.

Lo scopo di questo articolo è quello di mostrare come configurare il controllo dell'applicazione sui router serie RV34x usando la procedura guidata di controllo dell'applicazione e la configurazione manuale.

Dispositivi interessati

- Serie RV34x

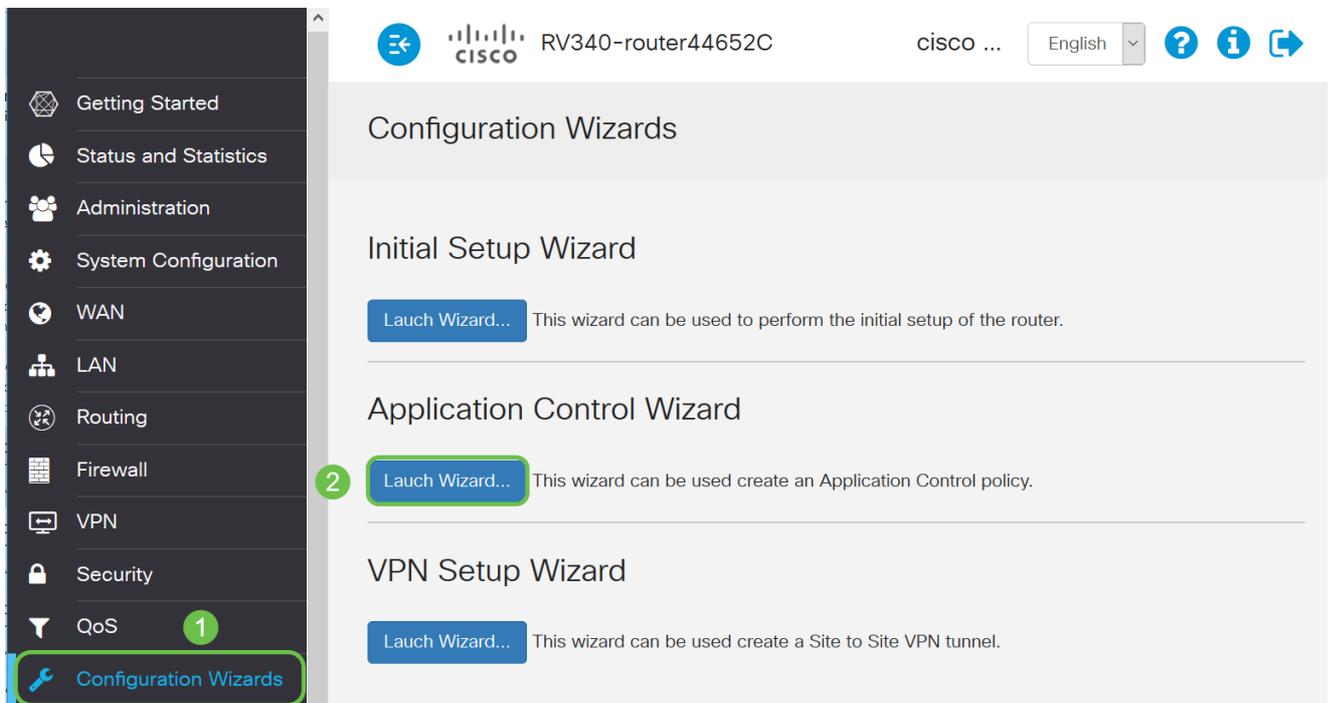
Versione del software

- 1.0.02.16

Configura controllo applicazione

[Tramite la Creazione guidata controllo applicazione](#)

Passaggio 1. Accedere all'utility basata sul Web e scegliere **Configurazione guidata > Avvia procedura guidata....**



Passaggio 2. Fare clic sul pulsante di opzione **On** per abilitare *Application Controller*. Questa funzione è disabilitata per impostazione predefinita.

Application Control Wizard

1. Policy Name

2. Application Name

Application Controller: On Off

Enter a name for this policy:

Passaggio 3. Creare un nome univoco per il criterio nel campo *Nome criterio*. Il nome non può contenere spazi o caratteri speciali.

Nota: Per questo esempio viene utilizzato *MobileControl*.

Application Control Wizard

1. Policy Name

2. Application Name

Application Controller: On Off

Enter a name for this policy:

Passaggio 4. Fare clic su **Avanti**.

Passaggio 5. Fare clic sul pulsante **Modifica** per definire i parametri e le categorie che

verranno utilizzati dal controllo applicazione per filtrare i dati.

The screenshot shows a configuration interface with a sidebar on the left containing four steps: '1. Policy Name' (checked), '2. Application Name' (highlighted in blue), '3. Schedule', and '4. Summary'. The main area is titled 'Application List Table' and contains a table with columns for 'Category', 'Application', and 'Behavior'. Above the table, there is a text input field with the placeholder 'Enter the application names to be blocked:' and an 'Edit' button.

Passaggio 6. Fare clic sul segno + accanto a qualsiasi categoria per espandere e visualizzare le sottocategorie e le applicazioni specifiche. In alternativa, per visualizzare tutte le categorie e le relative sottocategorie, fare clic su **Espandi** nella parte inferiore della pagina.

Nota: In questo esempio, la categoria *Risorse IT* è espansa.

This screenshot shows the same configuration interface as above, but with the 'IT Resources' category expanded. The expanded list includes: 'Streaming Media', 'Shareware and Freeware', 'File Hosting / Storage', 'Web based email', and 'Internet Communications'. Each item has a checkbox and a dropdown menu. The 'IT Resources' category is marked with a minus sign, while the others have plus signs. A green rounded rectangle highlights the expanded list.

Passaggio 7. Selezionare la casella di controllo delle categorie e sottocategorie che si desidera applicare al criterio.

Nota: Per questo esempio, *Streaming Media* e *Comunicazioni Internet* sono le sottocategorie in Risorse IT utilizzate come esempi.

