

# Configurar o controle de aplicativos no roteador RV34x Series

## Objetivo

O controle de aplicativos é um recurso de segurança adicional no roteador que pode aprimorar uma rede já protegida, promover a produtividade no local de trabalho e maximizar a largura de banda. O controle de aplicativos pode ser útil para smartphones e outros aplicativos baseados em navegador. Se você conectar um ponto de acesso sem fio (WAP) a um roteador, o roteador poderá permitir ou negar tráfego para qualquer host conectado ao WAP. Por sua vez, isso desencoraja os usuários a acessarem alguns aplicativos.

O objetivo deste artigo é mostrar a você como configurar o controle de aplicativos nos RV34x Series Routers usando o Application Control Wizard e através da configuração manual.

## Dispositivos aplicáveis

- Série RV34x

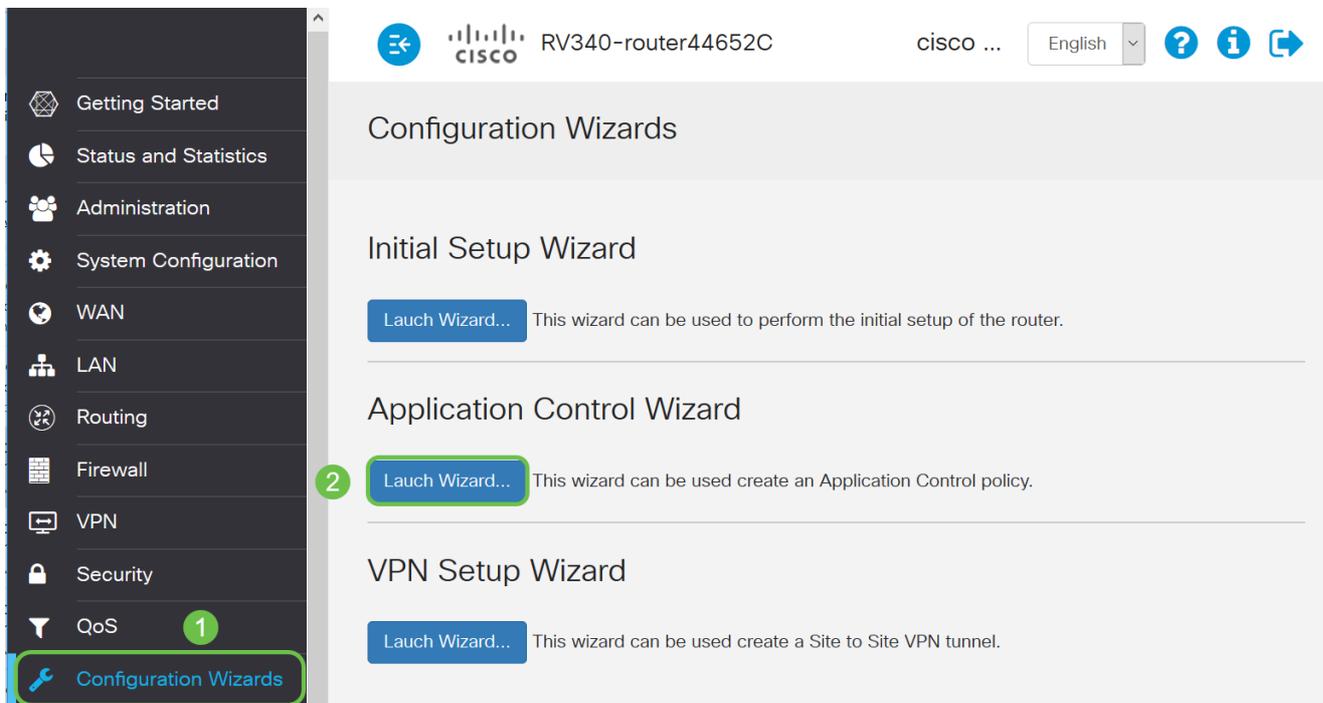
## Versão de software

- 1.0.02.16

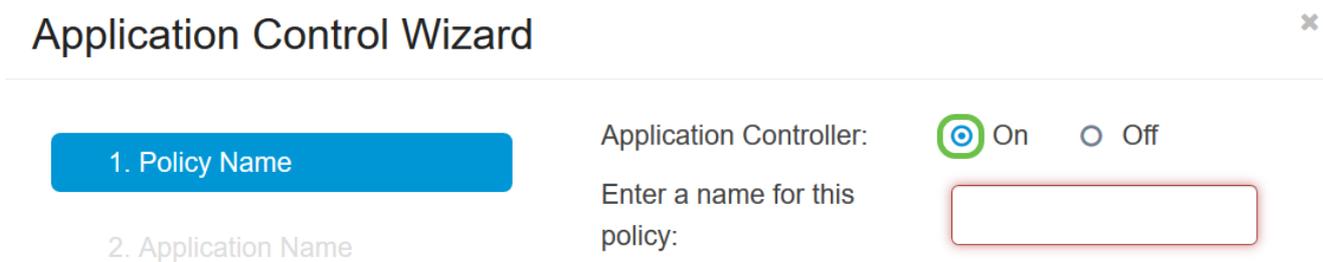
## Configurar controle de aplicativo

### [Através do Assistente de Controle de Aplicativos](#)

Etapa 1. Efetue login no utilitário baseado na Web e escolha **Assistentes de configuração > Iniciar assistente...**

