

Toepassingscontrole configureren op de RV34x Series router

Doel

Toepassingscontrole is een extra veiligheidsfunctie op de router die een reeds beveiligd netwerk kan verbeteren, productiviteit op de werkplek kan bevorderen en bandbreedte kan maximaliseren. Toepassingscontrole kan nuttig zijn voor smartphones en andere browser toepassingen. Als u een Wireless Access Point (WAP) aansluit op een router, kan de router verkeer toestaan of ontkennen aan elke host die met WAP is verbonden. Dit ontmoedigt gebruikers op hun beurt om toegang te krijgen tot bepaalde toepassingen.

Dit artikel is bedoeld om u te tonen hoe u Application Control op de RV34x Series routers kunt configureren met behulp van de Application Control Wizard en via de handmatige configuratie.

Toepasselijke apparaten

- RV34x Series

Softwareversie

- 1.0.02.16

Toepassingscontrole instellen

Via de wizard Application Control

Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Configuratiescherm > Wizard Start....**

Stap 2. Klik op de knop **Aan** om *Application Controller* in te schakelen. Deze optie is standaard uitgeschakeld.

Stap 3. Maak een unieke naam voor het beleid in het veld *Beleidsnaam*. Deze naam mag geen spaties of speciale tekens bevatten.

Opmerking: Bijvoorbeeld, *MobileControl* wordt gebruikt.

Stap 4. Klik op **Volgende**.

Stap 5. Klik op de knop **Bewerken** om de parameters en categorieën te definiëren die de

toepassingscontrole voor het filter zal gebruiken.

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

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

3. Schedule

Category ▾ Application ▾ Behavior ▾

Stap 6. Klik op + naast elke categorie om de subcategorieën en specifieke toepassingen uit te vouwen en te bekijken. In plaats hiervan kunt u ook op **Uitvouwen** in het onderste gedeelte van de pagina klikken om alle categorieën en subcategorieën te bekijken.

Opmerking: In dit voorbeeld is *IT-middelen* de uitgebreide categorie.

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
 ▾

Stap 7. Controleer het aanvinkvakje van de categorieën en subcategorieën die u op het beleid wilt toepassen.

Opmerking: Bijvoorbeeld, *Streamingmedia* en *internetcommunicatie* zijn de subcategorieën onder IT-bronnen die als voorbeelden worden gebruikt.

✓ 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

----- ▾

Stap 8. (Optioneel) Klik op de vervolgkeuzelijst naast de toepassing die u op het beleid wilt toepassen. Herhaal deze stap indien nodig. De opties zijn:

- Vergunning & logboek — Gegevens mogen stromen en zijn geregistreerd.
- Vergunning — Gegevens zijn toegestaan.
- Blok — Gegevens zijn geblokkeerd.
- Blok & loggen — Gegevens zijn geblokkeerd en zijn geregistreerd.

Opmerking: Zorg ervoor dat Logging op de router is ingeschakeld door **stysteemconfiguratie** > **Log** te kiezen. Controleer het aanvinkvakje **Inschakelen** en klik vervolgens op **Toepassen**.

✓ 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

Opmerking: Dit voorbeeld wordt *Block* gebruikt voor streaming media.

Stap 9. Klik op **Toepassen**. U wordt terugverwezen naar de tweede pagina van de configuratiewizard.

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

Opmerking: De tabel op de toepassingslijst bevat de geselecteerde categorieën en toepassingen.

✓ 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

Stap 10. Klik op **Next** om naar de Schedule pagina te worden gebracht.

✓ 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

Stap 1. Kies een schema in de vervolgkeuzelijst Schedule, dat u het beleid wilt instellen. De opties kunnen verschillen afhankelijk van eerder gedefinieerde schema's. Om een programma te configureren gaat u naar **Systemconfiguratie > Planningen**. Klik op **Volgende**

- ✓ 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

Opmerking: Bijvoorbeeld, *altijd On* wordt gebruikt.