✓ 1. Policy Name

2. Application Name

3. Schedule

4. Summary

+ Adult/Mature Content

+ Business/Investment

+ Entertainment

+ Illegal/Questionable

- IT Resources

+ Streaming Media

+ Shareware and Freeware

+ File Hosting / Storage

+ Web based email

+ Internet Communications

Passaggio 8. (Facoltativo) Fare clic sull'elenco a discesa accanto all'applicazione che si desidera applicare al criterio. Se necessario, ripetere questo passaggio. Le opzioni sono:

- Permit & Log: il flusso e la registrazione dei dati è consentito.
- Permit: i dati sono consentiti.
- Blocco: i dati sono bloccati.
- Blocco e registro: i dati vengono bloccati e registrati.

Nota: Verificare che la registrazione sia abilitata sul router scegliendo **Configurazione di sistema > Registro**. Selezionare la casella di controllo **Abilita** e quindi fare clic su **Applica**.

✓ 1. Policy Name

2. Application Name

3. Schedule

4. Summary

+ Adult/Mature Content

+ Business/Investment

+ Entertainment

+ Illegal/Questionable

- IT Resources

+ Streaming Media

Permit & Log
Permit
Block
Block & Log

Shareware and Freeware

File Hosting / Storage

Nota: Nell'esempio, *Block* viene utilizzato per lo streaming multimediale.

Passaggio 9. Fare clic su **Applica**. Verrà eseguito il reindirizzamento alla seconda pagina della configurazione guidata.

1. Policy Name

2. Application Name

3. Schedule

4. Summary

- + Entertainment
- + Illegal/Questionable
- IT Resources
 - + Streaming Media
 - Block
 - + Shareware and Freeware
 -
 - + File Hosting / Storage
 -
 - + Web based email
 -
 - + Internet Communications
 - Block
- + Lifestyle/Culture
- + Other
- + Security

Apply Cancel

Nota: Nella tabella Elenco applicazioni vengono inserite le categorie e le applicazioni selezionate.

✓ 1. Policy Name

Enter the application names to be blocked: [Edit](#)

2. Application Name

Application List Table

3. Schedule

4. Summary

Category	Application	Behavior
Streamin...	Musical.ly	DataFlow
Streamin...	Plex	DataFlow
Streamin...	Apple iTun...	DataFlow
Internet C...	AIM	Login
Internet C...	Gadu-Gadu	DataFlow
Internet C...	Facetime	DataFlow
Internet C...	FreePP	Message

Back

Next

Cancel

Passaggio 10. Fare clic su **Avanti** per passare alla pagina Pianificazione.

✓ 1. Policy Name

Enter the application names to be blocked: [Edit](#)

2. Application Name

Application List Table

3. Schedule

4. Summary

Category	Application	Behavior
Streamin...	Musical.ly	DataFlow
Streamin...	Plex	DataFlow
Streamin...	Apple iTun...	DataFlow
Internet C...	AIM	Login
Internet C...	Gadu-Gadu	DataFlow
Internet C...	Facetime	DataFlow
Internet C...	FreePP	Message

Back

Next

Cancel

Passaggio 11. Dall'elenco a discesa Programmazione, scegliere una programmazione per la quale impostare il criterio. Le opzioni possono variare a seconda delle pianificazioni definite in precedenza. Per configurare una pianificazione, selezionare **Configurazione di sistema >**

Pianificazioni. Fare clic su **Next** (Avanti).

Select the schedule to block the application:

- 1. Policy Name
- 2. Application Name
- 3. Schedule
- 4. Summary

Always On

Always On

ANYTIME

BUSINESS

EVENINGHOURS

WORKHOURS

Back Next Cancel

Nota: Per questo esempio viene utilizzato *Always On*.

Passaggio 12. Verrà visualizzata la pagina Riepilogo. Nella tabella Criteri di controllo delle applicazioni sono ora inseriti i criteri configurati. Nella pagina di riepilogo, rivedere le impostazioni e fare clic su **Invia**. È possibile fare clic su **Indietro** per modificare le impostazioni.

Policy: MobileControl

Application List Table

Category	Application	Behavior
Streamin...	56.com	DataFlow
Streamin...	Amazon In...	DataFlow
Streamin...	Baidu Video	DataFlow
Streamin...	Baofeng Vi...	DataFlow
Streamin...	Bild	DataFlow
Streamin...	CinemaNow	DataFlow
Streamin...	DailyMotion	DataFlow

Back Submit Cancel

Passaggio 13. Viene visualizzata una finestra popup che mostra l'impostazione dei criteri di

controllo dell'applicazione. Fare clic su **OK**.

Success



Congratulations, your Application Control Policy has been set up successfully.

Ok

Passaggio 14. Per visualizzare il nuovo criterio, selezionare **Protezione > Controllo applicazione > Impostazioni**.