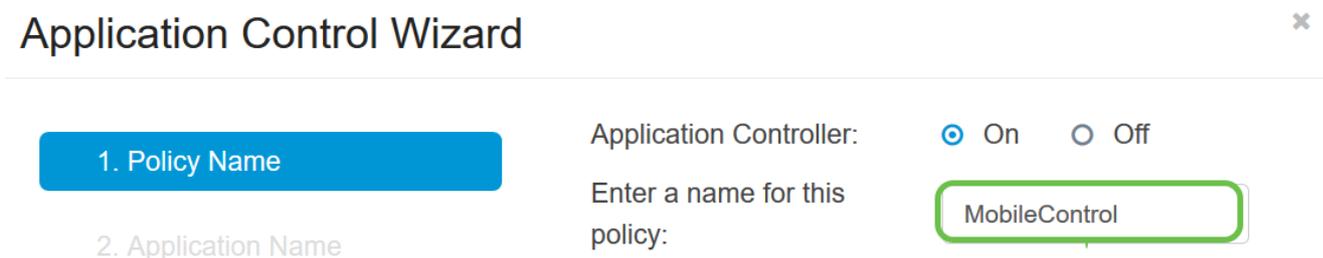


Etapa 2. Clique no botão de opção **On (Ativado)** para habilitar o *Application Controller (Controlador de aplicativo)*. Por padrão, este recurso está desabilitado.



Etapa 3. Crie um nome exclusivo para a política no campo *Nome da política*. Este nome não deve conter espaços ou caracteres especiais.

**Note:** Para este exemplo, é usado *MobileControl*.



Etapa 4. Clique em Next.



Etapa 5. Clique no botão **Editar** para definir os parâmetros e as categorias que o controle de

aplicativo usará para filtrar dados.

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

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

3. Schedule

Category ▾ Application ▾ Behavior ▾

---

Etapa 6. Clique em + ao lado de qualquer categoria para expandir e exibir as subcategorias e os aplicativos específicos. Como alternativa, para visualizar todas as categorias e suas subcategorias, clique em **Expandir** na parte inferior da página.

**Note:** Neste exemplo, *Recursos de TI* é a categoria expandida.

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  
 ▾

Passo 7. Marque a caixa de seleção das categorias e subcategorias que deseja aplicar à política.

**Note:** Para este exemplo, *Streaming Media* e *Internet Communications* são as subcategorias em IT Resources que são usadas como exemplos.

1. Policy Name

2. Application Name

3. Schedule

4. Summary

+  Adult/Mature Content

+  Business/Investment

+  Entertainment

+  Illegal/Questionable

-  IT Resources

+  Streaming Media

----- v

+  Shareware and Freeware

----- v

+  File Hosting / Storage

----- v

+  Web based email

----- v

+  Internet Communications

----- v

Etapa 8. (Opcional) Clique na lista suspensa ao lado do aplicativo que deseja aplicar à diretiva. Repita essa etapa conforme necessário. As opções são:

- Permit & Log - Os dados têm permissão para fluir e estão registrados.
- Permit (Permitir) — Os dados são permitidos.
- Bloquear — Os dados estão bloqueados.
- Bloquear e registrar — os dados estão bloqueados e registrados.

**Note:** Certifique-se de que o registro esteja ativado no roteador escolhendo **System Configuration > Log** (Configuração do sistema > Registro). Marque a caixa de seleção **Habilitar** e clique em **Aplicar**.

1. Policy Name

2. Application Name

3. Schedule

4. Summary

+  Adult/Mature Content

+  Business/Investment

+  Entertainment

+  Illegal/Questionable

-  IT Resources

+  Streaming Media

----- v

Permit & Log

Permit

Block

Block & Log

**Note:** Para este exemplo, *Block* é usado para Streaming Media.

Etapa 9. Clique em Apply. Você será redirecionado de volta para a segunda página do assistente de configuração.

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

**Note:** A tabela Lista de aplicativos é preenchida com as categorias e aplicativos escolhidos.

✓ 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

Etapa 10. Clique em **Avançar** para ir para a página Agendar.

✓ 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

Etapa 11. Na lista suspensa Agendar, escolha uma agenda na qual a política deve ser definida. As opções podem variar de acordo com os agendamentos definidos anteriormente. Para configurar um agendamento, vá para **Configuração do sistema > Agendamentos**.

Clique em Next.

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

**Note:** Para este exemplo, é usado *Always On*.

Etapa 12. Você será levado à página Resumo. A tabela Políticas de controle de aplicativos agora é preenchida com a política configurada. Na página de resumo, revise suas configurações e clique em **Enviar**. Você pode clicar em Voltar para modificar suas configurações.

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

Etapa 13. Será aberta uma janela pop-up que mostra que sua política de controle de

aplicativos foi configurada com êxito. Click **OK**.

# Success



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

Ok

Etapa 14. Para exibir a nova política, navegue para **Segurança > Controle de aplicativo > Configurações**.