Stap 12. U wordt naar de overzichtspagina gebracht. De tabel Toepassingsbeleid is nu ingevuld met het beleid dat u hebt ingesteld. Controleer uw instellingen op de overzichtspagina en klik op **Indienen**. U kunt op Terug klikken om uw instellingen te wijzigen.

- ✓ 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

Stap 13. Er wordt een pop-upvenster geopend waaruit blijkt dat uw beleid voor toepassingscontrole is ingesteld. Klik op **OK**.

Success



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

Ok

Stap 14. Om het nieuwe beleid te bekijken, navigeer dan naar **Security > Application Control > Instellingen**.

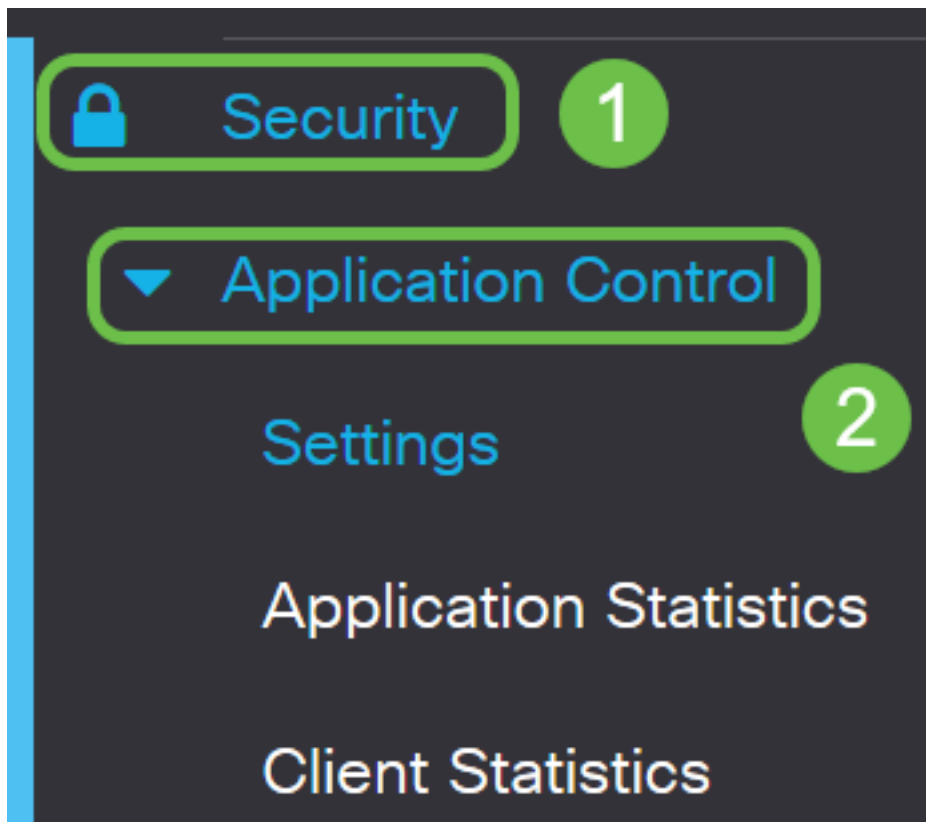
Policy Name	IP Group	Schedule Name	Enable
MobileControl	Any	Always On	<input checked="" type="checkbox"/>

U hebt nu met succes een toepassingsbeheerbeleid ingesteld via de Wizard Application Control.

