

# Konfigurieren der Anwendungskontrolle auf dem Router der Serie RV34x

## Ziel

Anwendungskontrolle ist eine zusätzliche Sicherheitsfunktion auf dem Router, die ein bereits gesichertes Netzwerk optimieren, die Produktivität am Arbeitsplatz steigern und die Bandbreite maximieren kann. Die Anwendungskontrolle kann für Smartphones und andere browserbasierte Anwendungen hilfreich sein. Wenn Sie einen Wireless Access Point (WAP) mit einem Router verbinden, kann der Router den Datenverkehr zu einem mit dem WAP verbundenen Host zulassen oder verweigern. Dies wiederum hindert Benutzer daran, auf bestimmte Anwendungen zuzugreifen.

In diesem Artikel wird erläutert, wie Sie die Anwendungskontrolle auf den Routern der Serie RV34x mithilfe des Assistenten für die Anwendungssteuerung und mithilfe der manuellen Konfiguration konfigurieren.

## Anwendbare Geräte

- Serie RV34x

## Softwareversion

- 1.0.2.16

## Konfigurieren der Anwendungskontrolle

### Mit dem Anwendungssteuerungs-Assistenten

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Konfigurationsassistenten > Launch Wizard...**

Configuration Wizards

Initial Setup Wizard

Lauch Wizard... This wizard can be used to perform the initial setup of the router.

Application Control Wizard

Lauch Wizard... This wizard can be used create an Application Control policy.

VPN Setup Wizard

Lauch Wizard... This wizard can be used create a Site to Site VPN tunnel.

Schritt 2: Klicken Sie auf das Optionsfeld **Ein**, um den *Application Controller* zu aktivieren. Diese Funktion ist standardmäßig deaktiviert.

Application Control Wizard

1. Policy Name

2. Application Name

Application Controller:  On  Off

Enter a name for this policy:

Schritt 3: Erstellen Sie einen eindeutigen Namen für die Richtlinie im Feld *Policy Name* (*Richtliniennamen*). Dieser Name darf keine Leerzeichen oder Sonderzeichen enthalten.

**Hinweis:** In diesem Beispiel wird *MobileControl* verwendet.

Application Control Wizard

1. Policy Name

2. Application Name

Application Controller:  On  Off

Enter a name for this policy:

MobileControl

Schritt 4: Klicken Sie auf **Weiter**.

Next

Cancel

Schritt 5: Klicken Sie auf die Schaltfläche **Bearbeiten**, um die Parameter und Kategorien zu

definieren, die das Anwendungssteuerelement zum Filtern von Daten verwendet.

1. Policy Name Enter the application names to be blocked: [Edit](#)

2. Application Name **Application List Table** ^

3. Schedule

Category ▾ Application ▾ Behavior ▾

---

Schritt 6: Klicken Sie auf das + neben einer Kategorie, um die Unterkategorien und spezifischen Anwendungen zu erweitern und anzuzeigen. Sie können auch alle Kategorien und deren Unterkategorien anzeigen, indem Sie unten auf der Seite auf **Erweitern** klicken.

**Hinweis:** In diesem Beispiel wird die Kategorie *IT-Ressourcen* erweitert.

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  
 ▾

Schritt 7: Aktivieren Sie das Kontrollkästchen der Kategorien und Unterkategorien, die auf die Richtlinie angewendet werden sollen.

**Hinweis:** In diesem Beispiel sind *Streaming Media* und *Internet Communications* die Unterkategorien unter *IT-Ressourcen*, die als Beispiele verwendet werden.

✓ 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

Schritt 8: (Optional) Klicken Sie auf die Dropdown-Liste neben der Anwendung, die Sie auf die Richtlinie anwenden möchten. Wiederholen Sie diesen Schritt bei Bedarf. Folgende Optionen stehen zur Verfügung:

- Zulassen und Protokollieren: Daten können übertragen und protokolliert werden.
- Zulassen - Daten sind zulässig.
- Sperren - Daten werden blockiert.
- Block & Log (Blockieren und Protokoll): Daten werden blockiert und protokolliert.

**Hinweis:** Stellen Sie sicher, dass die Protokollierung auf dem Router aktiviert ist, indem Sie **Systemkonfiguration > Protokoll** auswählen. Aktivieren Sie das Kontrollkästchen **Aktivieren**, und klicken Sie dann auf **Übernehmen**.

✓ 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

**Hinweis:** In diesem Beispiel wird *Block* für Streaming-Medien verwendet.

Schritt 9: Klicken Sie auf **Übernehmen**. Sie werden zurück zur zweiten Seite des Konfigurationsassistenten weitergeleitet.

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

**Hinweis:** Die Tabelle der Anwendungsliste enthält die ausgewählten Kategorien und Anwendungen.

✓ 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

Schritt 10: Klicken Sie auf **Weiter**, um zur Seite "Zeitplan" zu gelangen.