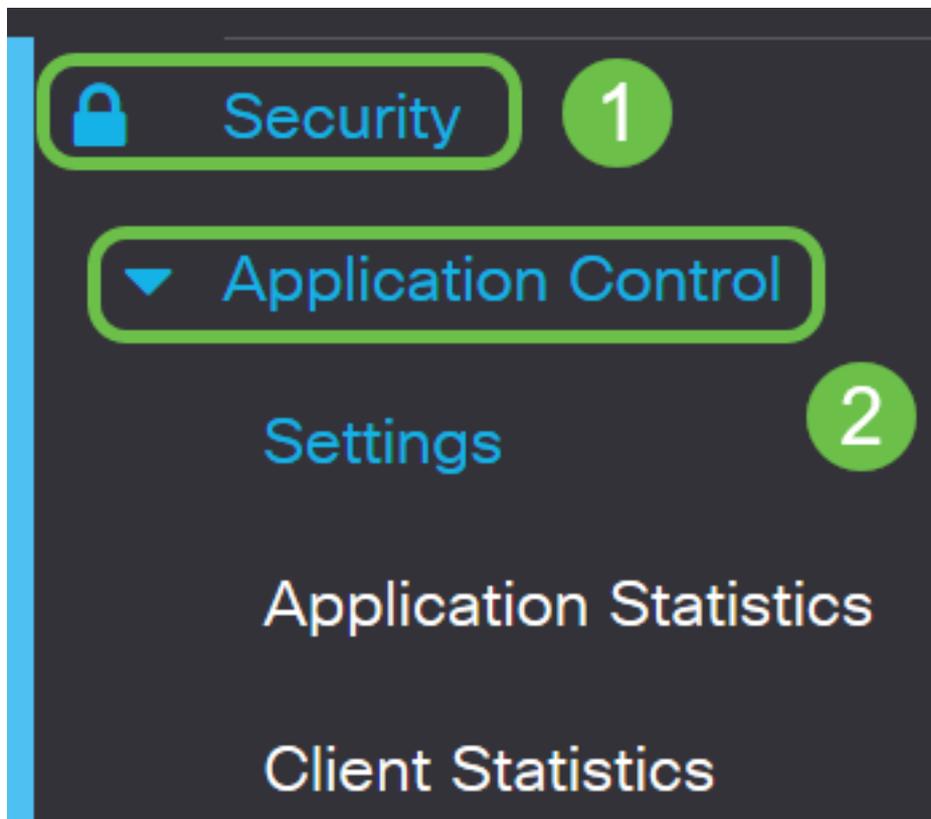
Policy Name	IP Group	Schedule Name	Enable
MobileControl	Any	Always On	<input checked="" type="checkbox"/>

Agora você deve ter configurado com êxito uma política de controle de aplicativos por meio do Assistente de controle de aplicativos.

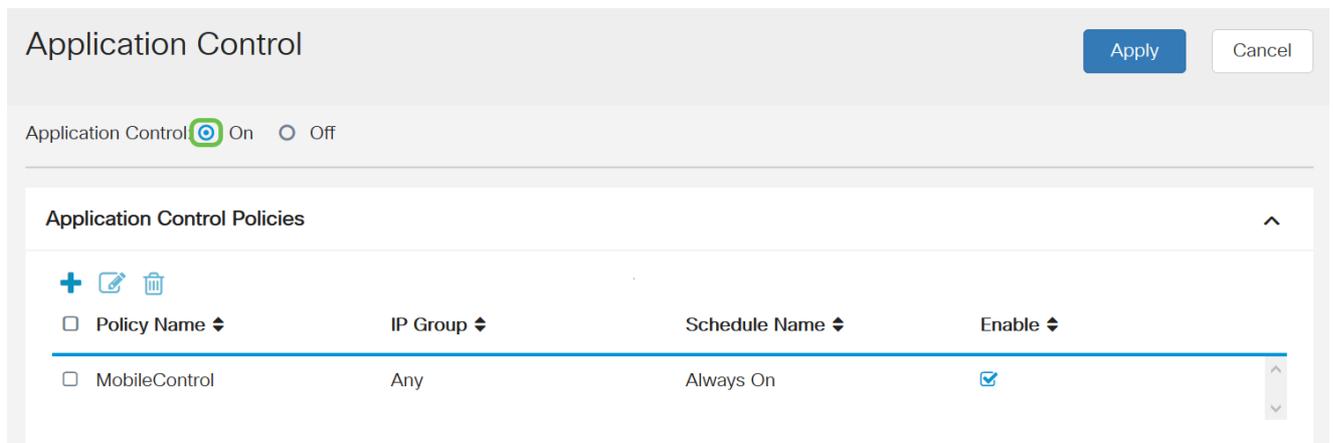
## Através da configuração manual

**Note:** Para políticas configuradas através do assistente, esta é a área onde você pode definir e ajustar suas políticas.