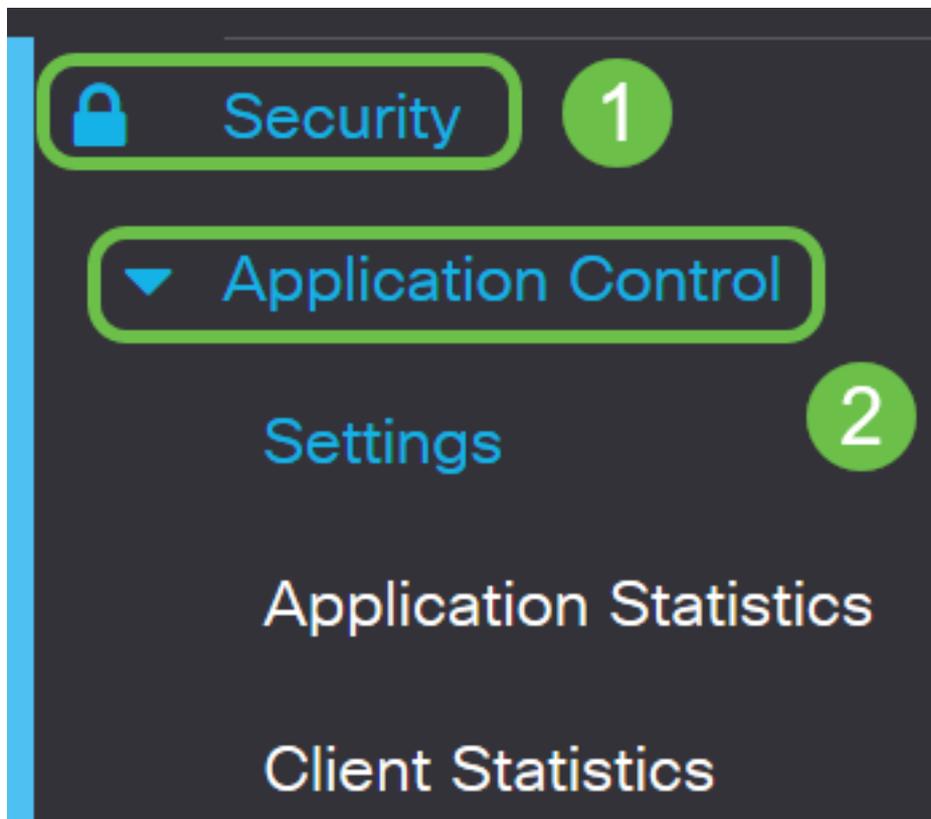
Policy Name	IP Group	Schedule Name	Enable
MobileControl	Any	Always On	<input checked="" type="checkbox"/>

È ora necessario aver configurato correttamente un criterio di controllo dell'applicazione mediante la Creazione guidata Controllo applicazione.

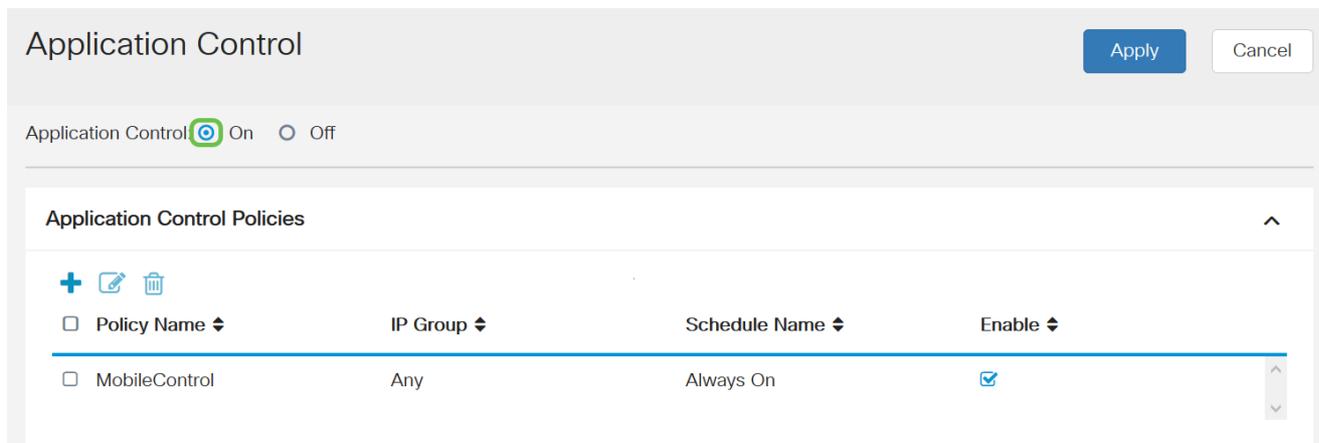
Mediante la configurazione manuale

Nota: Per i criteri configurati tramite la procedura guidata, si tratta dell'area in cui è possibile definire e ottimizzare ulteriormente i criteri.

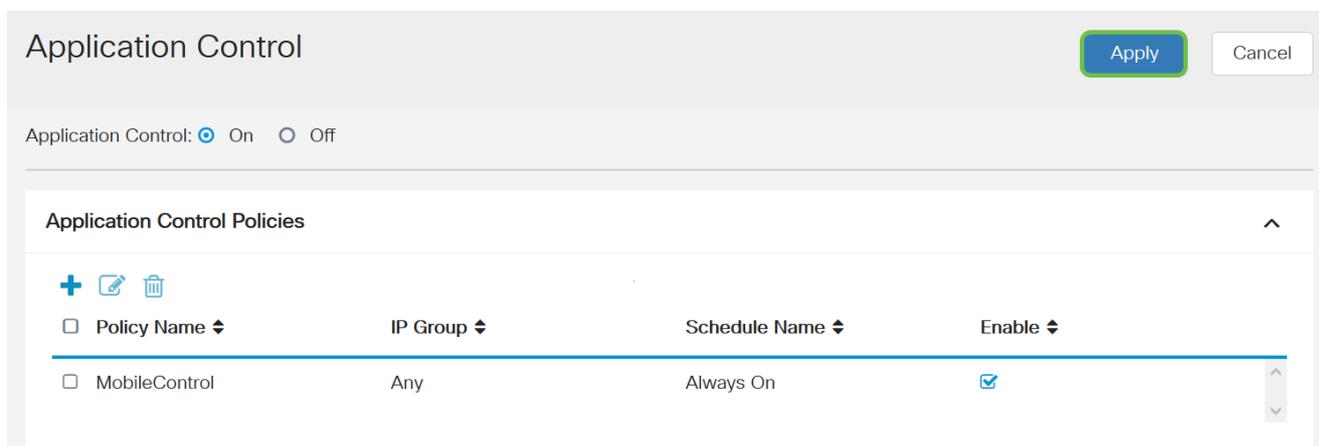
Passaggio 1. Accedere all'utility basata sul Web e scegliere **Sicurezza > Controllo applicazione**.