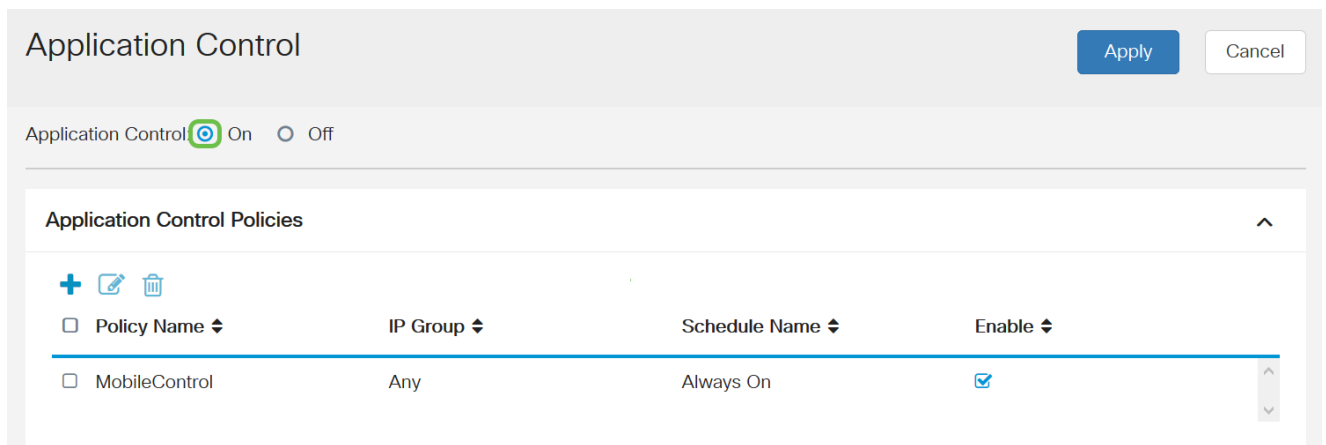
Via de handmatige configuratie

Opmerking: Voor beleid ingesteld door de wizard is dit het gebied waar u uw beleid verder kunt definiëren en aanpassen.

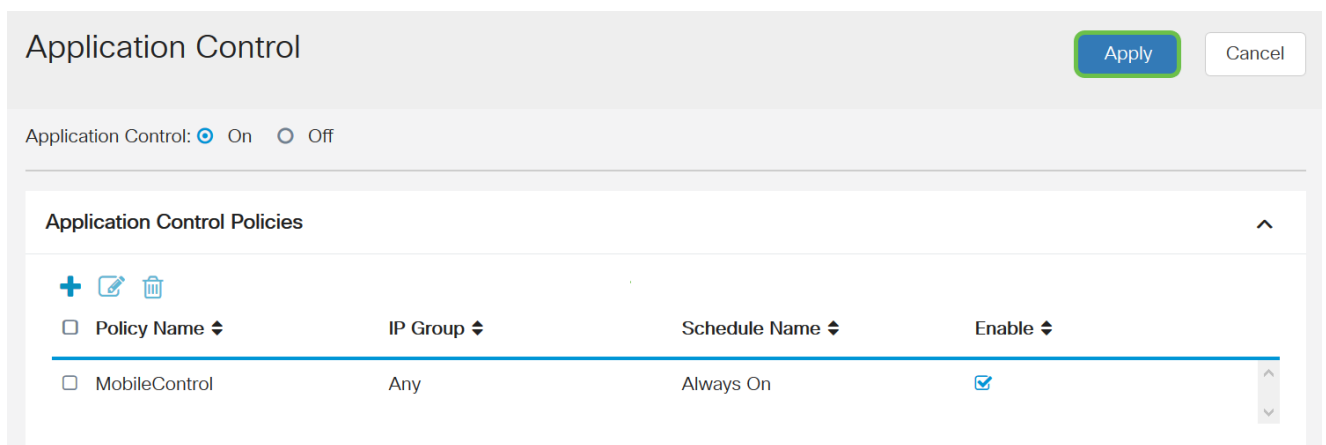
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en kies **Security > Application Control**.



Stap 2. Klik op de radioknop **On** Application Control om de functie Application Control in te schakelen. Deze optie is standaard uitgeschakeld.



Stap. 3 Klik op **Toepassen**.





Stap 4. Klik op **plus**-pictogram in de tabel Toepassingscontrolebeleid om een

toepassingsbeheerbeleid te maken.

Application Control: On Off

Application Control Policies ^

+  

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

Stap 5. Maak een naam voor het beleid. Deze naam mag geen spaties of speciale tekens bevatten.

Opmerking: Voor dit voorbeeld wordt *Sportbeleid* gebruikt.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Stap 6. Voer in het veld *Description* een omschrijving in voor het beleid.