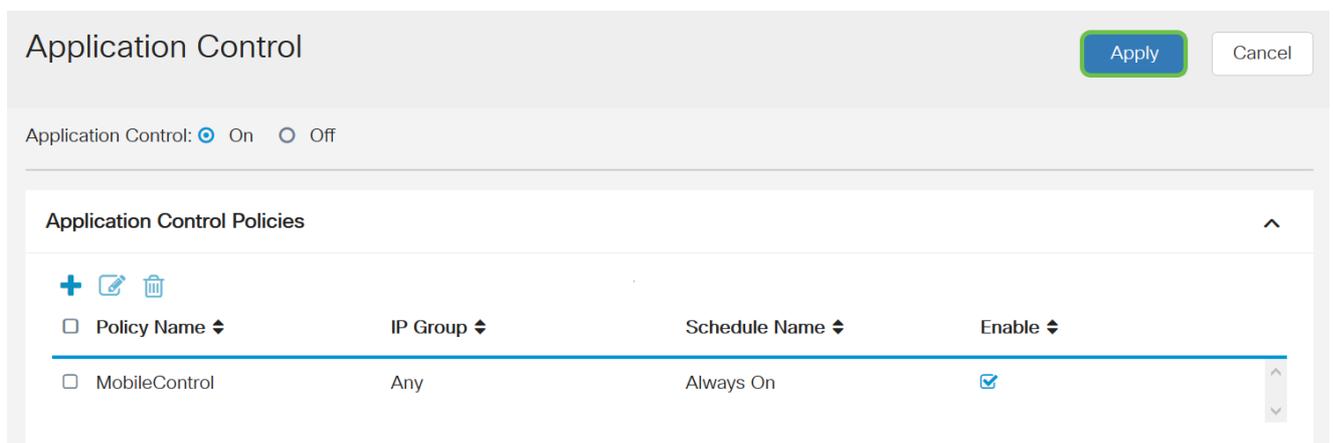
Etapa 1. Faça login no utilitário baseado na Web e escolha **Security > Application Control**.



Etapa 2. Clique no botão de opção **On** Application Control para ativar o recurso Application Control. O recurso é desativado por padrão.

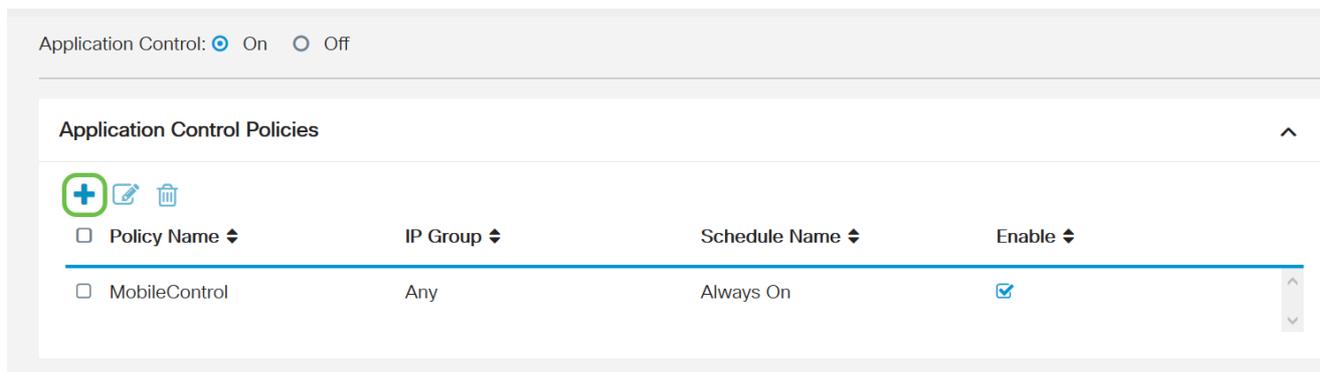


Etapa. 3 Clique em **Apply (Aplicar)**.



Etapa 4. Clique no ícone **mais** na tabela Políticas de controle de aplicativos para criar uma

política de controle de aplicativos.



Etapa 5. Crie um nome para a política. Este nome não deve conter espaços ou caracteres especiais.

**Note:** Para este exemplo, é usado *SportsPolicy*.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

---

Application:

Etapa 6. No campo *Descrição*, crie uma descrição para a política.

**Note:** Para este exemplo, *Bloquear todos os esportes* é usado.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Passo 7. Marque a caixa de seleção **Habilitar** para ativar esta política específica.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Etapa 8. Clique no botão **Editar** aplicativo para definir e ajustar os parâmetros a serem

aplicados à diretiva.

Policy Name:

Description:

Enable:

---

Application: [Edit](#)