✓ 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

Schritt 11: Wählen Sie in der Dropdown-Liste Schedule (Zeitplan) einen Zeitplan aus, für den die Richtlinie festgelegt werden soll. Die Optionen können je nach vorher festgelegten Zeitplänen variieren. Um einen Zeitplan zu konfigurieren, gehen Sie zu **Systemkonfiguration**

> **Zeitpläne.** Klicken Sie auf **Weiter.**

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

Select the schedule to block the application:

1

Always On

Always On

ANYTIME

BUSINESS

EVENINGHOURS

WORKHOURS

2

Back **Next** Cancel

**Hinweis:** In diesem Beispiel wird *Always On* verwendet.

Schritt 12: Sie werden zur Seite "Übersicht" weitergeleitet. Die Tabelle "Anwendungssteuerungsrichtlinien" wird nun mit der von Ihnen konfigurierten Richtlinie gefüllt. Überprüfen Sie Ihre Einstellungen auf der Übersichtsseite, und klicken Sie auf **Senden**. Sie können auf "Zurück" klicken, um Ihre Einstellungen zu ändern.

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

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

Schritt 13: Ein Popup-Fenster wird geöffnet, in dem angezeigt wird, dass die

Anwendungssteuerungsrichtlinie erfolgreich eingerichtet wurde. Klicken Sie auf **OK**.

# Success



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

Ok

Schritt 14: Um die neue Richtlinie anzuzeigen, navigieren Sie zu **Sicherheit > Anwendungskontrolle > Einstellungen**.

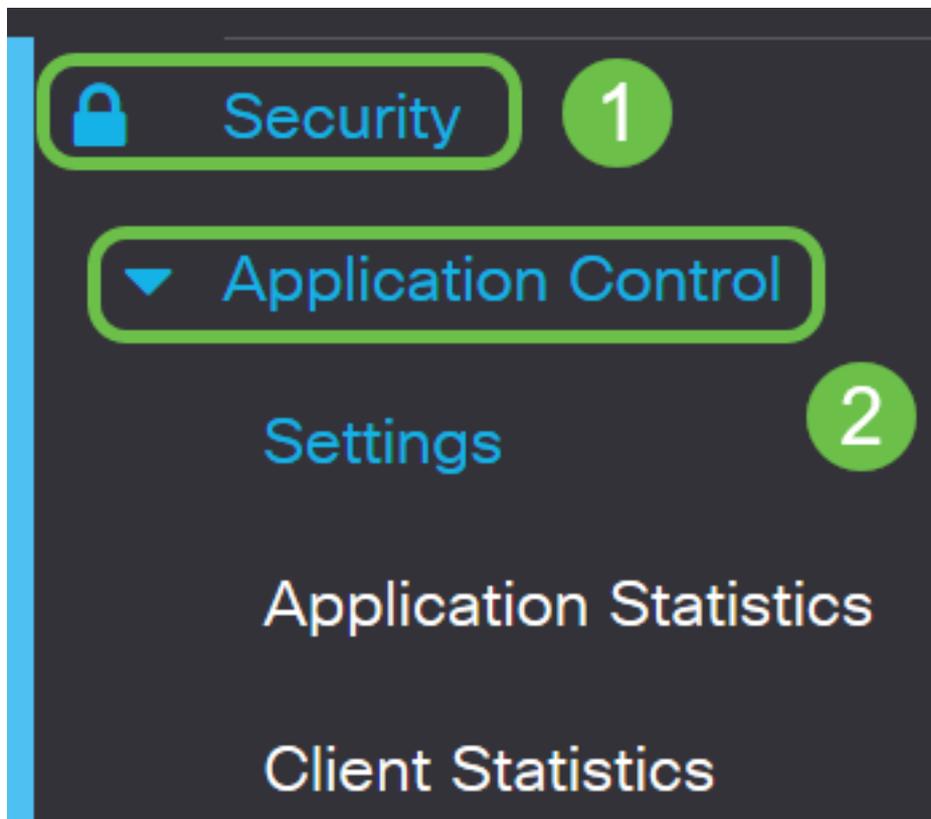
Policy Name	IP Group	Schedule Name	Enable
MobileControl	Any	Always On	<input checked="" type="checkbox"/>

Sie sollten jetzt über den Anwendungssteuerungsassistenten eine Anwendungssteuerungsrichtlinie erfolgreich konfiguriert haben.