Opmerking: Bijvoorbeeld, *Blokkeer alle Sportkleding*.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Stap 7. Controleer het vakje **Enable** om dit specifieke beleid te activeren.

Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Stap 8. Klik op de knop Toepassing **bewerken** om de parameters te definiëren en af te

stemmen die op het beleid moeten worden toegepast.

Policy Name:

Description:

Enable:

Application: [Edit](#)

Stap 9. Controleer het vakje voor de categorieën en subcategorieën die u op het beleid wilt toepassen.

Policy Profile-Add/Edit Categories

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

Stap 10. Klik op + naast een categorie om de subcategorieën en specifieke toepassingen uit te breiden en te bekijken. In plaats hiervan kunt u ook op **Uitvouwen** in het onderste gedeelte van de pagina klikken om alle categorieën en subcategorieën te bekijken.

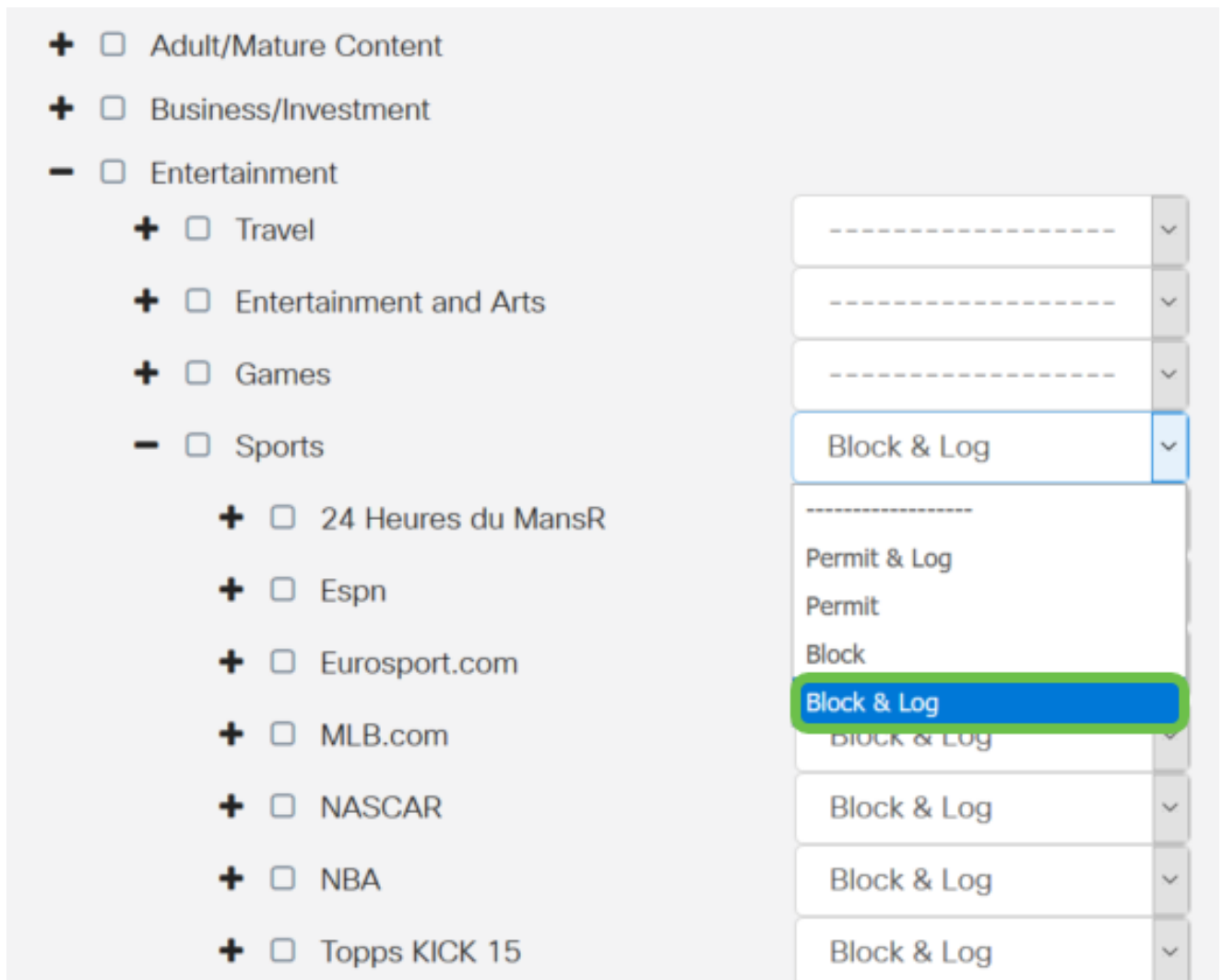
Opmerking: Zo worden bijvoorbeeld *entertainment* en *sport* gekozen.