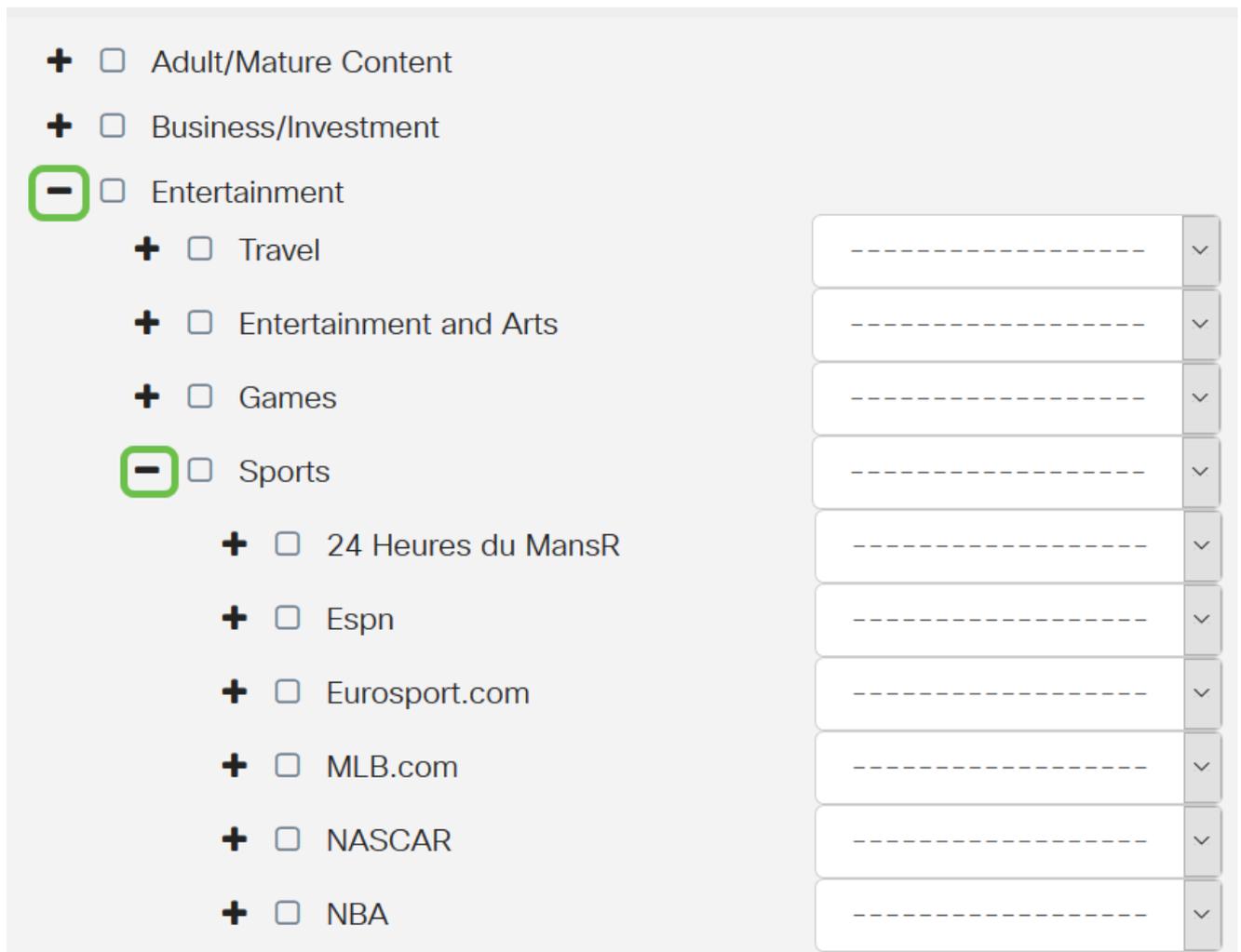
Etapa 9. Marque a caixa de seleção das categorias e subcategorias que deseja aplicar à política.

Policy Profile-Add/Edit Categories

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

Etapa 10. Clique em + ao lado de qualquer categoria para expandir e exibir as subcategorias e os aplicativos específicos. Como alternativa, para visualizar todas as categorias e suas subcategorias, clique em **Expandir** na parte inferior da página.

**Note:** Para este exemplo, são escolhidos *entretenimento* e */esportes*.



Etapa 11. (Opcional) Clique na lista suspensa ao lado do aplicativo que deseja aplicar à diretiva. Repita essa etapa conforme necessário. As opções são:

- Permit & Log - Os dados têm permissão para fluir e estão registrados.
- Permit (Permitir) — Os dados são permitidos.
- Bloquear — Os dados estão bloqueados.
- Bloquear e registrar — os dados estão bloqueados e registrados.

**Note:** Para este exemplo, *Block & Log* é escolhido para Sports.

<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"/> <input type="checkbox"/> Travel	----- ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Entertainment and Arts	----- ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Games	----- ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Sports	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> 24 Heures du MansR	----- Permit & Log
<input checked="" type="checkbox"/> <input type="checkbox"/> Espn	Permit
<input checked="" type="checkbox"/> <input type="checkbox"/> Eurosport.com	Block
<input checked="" type="checkbox"/> <input type="checkbox"/> MLB.com	Block & Log
<input checked="" type="checkbox"/> <input type="checkbox"/> NASCAR	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> NBA	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Topps KICK 15	Block & Log ▾

Etapa 12. A tabela Lista de aplicativos é preenchida com as categorias e aplicativos escolhidos. Clique em Apply.