Passaggio 2. Fare clic sul pulsante di opzione **Su** controllo applicazione per abilitare la funzione Controllo applicazione. La funzione è disattivata per default.

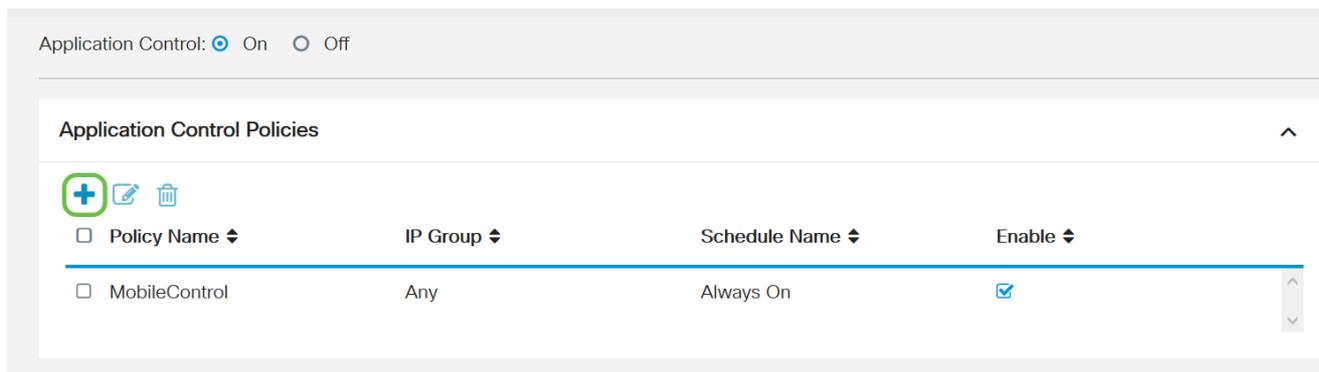


Passaggio. 3 Fare clic su **Apply (Applica)**.



Passaggio 4. Fare clic sull'icona **più** nella tabella Criteri di controllo dell'applicazione per

creare un criterio di controllo dell'applicazione.



Passaggio 5. Creare un nome per il criterio. Il nome non può contenere spazi o caratteri speciali.

Nota: Per questo esempio viene utilizzato *SportsPolicy*.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Passaggio 6. Nel campo *Descrizione*, creare una descrizione per il criterio.

Nota: In questo esempio viene utilizzato *Blocca tutti gli sport*.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Passaggio 7. Selezionare la casella di controllo **Abilita** per attivare questo criterio specifico.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Passaggio 8. Fare clic sul pulsante **Modifica** applicazione per definire e ottimizzare i

parametri da applicare al criterio.

Policy Name:

Description:

Enable:

Application:

Passaggio 9. Selezionare la casella di controllo delle categorie e sottocategorie che si desidera applicare al criterio.

Policy Profile-Add/Edit Categories

- + Adult/Mature Content
- + Business/Investment
- + Entertainment
- + Illegal/Questionable
- + IT Resources
- + Lifestyle/Culture
- + Other
- + Security

Passaggio 10. Fare clic sul segno + accanto a qualsiasi categoria per espandere e visualizzare le sottocategorie e le applicazioni specifiche. In alternativa, per visualizzare tutte le categorie e le relative sottocategorie, fare clic su **Espandi** nella parte inferiore della pagina.

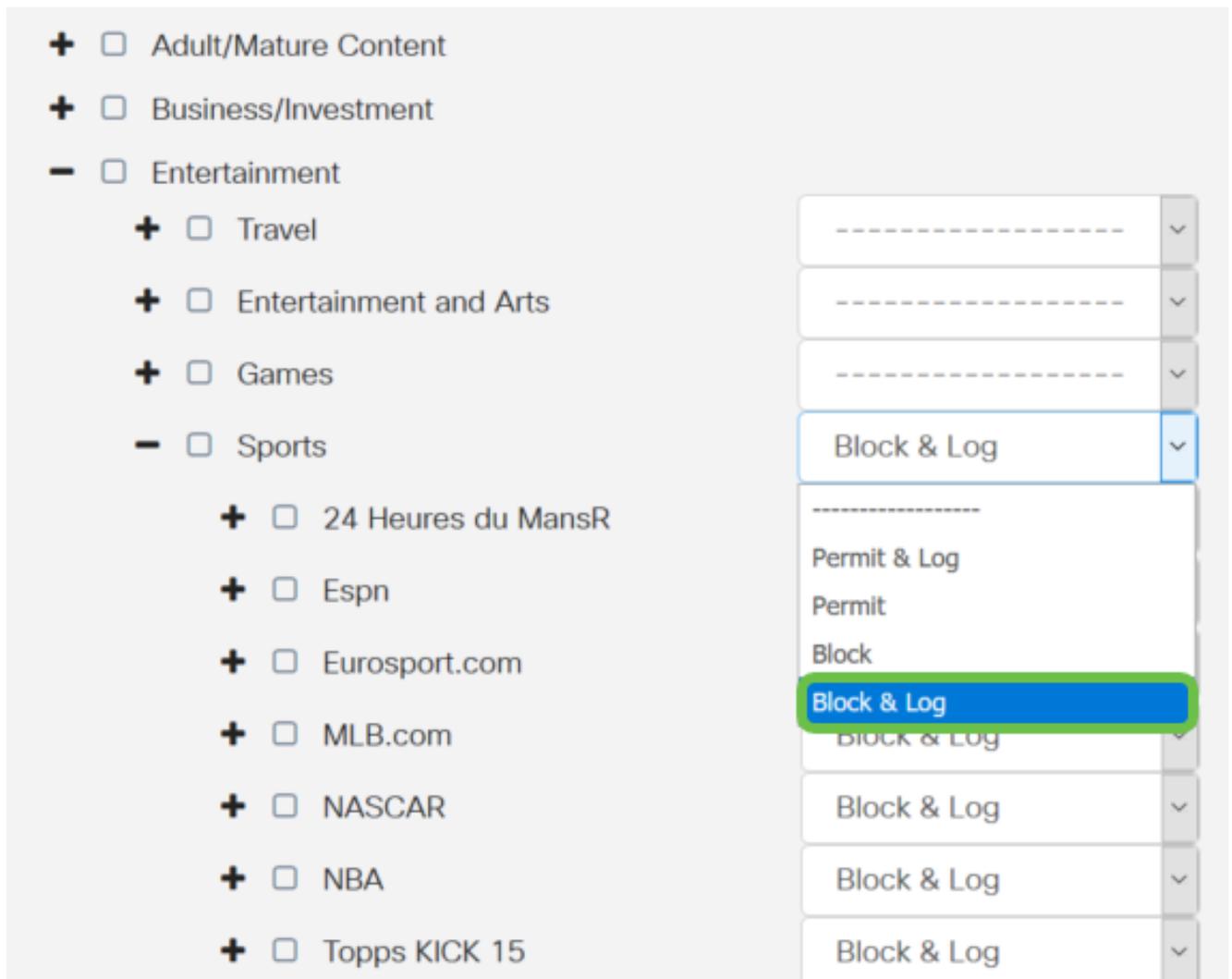
Nota: Per questo esempio, vengono scelti *intrattenimento* e */sport*.