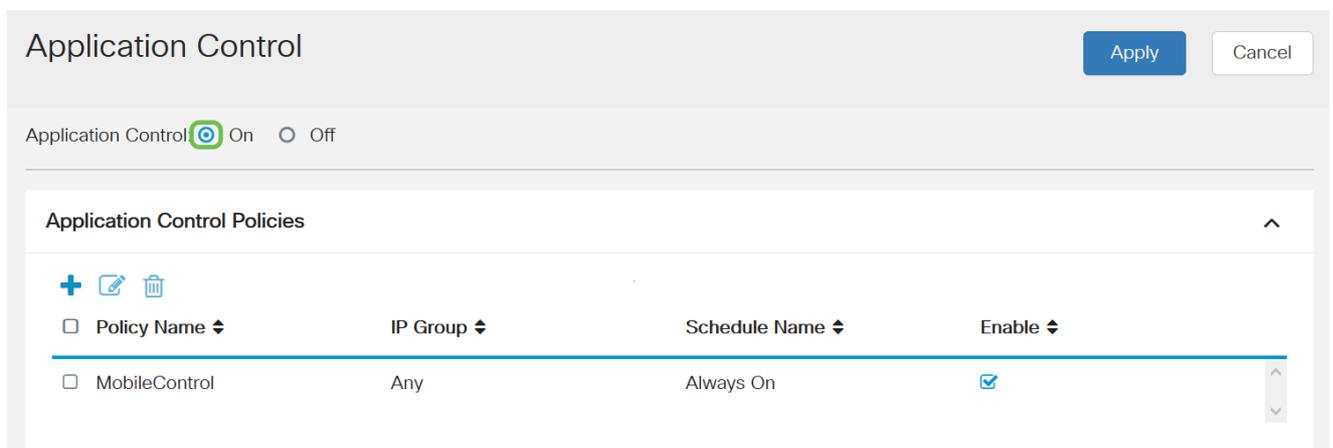
## Über die manuelle Konfiguration

**Hinweis:** Für Richtlinien, die über den Assistenten konfiguriert werden, können Sie in diesem Bereich Ihre Richtlinien weiter definieren und anpassen.

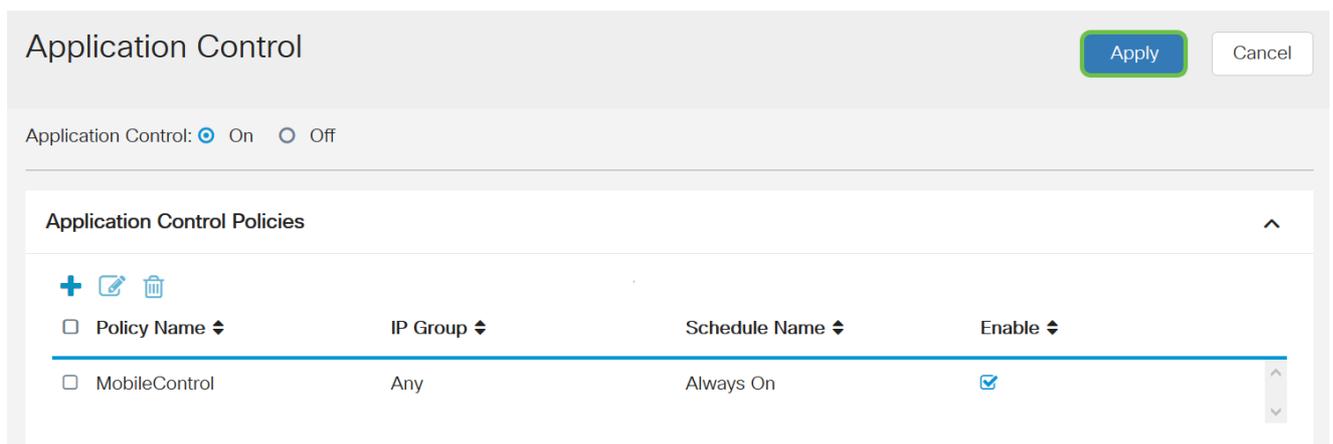
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Sicherheit > Anwendungskontrolle** aus.



Schritt 2: Klicken Sie auf das Optionsfeld **On** Application Control (Anwendungssteuerung), um das Feature Application Control (Anwendungssteuerung) zu aktivieren. Die Funktion ist standardmäßig deaktiviert.



Schritt. 3 Klicken Sie auf **Übernehmen**.



Schritt 4: Klicken Sie in der Tabelle Anwendungssteuerungsrichtlinien auf das **Pluszeichen**, um eine Anwendungssteuerungsrichtlinie zu erstellen.

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

Schritt 5: Erstellen Sie einen Namen für die Richtlinie. Dieser Name darf keine Leerzeichen oder Sonderzeichen enthalten.

**Hinweis:** In diesem Beispiel wird *SportsPolicy* verwendet.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Schritt 6: Erstellen Sie im Feld *Beschreibung* eine Beschreibung für die Richtlinie.

**Hinweis:** In diesem Beispiel wird *Block all Sports* verwendet.

# Policy Profile-Add/Edit

Policy Name:

SportsPolicy

Description:

Block all Sports

Enable:

Application:

Edit

Schritt 7: Aktivieren Sie das Kontrollkästchen **Aktivieren**, um diese bestimmte Richtlinie zu aktivieren.