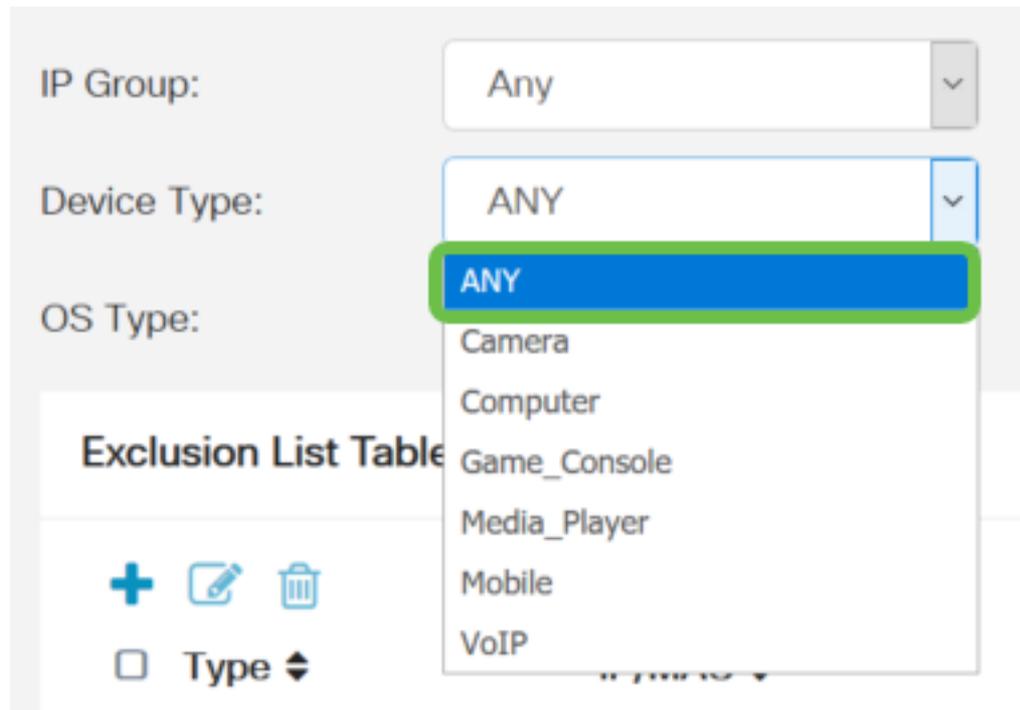
Policy Profile-Add/Edit Categories

<input checked="" type="checkbox"/> <input type="checkbox"/> Entertainment and Arts	----- ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Games	----- ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Sports	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> 24 Heures du MansR	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Espn	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Eurosport.com	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> MLB.com	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> NASCAR	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> NBA	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> Topps KICK 15	Block & Log ▾
<input checked="" type="checkbox"/> <input type="checkbox"/> WWE	Block & Log ▾

Etapa 13. Na lista suspensa Tipo de dispositivo, selecione a origem ou o destino dos pacotes a serem filtrados. Apenas uma opção pode ser escolhida de cada vez. As opções são:

- ANY — Escolha esta opção para aplicar a política a qualquer dispositivo.
- Câmera — Escolha essa opção para aplicar a política às câmeras (como câmeras de segurança IP).
- Computador — Escolha esta opção para aplicar a política aos computadores.
- Game\_Console — Escolha esta opção para aplicar a política aos consoles de jogos.
- Media\_Player — Escolha esta opção para aplicar a política aos Media Players.
- Móvel — Escolha esta opção para aplicar a política aos dispositivos móveis.
- VoIP — Escolha esta opção para aplicar a política aos dispositivos Voice over Internet Protocol .

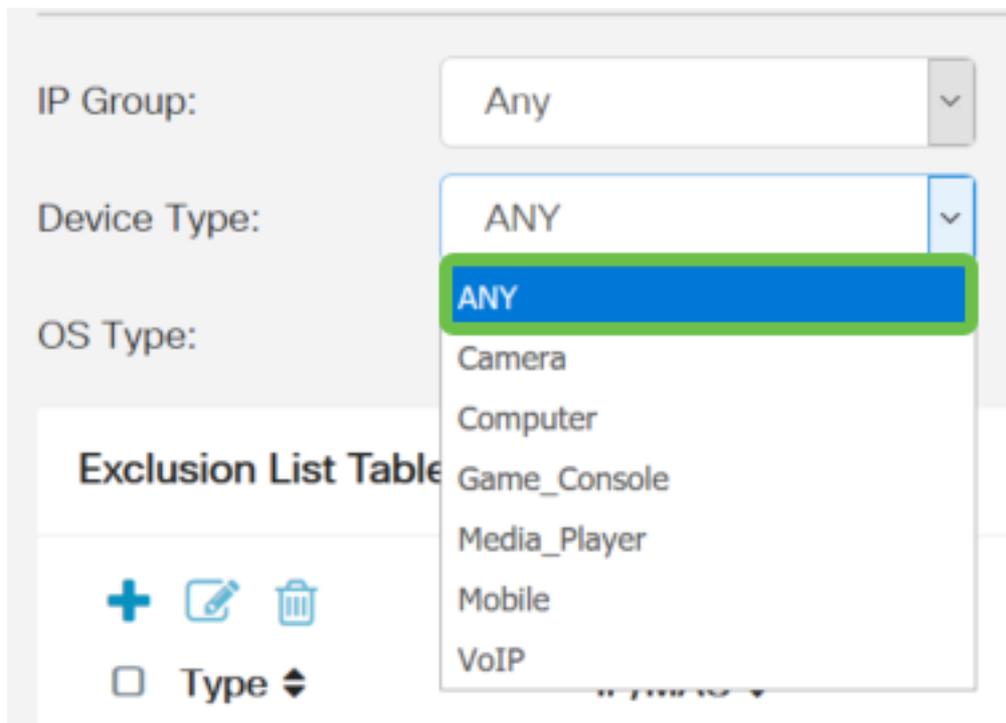
**Note:** Para este exemplo, ANY é escolhida.