<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adult/Mature Content	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Business/Investment	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Entertainment	
	<input checked="" type="checkbox"/>	Travel	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	Entertainment and Arts	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	Games	<input type="text" value="-----"/> ▾
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sports	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	24 Heures du MansR	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	Espn	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	Eurosport.com	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	MLB.com	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	NASCAR	<input type="text" value="-----"/> ▾
	<input checked="" type="checkbox"/>	NBA	<input type="text" value="-----"/> ▾

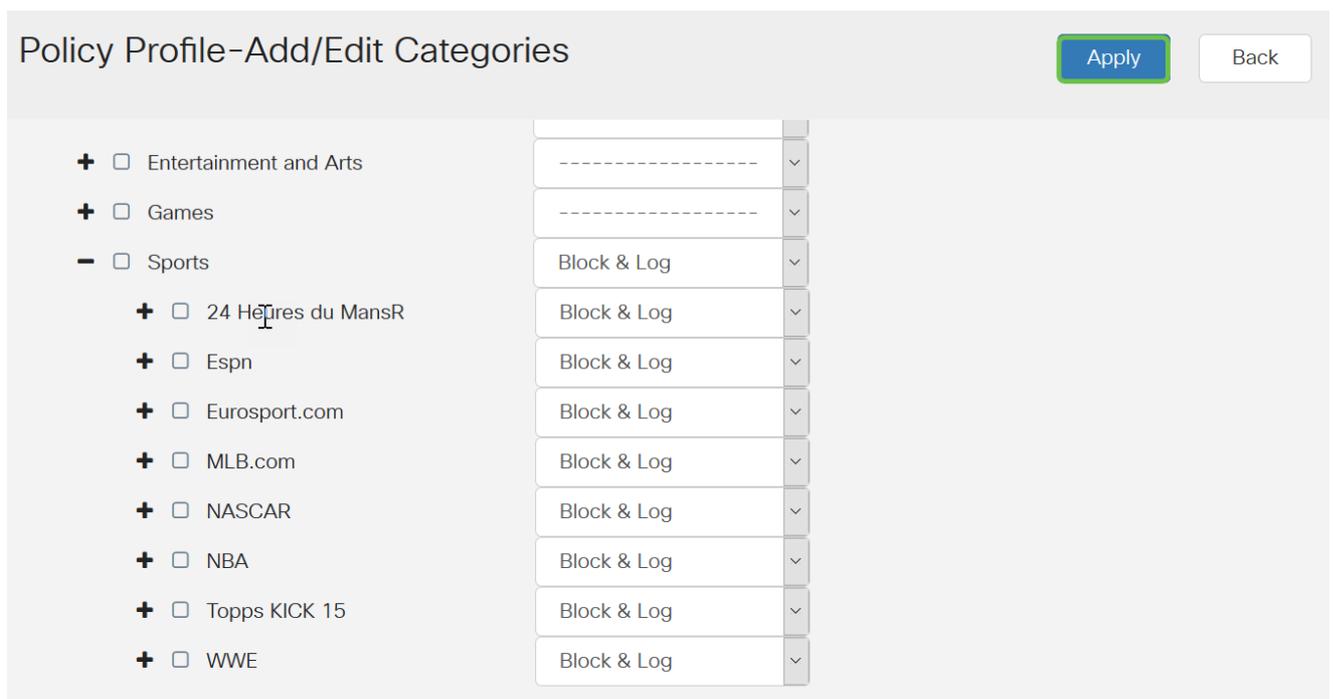
Passaggio 11. (Facoltativo) Fare clic sull'elenco a discesa accanto all'applicazione che si desidera applicare al criterio. Se necessario, ripetere questo passaggio. Le opzioni sono:

- Permit & Log: il flusso e la registrazione dei dati è consentito.
- Permit: i dati sono consentiti.
- Blocco: i dati sono bloccati.
- Blocco e registro: i dati vengono bloccati e registrati.

Nota: Per questo esempio, è stato scelto *Blocca & Registra* per Sport.