# Policy Profile-Add/Edit

Policy Name:

SportsPolicy

Description:

Block all Sports

Enable:

Application:

Edit

Schritt 8: Klicken Sie auf die Schaltfläche Anwendung **bearbeiten**, um die Parameter zu definieren und anzupassen, die auf die Richtlinie angewendet werden sollen.

Policy Name:

Description:

Enable:

---

Application:

Schritt 9: Aktivieren Sie das Kontrollkästchen der Kategorien und Unterkategorien, die auf die Richtlinie angewendet werden sollen.

Policy Profile-Add/Edit Categories

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

Schritt 10: Klicken Sie auf das **+** neben einer beliebigen Kategorie, um die Unterkategorien und spezifischen Anwendungen zu erweitern und anzuzeigen. Sie können auch alle Kategorien und deren Unterkategorien anzeigen, indem Sie unten auf der Seite auf **Erweitern** klicken.

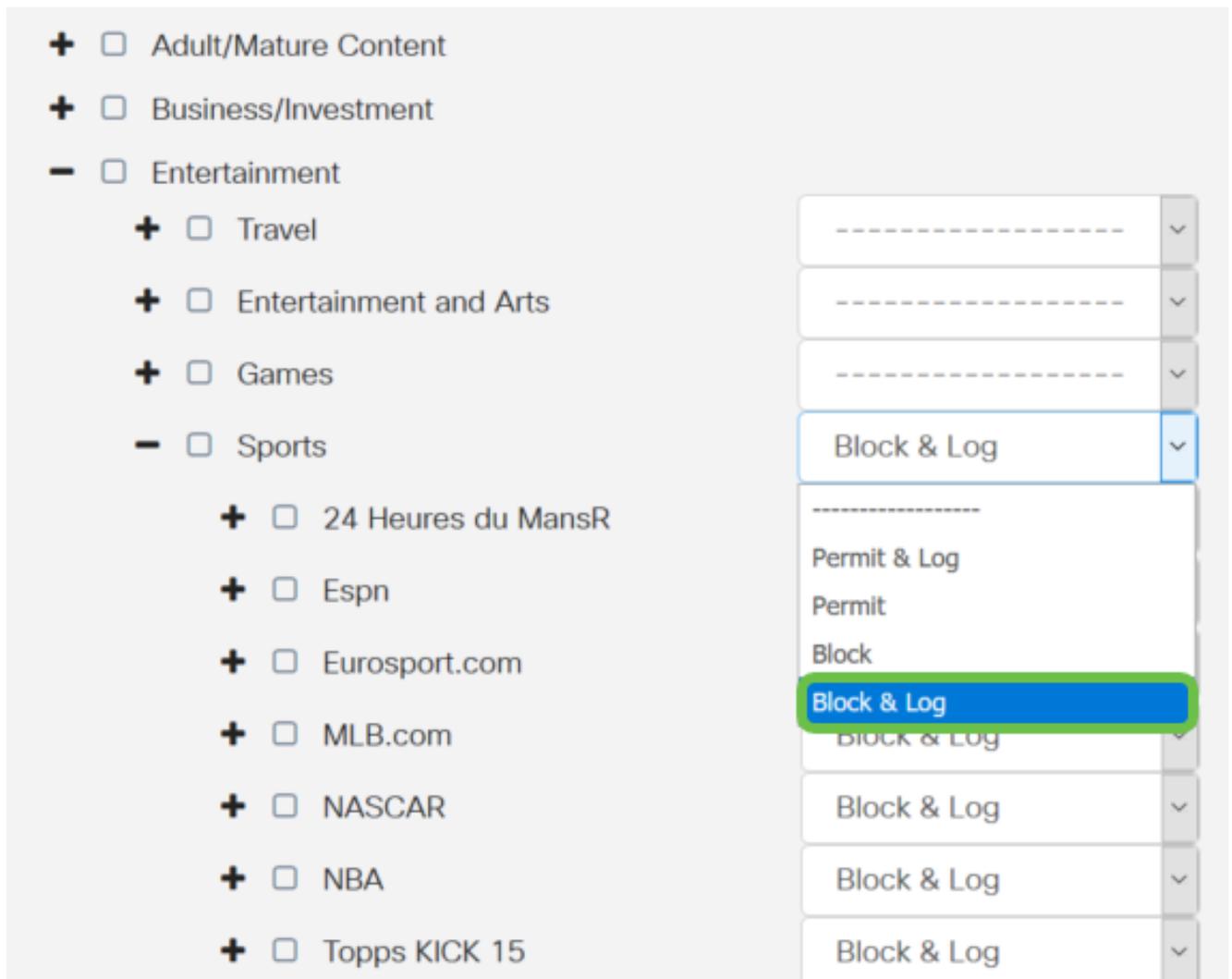
**Hinweis:** In diesem Beispiel werden *Unterhaltung* und *oder Sport* ausgewählt.