<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="-----"/> ▾

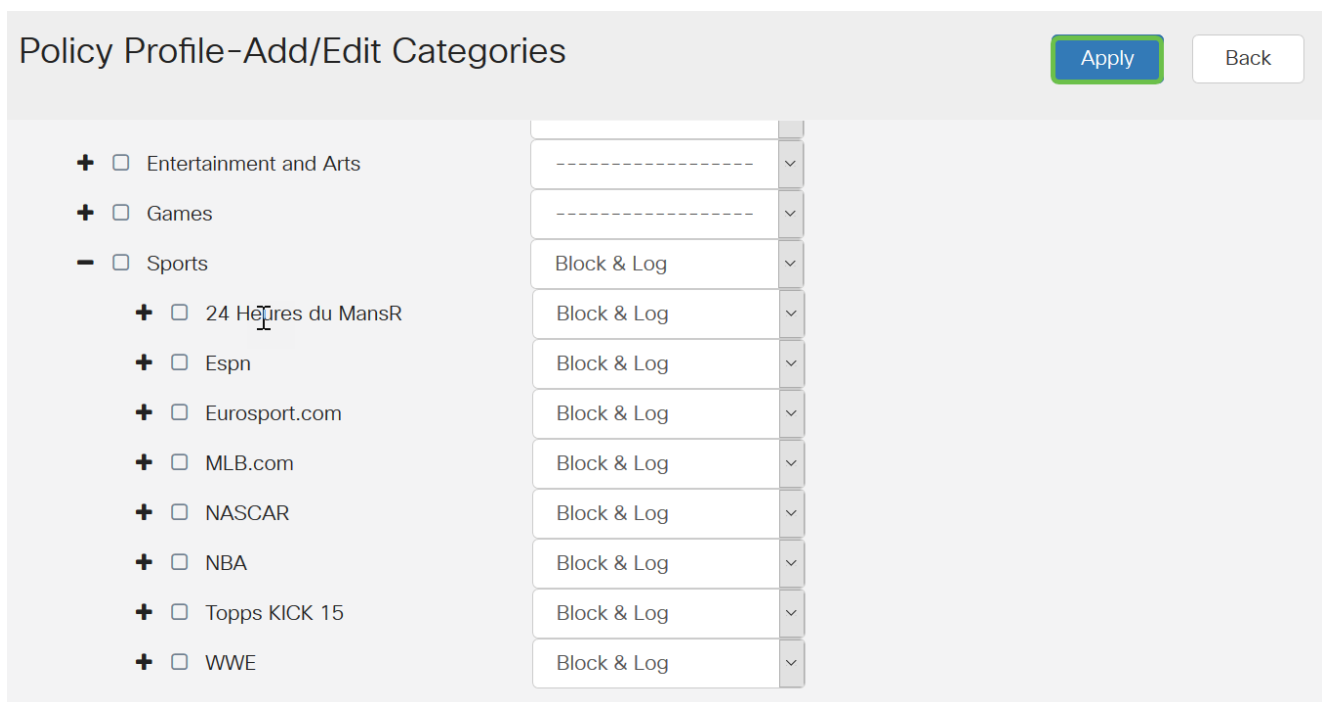
Stap 1. (Optioneel) Klik op de vervolgkeuzelijst naast de toepassing die u op het beleid wilt toepassen. Herhaal deze stap indien nodig. De opties zijn:

- Vergunning & logboek — Gegevens mogen stromen en zijn geregistreerd.
- Vergunning — Gegevens zijn toegestaan.
- Blok — Gegevens zijn geblokkeerd.
- Blok & loggen — Gegevens zijn geblokkeerd en zijn geregistreerd.