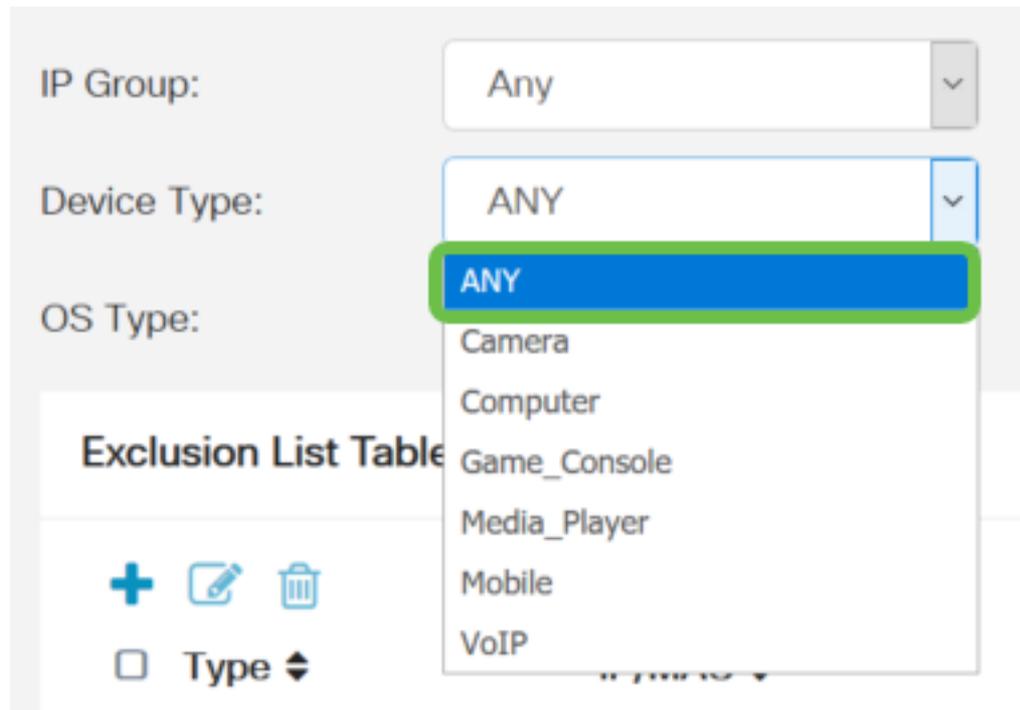
Passaggio 12. Nella tabella Elenco applicazioni vengono inserite le categorie e le applicazioni scelte. Fare clic su **Apply** (Applica).



Passaggio 13. Dall'elenco a discesa Device Type (Tipo di dispositivo), selezionare l'origine o la destinazione dei pacchetti da filtrare. È possibile scegliere una sola opzione alla volta. Le opzioni sono:

- ANY - Consente di applicare il criterio a qualsiasi dispositivo.
- Fotocamera: selezionare questa opzione per applicare il criterio alle videocamere (ad esempio, le videocamere di sicurezza IP).
- Computer — scegliere questa opzione per applicare il criterio ai computer.
- Game_Console: scegliere questa opzione per applicare la policy alle console di gioco.
- Media_Player: scegliere questa opzione per applicare il criterio a Media Player.
- Mobile: scegliere questa opzione per applicare il criterio ai dispositivi mobili.
- VoIP: scegliere questa opzione per applicare il criterio ai dispositivi Voice over Internet Protocol.

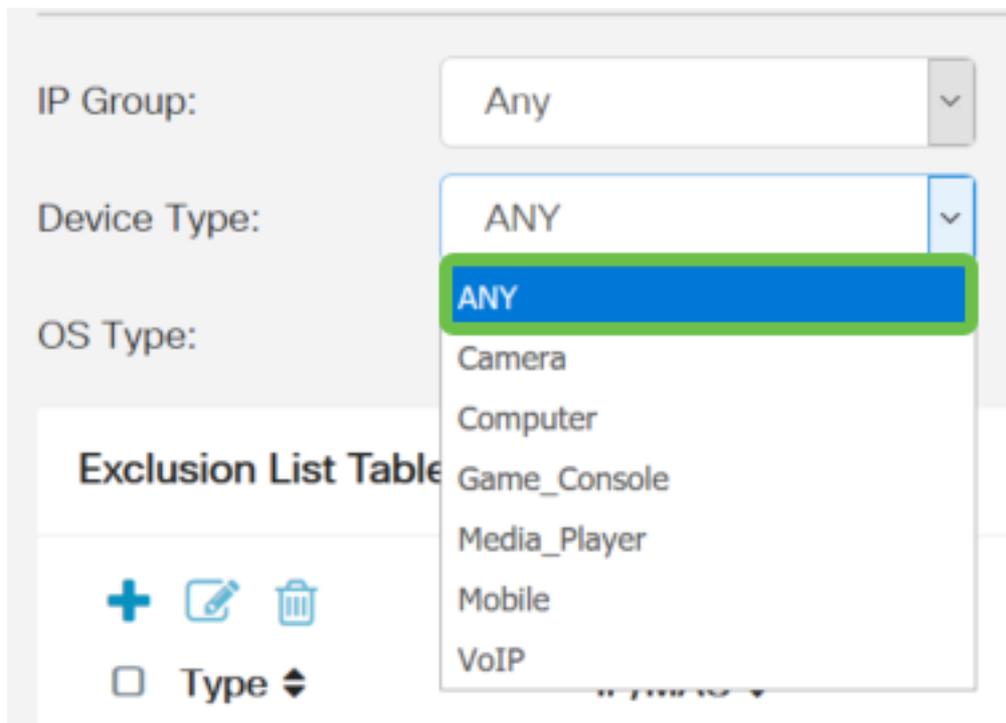
Nota: Per questo esempio, viene scelto ANY (QUALSIASI).