<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="-----"/> ▾

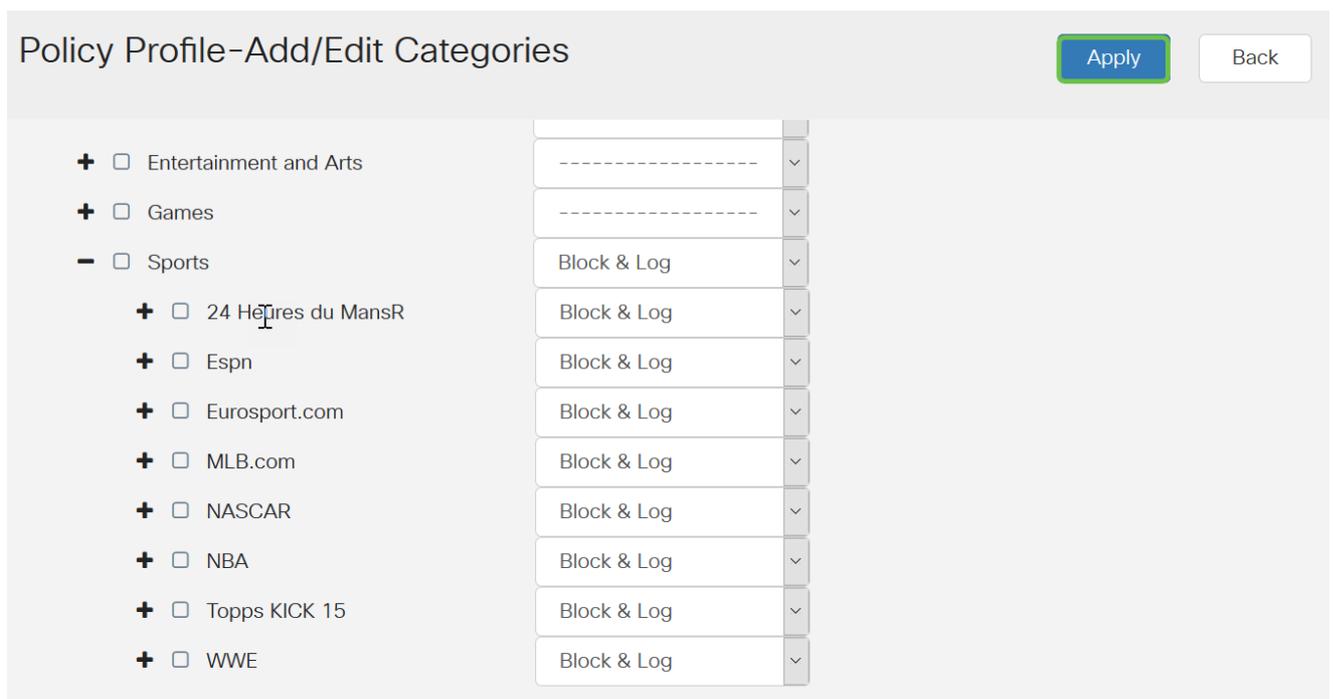
Schritt 11: (Optional) Klicken Sie auf die Dropdown-Liste neben der Anwendung, die Sie auf die Richtlinie anwenden möchten. Wiederholen Sie diesen Schritt bei Bedarf. Folgende Optionen stehen zur Verfügung:

- Zulassen und Protokollieren: Daten können übertragen und protokolliert werden.
- Zulassen - Daten sind zulässig.
- Sperren - Daten werden blockiert.
- Block & Log (Blockieren und Protokoll): Daten werden blockiert und protokolliert.