Opmerking: In dit voorbeeld wordt *Block & Log* gekozen voor Sportkleding.



Stap 12. De tabel op de toepassingslijst bevat de gekozen categorieën en toepassingen. Klik op **Toepassen**.



Stap 13. Selecteer de bron of bestemming van de pakketten die worden gefilterd in de vervolkeuzelijst Type apparaat. Er kan slechts één optie tegelijkertijd worden gekozen. De opties zijn:

- ALLE — Kies dit om het beleid op elk apparaat toe te passen.
- Camera — Kies dit om het beleid op camera's toe te passen (zoals IP veiligheidscamera's).
- Computer — Kies dit om het beleid op computers toe te passen.
- Game_Console — Kies dit om het beleid toe te passen op Gaming Consoles.
- Media_Player — Kies dit om het beleid op mediaspelers toe te passen.
- Mobiel — Kies dit om het beleid toe te passen op mobiele apparaten.
- VoIP — Kies dit om het beleid toe te passen op Voice over Internet Protocol apparaten.

Opmerking: Hiervoor wordt bijvoorbeeld *EEN* willekeurige keuze geselecteerd.

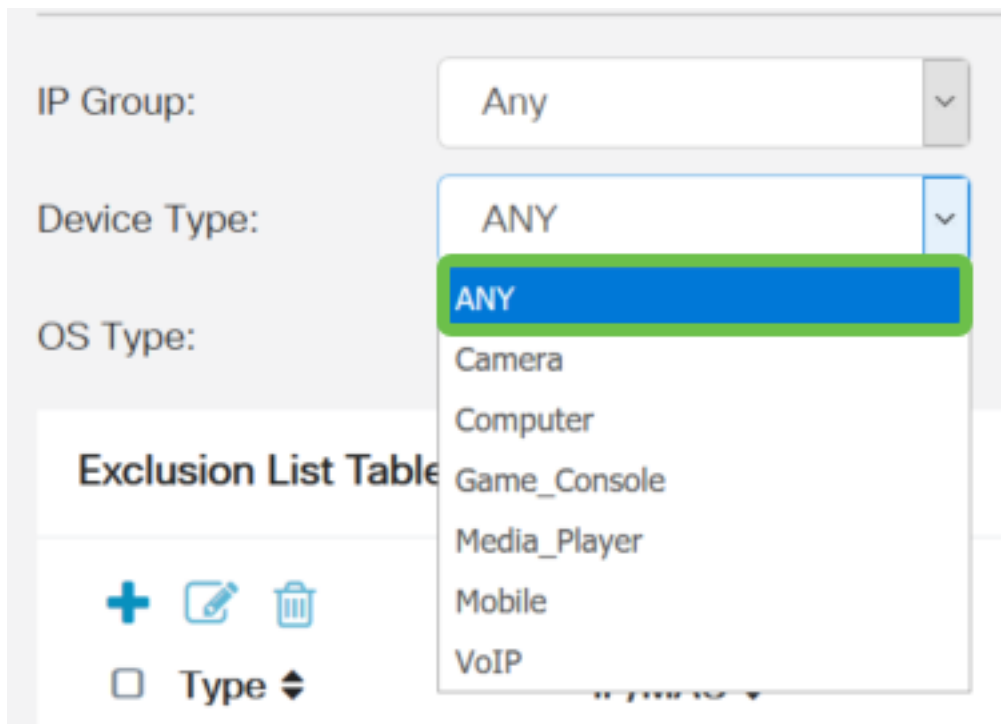
The screenshot shows a configuration panel with the following elements:

- IP Group:** A dropdown menu with 'Any' selected.
- Device Type:** A dropdown menu with 'ANY' selected.
- OS Type:** A dropdown menu with 'ANY' selected and highlighted by a green box. The menu is open, showing options: ANY, Camera, Computer, Game_Console, Media_Player, Mobile, and VoIP.
- Exclusion List Table:** A table with a header and three icons: a plus sign (+), a pencil (edit), and a trash can (delete).
- Type:** A dropdown menu with a plus sign icon and a double-headed arrow.