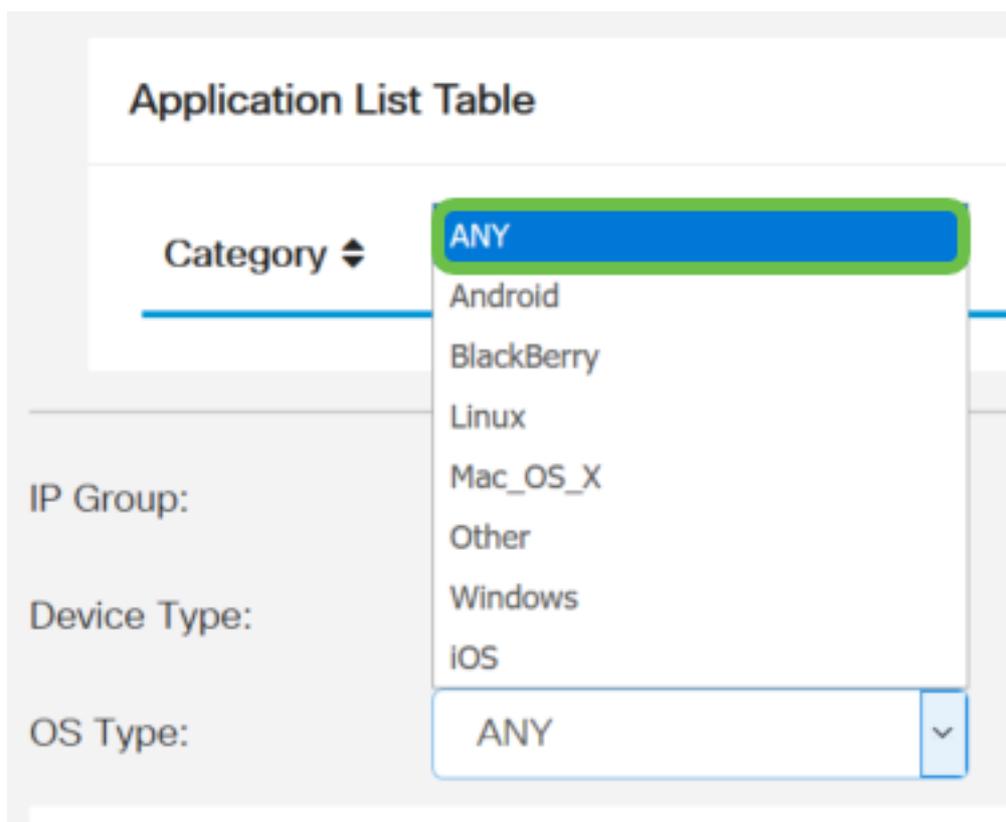
Etapa 14. Na lista suspensa Tipo de SO, escolha um sistema operacional (SO) ao qual a política deve ser aplicável. Apenas um pode ser escolhido de cada vez. As opções são:

- ANY — Aplica a política a qualquer tipo de SO. Esse é o padrão.
- Android — Aplica a política somente ao sistema operacional Android.
- BlackBerry — Aplica a política somente ao Blackberry OS.
- Linux — Aplica a política somente ao sistema operacional Linux.
- Mac\_OS\_X — Aplica a política somente ao Mac OS.
- Outro — Aplica a política a um SO que não está listado.
- Windows — Aplica a política ao sistema operacional Windows.
- iOS — Aplica a política somente ao iOS OS.

**Note:** Para este exemplo, ANY é escolhida.

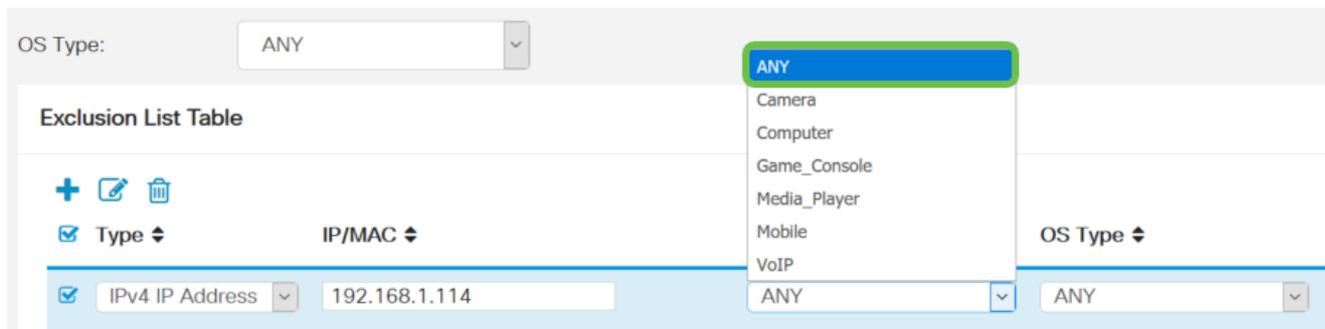


Etapa 15. Escolha um grupo IP na lista suspensa *Grupos IP*. As opções podem variar dependendo se algum grupo IP tiver sido configurado anteriormente. O padrão é Qualquer.