**Hinweis:** In diesem Beispiel wird *Block & Log* für Sport ausgewählt.



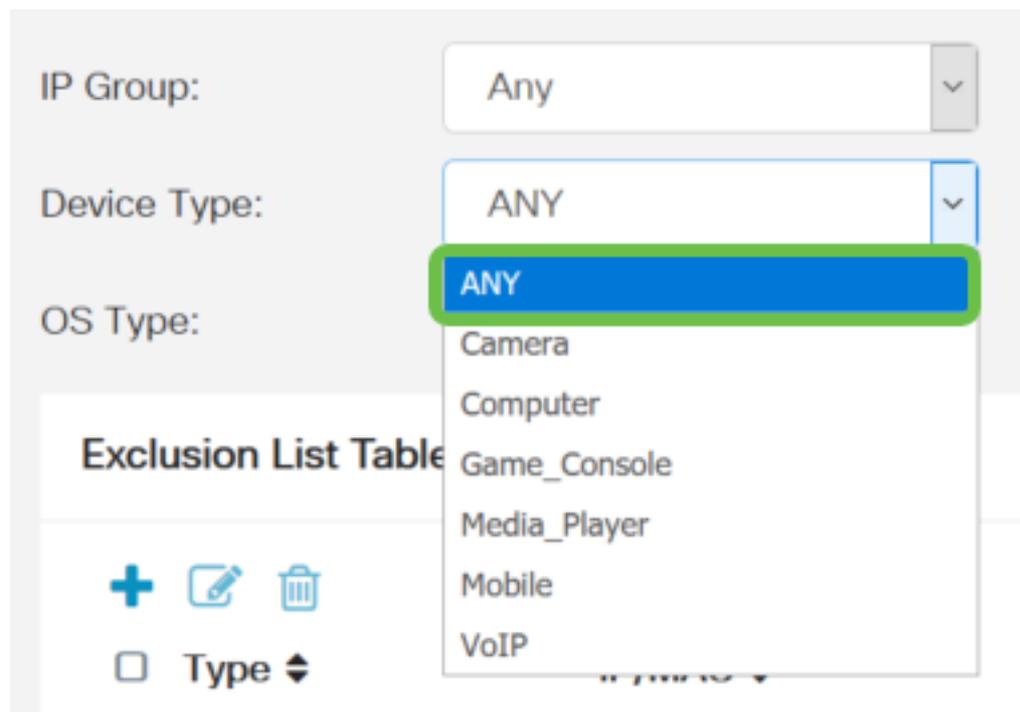
Schritt 12: Die Tabelle der Anwendungsliste enthält die ausgewählten Kategorien und Anwendungen. Klicken Sie auf **Übernehmen**.



Schritt 13: Wählen Sie in der Dropdown-Liste Device Type (Gerätetyp) die Quelle oder das Ziel der zu filternden Pakete aus. Es kann jeweils nur eine Option ausgewählt werden. Folgende Optionen stehen zur Verfügung:

- BELIEBIG - Wählen Sie diese Option, um die Richtlinie auf jedes Gerät anzuwenden.
- Kamera: Wählen Sie diese Option aus, um die Richtlinie auf Kameras (z. B. IP-Sicherheitskameras) anzuwenden.
- Computer - Wählen Sie diese Option aus, um die Richtlinie auf Computer anzuwenden.
- Game\_Console: Wählen Sie diese Option aus, um die Richtlinie auf Spielekonsolen anzuwenden.
- Media\_Player: Wählen Sie diese Option, um die Richtlinie auf Media Player anzuwenden.
- Mobile - Wählen Sie diese Option, um die Richtlinie auf mobile Geräte anzuwenden.
- VoIP: Wählen Sie diese Option aus, um die Richtlinie auf Voice over Internet Protocol-Geräte anzuwenden.

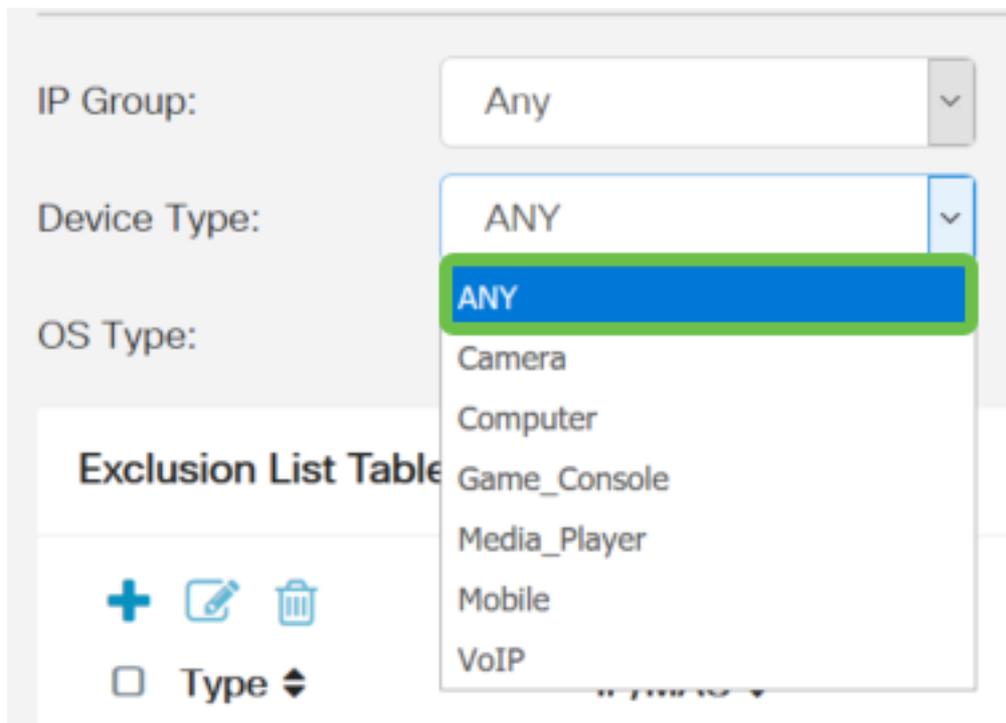
**Hinweis:** In diesem Beispiel wird *JEDER* ausgewählt.