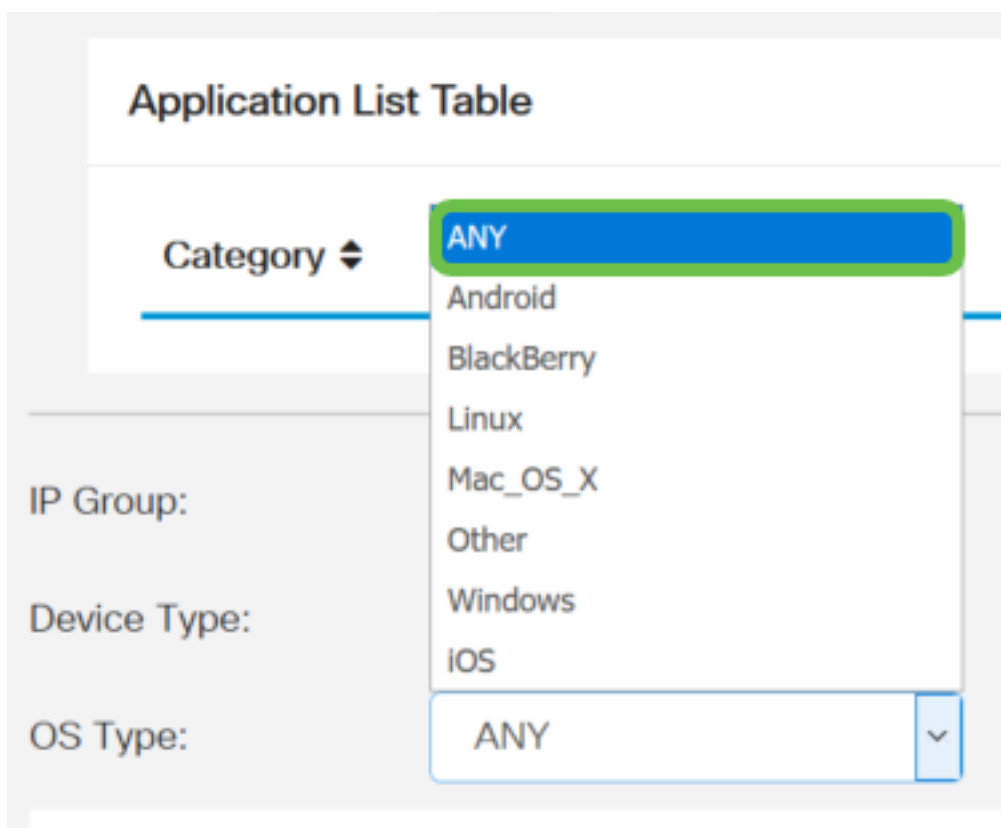
Stap 14. Kies in de vervolgkeuzelijst Type OS een besturingssysteem waarop het beleid van toepassing moet zijn. Er kan slechts één keer worden gekozen. De opties zijn:

- ALLE — past het beleid toe op elk type besturingssysteem. Dit is de standaard.
- Android — past het beleid alleen op Android OS toe.
- BlackBerry — past het beleid alleen toe op Blackberry OS.
- Linux — is alleen van toepassing op Linux OS.
- Mac_OS_X — Past het beleid alleen op Mac OS toe.
- Overige — past het beleid toe op een niet in de lijst opgenomen besturingssysteem.
- Windows — past het beleid op Windows OS toe.
- iOS — Past het beleid alleen op iOS toe.