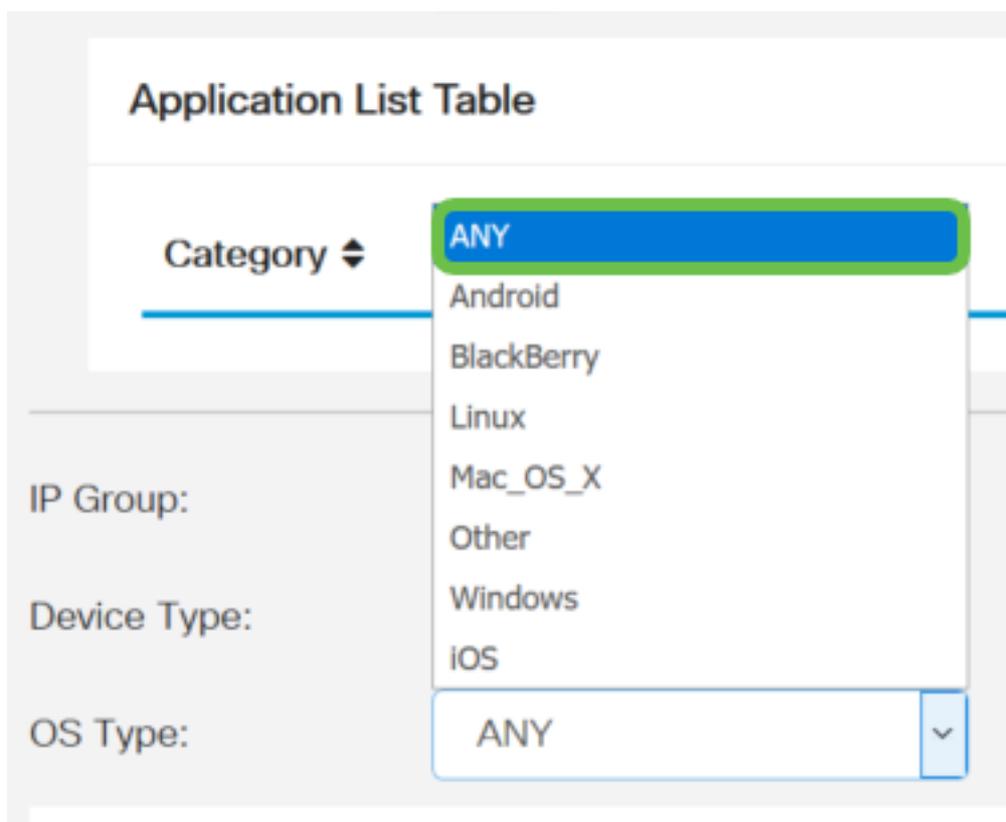
Passaggio 14. Dall'elenco a discesa Tipo di sistema operativo, scegliere un sistema operativo al quale applicare il criterio. È possibile sceglierne solo uno alla volta. Le opzioni sono:

- ANY - Applica il criterio a qualsiasi tipo di sistema operativo. Questa è l'impostazione predefinita.
- Android: applica il criterio solo al sistema operativo Android.
- BlackBerry: applica il criterio solo al sistema operativo Blackberry.
- Linux: applica la policy solo al sistema operativo Linux.
- Mac_OS_X — applica il criterio solo a Mac OS.
- Altro - applica il criterio a un sistema operativo non elencato.
- Windows: applica il criterio al sistema operativo Windows.
- iOS: applica la policy solo a iOS OS.

Nota: Per questo esempio, viene scelto ANY (QUALSIASI).



Passaggio 15. Selezionare un gruppo IP dall'elenco a discesa *Gruppi IP*. Le opzioni possono variare in base al fatto che siano stati precedentemente configurati gruppi IP. Il valore predefinito è Any.



Passaggio 16. (Facoltativo) Fare clic sul pulsante **più** nella tabella Elenco esclusioni per escludere utenti specifici dal criterio.

IP Group:

Device Type:

OS Type:

Exclusion List Table

Passaggio 17. Dall'elenco a discesa Tipo, scegliere il tipo di indirizzo da escludere dal criterio. Le opzioni sono:

- MAC — specificare un indirizzo MAC da escludere dal criterio.
- Indirizzo IPv4: specificare un singolo indirizzo IPv4 da escludere dal criterio.
- Intervallo IPv4: specificare un intervallo di host di indirizzi IPv4 da escludere dal criterio. Immettere un indirizzo IP iniziale e un indirizzo IP finale nei rispettivi campi.
- Indirizzo IPv6 — Specificare un singolo indirizzo IPv6 da escludere dal criterio.
- Intervallo IP IPv6: specificare un intervallo di host di indirizzi IPv6 da escludere dal criterio. Immettere un indirizzo IP iniziale e un indirizzo IP finale nei rispettivi campi.

Nota: Nell'esempio, viene usato l'indirizzo IPv4.

Exclusion List Table

Schedul

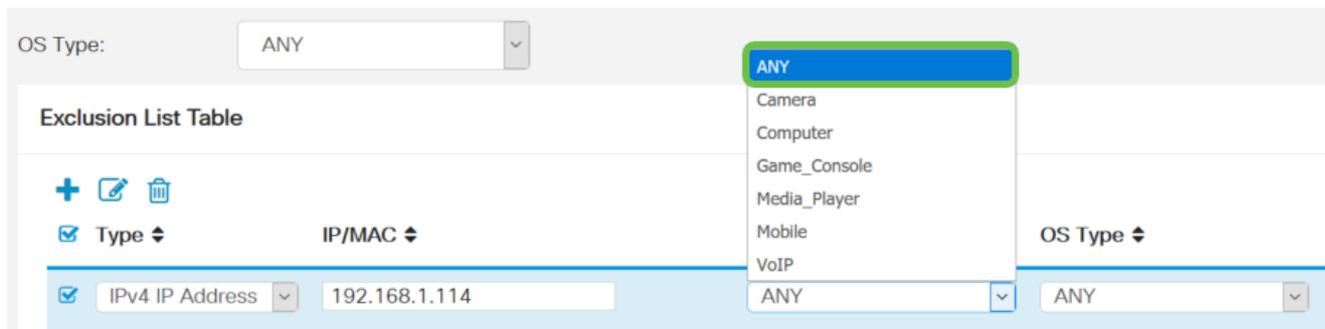
Passaggio 18. Immettere un indirizzo IPv4 nel campo IP.