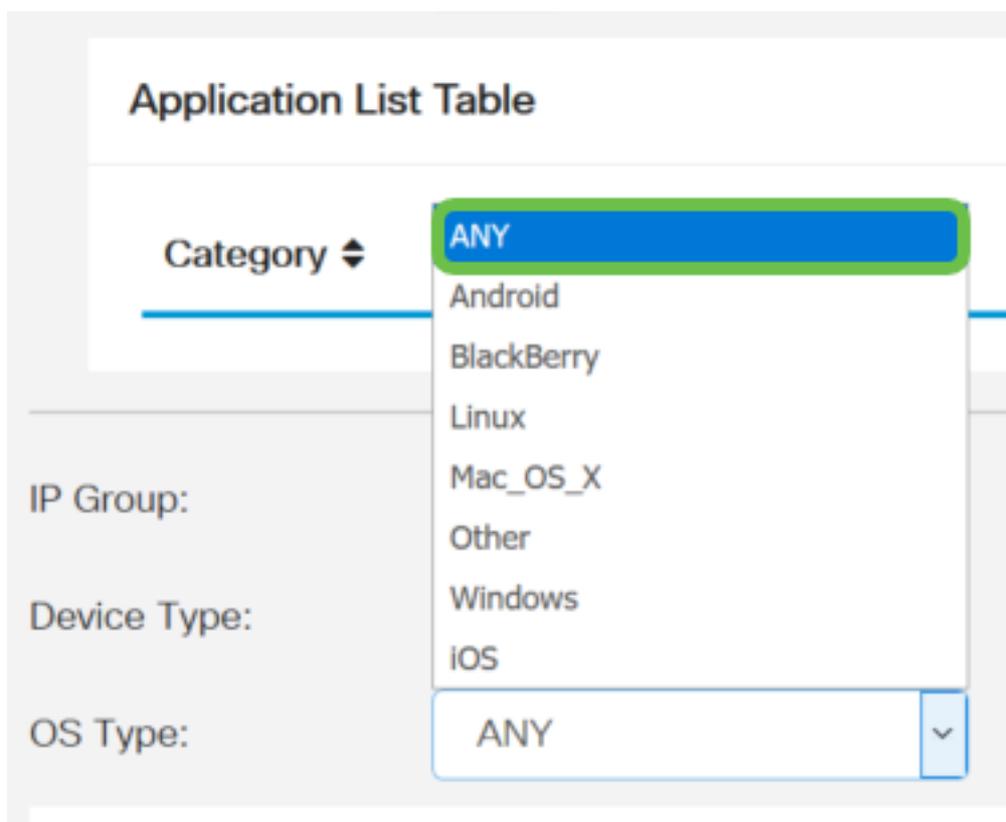
Schritt 14: Wählen Sie in der Dropdown-Liste OS Type (Betriebssystemtyp) ein Betriebssystem aus, für das die Richtlinie gelten soll. Es kann jeweils nur eine ausgewählt werden. Folgende Optionen stehen zur Verfügung:

- BELIEBIG - Wendet die Richtlinie auf jeden Betriebssystemtyp an. Dies ist die Standardeinstellung.
- Android - Diese Richtlinie gilt nur für Android-Betriebssysteme.
- BlackBerry - Wendet die Richtlinie nur auf BlackBerry-Betriebssysteme an.
- Linux — Anwendung der Richtlinie nur auf Linux-Betriebssysteme.
- Mac\_OS\_X — Wendet die Richtlinie nur auf Mac OS an.
- Other (Andere) - Wendet die Richtlinie auf ein Betriebssystem an, das nicht aufgeführt ist.
- Windows — Wendet die Richtlinie auf das Windows-Betriebssystem an.
- iOS - Gilt nur für iOS-Betriebssysteme.

**Hinweis:** In diesem Beispiel wird *JEDER* ausgewählt.



Schritt 15: Wählen Sie eine IP-Gruppe aus der Dropdown-Liste *IP Groups (IP-Gruppen)* aus. Die Optionen können variieren, wenn zuvor IP-Gruppen konfiguriert wurden. Der Standardwert ist Any (Beliebig).



Schritt 16: (Optional) Klicken Sie unter der Ausschlussliste auf das **Pluszeichen**, um bestimmte Benutzer von der Richtlinie auszuschließen.