Opmerking: Hiervoor wordt bijvoorbeeld *EEN* willekeurige keuze geselecteerd.



Stap 15. Kies een IP-groep uit de vervolgkeuzelijst *IP-groepen*. De opties kunnen variëren afhankelijk van de vraag of er al eerder een IP-groep is ingesteld. De standaardinstelling is Any.



Stap 16. (Optioneel) Klik op het pictogram **plus** onder de tabel Uitsluitingslijst om specifieke gebruikers van het beleid uit te sluiten.

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

Stap 17. Kies in de vervolgkeuzelijst Type het adrestype dat van het beleid moet worden uitgesloten. De opties zijn:

- MAC — Specificeer een MAC-adres om van het beleid uit te sluiten.
- IPv4 IP-adres - Specificeer één IPv4-adres om dit beleid uit te sluiten.
- IPv4-bereik — Specificeer een bereik van hosts met IPv4-adressen die van het beleid moeten worden uitgesloten. Voer in de respectievelijke velden een Start IP-adres en een End-IP-adres in.
- IPv6-adres — Specificeer één IPv6-adres dat u buiten het beleid wilt houden.
- IPv6-bereik — Specificeer een bereik van hosts met IPv6-adressen die van het beleid moeten worden uitgesloten. Voer in de respectievelijke velden een Start IP-adres en een End-IP-adres in.

Opmerking: Bijvoorbeeld, *IPv4 Adres* wordt gebruikt.

Exclusion List Table

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

Schedule:

Stap 18. Voer in het veld *IP* een IPv4-adres in.

Opmerking: In dit voorbeeld wordt 192.168.1.114 gebruikt.

Exclusion List Table

<input checked="" type="checkbox"/> Type	IP/MAC	Device Type	OS Type
<input checked="" type="checkbox"/> IPv4 IP Address	192.168.1.114	ANY	ANY

Stap 19. Kies een apparaattype dat van het beleid moet worden uitgesloten.

Opmerking: Hiervoor wordt bijvoorbeeld *EEN* willekeurige keuze geselecteerd.

OS Type: ANY

Exclusion List Table

+ ✎ 🗑

☑ Type ⇅ IP/MAC ⇅ OS Type ⇅

Type	IP/MAC	OS Type
☑ IPv4 IP Address	192.168.1.114	ANY

Stap 20. Kies een OS-type dat van het beleid moet worden uitgesloten.

Opmerking: Hiervoor wordt bijvoorbeeld *EEN* willekeurige keuze geselecteerd.

OS Type: ANY

Exclusion List Table

+ ✎ 🗑

☑ Type ⇅ IP/MAC ⇅ OS Type ⇅

Type	IP/MAC	OS Type
☑ IPv4 IP Address	192.168.1.114	ANY

Stap 21. Kies een schema in de vervolgkeuzelijst Programma dat u wilt instellen. De opties kunnen verschillen afhankelijk van eerder gedefinieerde schema's. Om een programma te configureren gaat u naar **Systeemconfiguratie > Planningen**.

Opmerking: Bijvoorbeeld, *altijd On* wordt gekozen.

Exclusion List Table

+ ✎ 🗑

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

Type	IP/MAC	Device Type	OS Type
☑ IPv4 IP Address		ANY	ANY

Schedule: Always On

Stap 2. Klik op **Toepassen**.

Apply Cancel

Stap 23. (Optioneel) Klik om de configuratie permanent op het pictogram **Opslaan**.

Opmerking: Als u deze configuratie permanent wilt opslaan, dient u de draaiende configuratie dan op te slaan naar de opstartconfiguratie.

U dient nu met succes de Application Control optie op uw RV34x Series router te hebben ingesteld.

Mogelijk vindt u dit artikel ook informatief: [RV34x Series router vaak gestelde vragen \(FAQ's\)](#)

Deze site biedt verschillende links naar andere artikelen die u interessant kunt vinden: [RV34x Series routerpagina](#)

Bekijk een video gerelateerd aan dit artikel...

[Klik hier om andere Tech Talks uit Cisco te bekijken](#)