Nota: nell'esempio viene usato 192.168.1.114.

Exclusion List Table

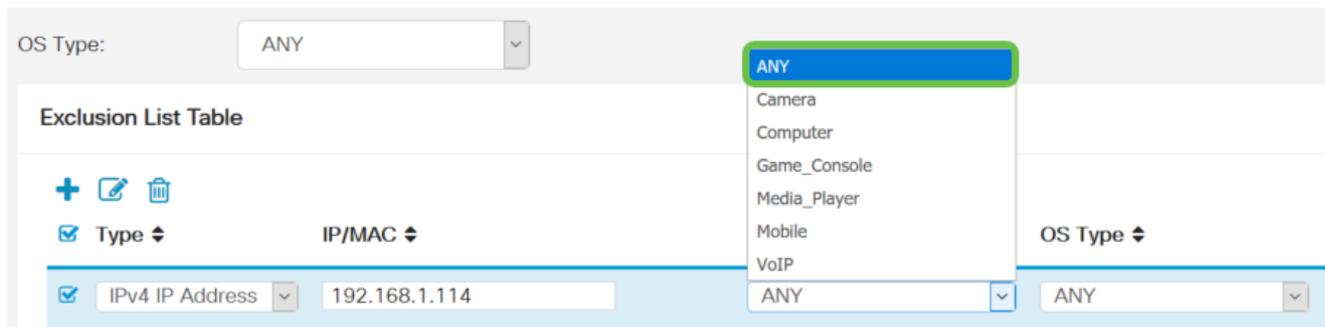
Passaggio 19. Scegliere un tipo di dispositivo da escludere dal criterio.

Nota: Per questo esempio, viene scelto ANY (QUALSIASI).



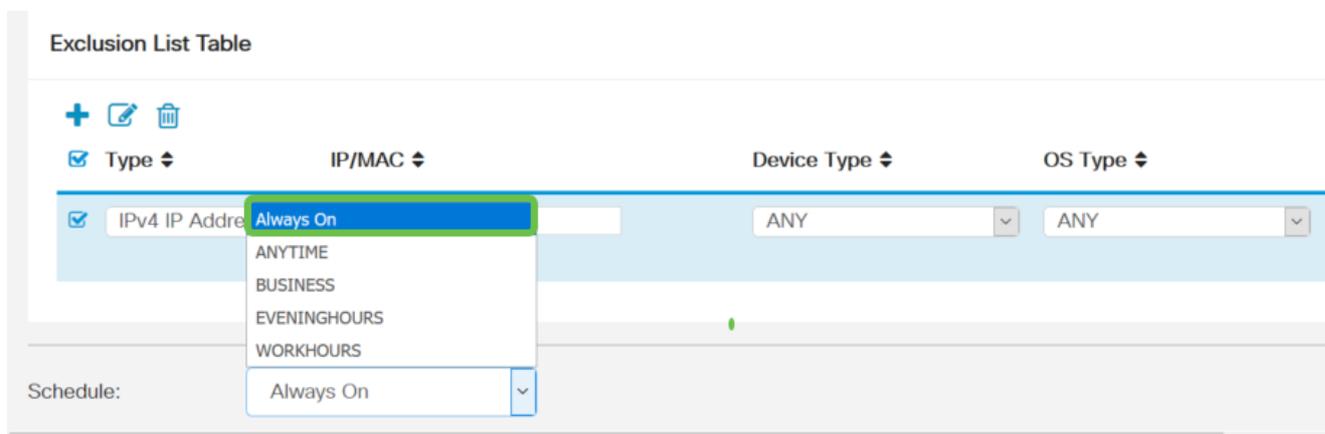
Passaggio 20. Scegliere un tipo di sistema operativo da escludere dal criterio.

Nota: Per questo esempio, viene scelto *ANY* (QUALSIASI).

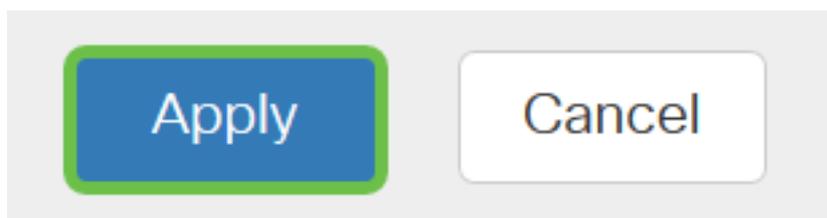


Passaggio 21. Dall'elenco a discesa Programmazione, scegliere una programmazione per la quale impostare il criterio. Le opzioni possono variare a seconda delle pianificazioni definite in precedenza. Per configurare una pianificazione, selezionare **Configurazione di sistema > Pianificazioni**.

Nota: Per questo esempio viene scelto *Always On*.



Passaggio 2. Fare clic su **Applica**.



Passaggio 23. (Facoltativo) Per salvare la configurazione in modo permanente, fare clic sull'icona **Salva**.

Nota: Per salvare definitivamente la configurazione, accertarsi di salvare la configurazione corrente nella configurazione di avvio.

A questo punto, è necessario configurare correttamente la funzione di controllo delle applicazioni sul router serie RV34x.

Potresti trovare anche questo articolo informativo: [Domande frequenti \(FAQ\) sui router serie RV34x](#)

Questo sito offre diversi collegamenti ad altri articoli che potrebbero essere interessanti: [Serie RV34x Router - Pagina del prodotto](#)

Qui è disponibile un video relativo a questo articolo...

[Fare clic qui per visualizzare altre Tech Talks di Cisco](#)