IP Group:

Device Type:

OS Type:

**Exclusion List Table**

<input checked="" type="checkbox"/> Type	IP/MAC	Device Type	OS Type
<input checked="" type="checkbox"/> Any	Any	ANY	ANY

Schritt 17: Wählen Sie in der Dropdown-Liste Type (Typ) den Adresstyp aus, der von der Richtlinie ausgeschlossen werden soll. Folgende Optionen stehen zur Verfügung:

- MAC (MAC): Geben Sie eine MAC-Adresse an, die von der Richtlinie ausgeschlossen werden soll.
- IPv4-IP-Adresse: Geben Sie eine einzelne IPv4-Adresse an, die von der Richtlinie ausgeschlossen werden soll.
- IPv4 IP Range (IPv4-IP-Bereich): Geben Sie einen Bereich von Hosts mit IPv4-Adressen an, die von der Richtlinie ausgeschlossen werden sollen. Geben Sie eine Start-IP-Adresse und eine End-IP-Adresse in die entsprechenden Felder ein.
- IPv6 IP Address (IPv6-Adresse): Geben Sie eine einzelne IPv6-Adresse an, die von der Richtlinie ausgeschlossen werden soll.
- IPv6 IP Range (IPv6-IP-Bereich): Geben Sie einen Bereich von Hosts mit IPv6-Adressen an, die von der Richtlinie ausgeschlossen werden sollen. Geben Sie eine Start-IP-Adresse und eine End-IP-Adresse in die entsprechenden Felder ein.

**Hinweis:** In diesem Beispiel wird *IPv4-IP-Adresse* verwendet.

**Exclusion List Table**

<input checked="" type="checkbox"/> Type	IP/MAC	Device Type	OS Type
<input checked="" type="checkbox"/> Any	Any	ANY	ANY

Schedule:

Schritt 18: Geben Sie eine IPv4-Adresse in das *IP*-Feld ein.

**Hinweis:** In diesem Beispiel wird 192.168.1.114 verwendet.

## Exclusion List Table

The screenshot shows the 'Exclusion List Table' interface. At the top, there are icons for adding (+), editing (pencil), and deleting (trash) entries. Below these are four columns: 'Type', 'IP/MAC', 'Device Type', and 'OS Type'. The 'Type' column has a checked checkbox and a dropdown menu set to 'IPv4 IP Address'. The 'IP/MAC' column contains the IP address '192.168.1.114', which is highlighted with a green border. The 'Device Type' column has a dropdown menu set to 'ANY'. The 'OS Type' column has a dropdown menu set to 'ANY'.

Schritt 19: Wählen Sie einen Gerätetyp aus, der von der Richtlinie ausgeschlossen werden soll.

**Hinweis:** In diesem Beispiel wird *JEDER* ausgewählt.

This screenshot is similar to the previous one, but the 'Device Type' dropdown menu is open, showing a list of options: 'ANY', 'Camera', 'Computer', 'Game\_Console', 'Media\_Player', 'Mobile', and 'VoIP'. The 'ANY' option is highlighted with a blue background and a green border.

Schritt 20: Wählen Sie einen Betriebssystemtyp aus, der von der Richtlinie ausgeschlossen werden soll.

**Hinweis:** In diesem Beispiel wird *JEDER* ausgewählt.

This screenshot is identical to the previous one, showing the 'OS Type' dropdown menu open with 'ANY' selected and highlighted.

Schritt 21: Wählen Sie in der Dropdown-Liste Schedule (Zeitplan) einen Zeitplan aus, für den die Richtlinie festgelegt werden soll. Die Optionen können je nach vorher festgelegten Zeitplänen variieren. Um einen Zeitplan zu konfigurieren, gehen Sie zu **Systemkonfiguration > Zeitpläne**.

**Hinweis:** In diesem Beispiel wird *Always On* ausgewählt.

Exclusion List Table

+ ✎ 🗑

Type ⇅ IP/MAC ⇅ Device Type ⇅ OS Type ⇅

Type	IP/MAC	Device Type	OS Type
<input checked="" type="checkbox"/> IPv4 IP Address	Always On	ANY	ANY

Schedule: Always On

Schritt 22: Klicken Sie auf **Übernehmen**.

Apply Cancel

Schritt 23: (Optional) Um die Konfiguration dauerhaft zu speichern, klicken Sie auf das Symbol **Speichern**.



**Hinweis:** Wenn Sie diese Konfiguration dauerhaft speichern möchten, speichern Sie die aktuelle Konfiguration in der Startkonfiguration.

Sie sollten jetzt die Anwendungssteuerungsfunktion auf Ihrem Router der Serie RV34x erfolgreich konfiguriert haben.

Dieser Artikel enthält außerdem hilfreiche Informationen: [Häufig gestellte Fragen \(FAQs\) zu Routern der Serie RV34x](#)

Diese Seite bietet mehrere Links zu anderen Artikeln, die Sie vielleicht interessant finden: [Produktseite für Router der Serie RV34x](#)

**Sehen Sie sich ein Video zu diesem Artikel an..**

**Klicken Sie hier, um weitere Tech Talks von Cisco anzuzeigen.**