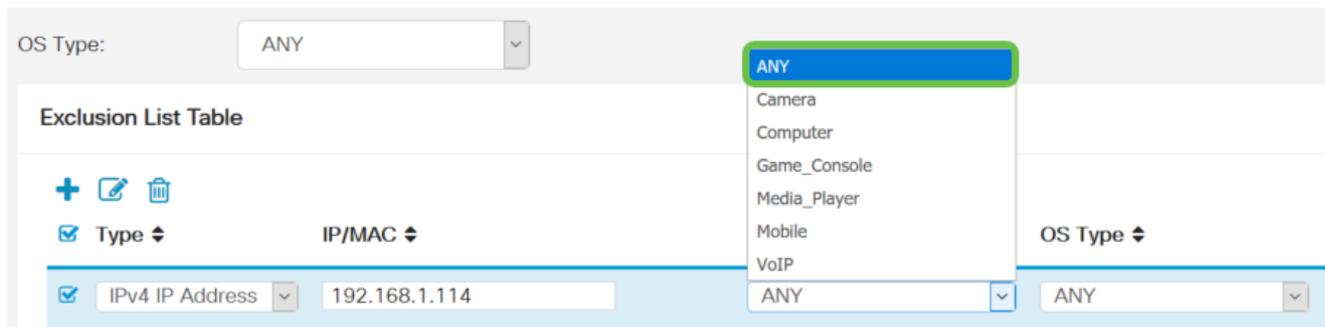
Etapa 16. (Opcional) Clique no ícone **de mais** na Tabela Lista de exclusões para excluir usuários específicos da política.





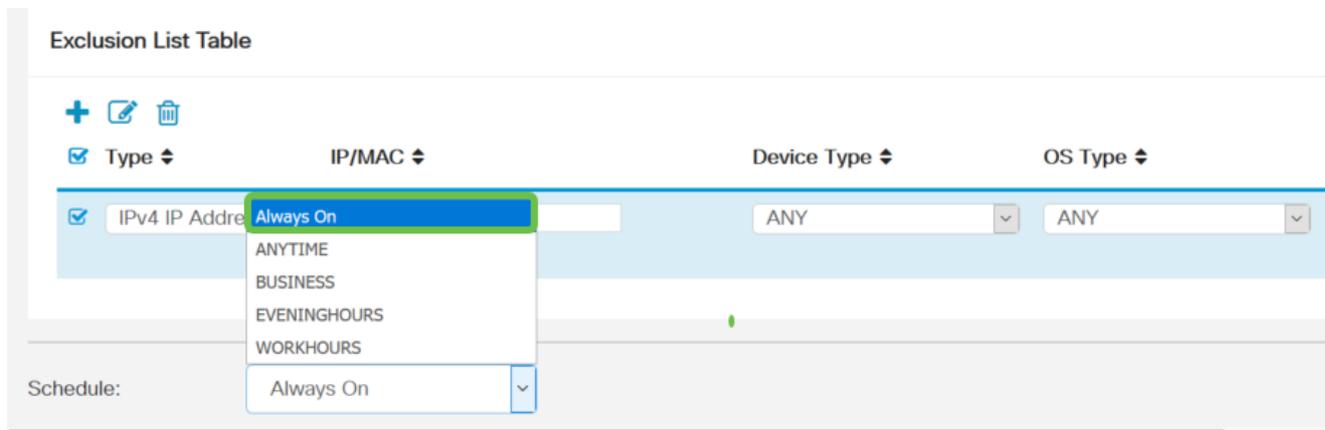
Etapa 20. Escolha um tipo de SO a ser excluído da política.

**Note:** Para este exemplo, *ANY* é escolhida.

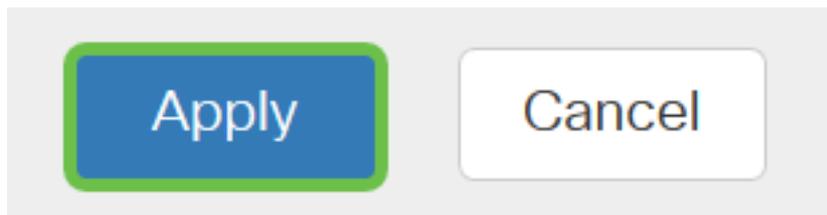


Etapa 21. Na lista suspensa Agendar, escolha uma agenda na qual a política deve ser definida. As opções podem variar de acordo com os agendamentos definidos anteriormente. Para configurar um agendamento, vá para **Configuração do sistema > Agendamentos**.

**Note:** Para este exemplo, *Always On* é Escolhido.



Etapa 22. Clique em Apply.



Etapa 23. (Opcional) Para salvar a configuração permanentemente, clique no ícone **Salvar**.

**Note:** Se você quiser salvar permanentemente essa configuração, salve a configuração atual na configuração de inicialização.

Agora você deve ter configurado com êxito o recurso de controle de aplicativos no RV34x Series Router.

Você também pode encontrar este artigo informativo: [Perguntas frequentes \(FAQs\) sobre o roteador RV34x Series](#)

Este site oferece vários links para outros artigos que você pode achar interessantes: [Página de produto do roteador RV34x Series](#)

## Exibir um vídeo relacionado a este artigo...

[Clique aqui para ver outras palestras técnicas da Cisco](#)