

# Configuración del control de aplicaciones en el router serie RV34x

## Objetivo

El control de aplicaciones es una función de seguridad adicional en el router que puede mejorar una red ya segura, promover la productividad en el lugar de trabajo y maximizar el ancho de banda. El control de aplicaciones puede ser útil para smartphones y otras aplicaciones basadas en navegador. Si conecta un punto de acceso inalámbrico (WAP) a un router, el router podrá permitir o denegar el tráfico a cualquier host conectado al WAP. A su vez, esto disuade a los usuarios de acceder a algunas aplicaciones.

En este artículo se explica cómo configurar el control de aplicaciones en los routers de la serie RV34x mediante el Asistente de control de aplicaciones y la configuración manual.

## Dispositivos aplicables

- Serie RV34x

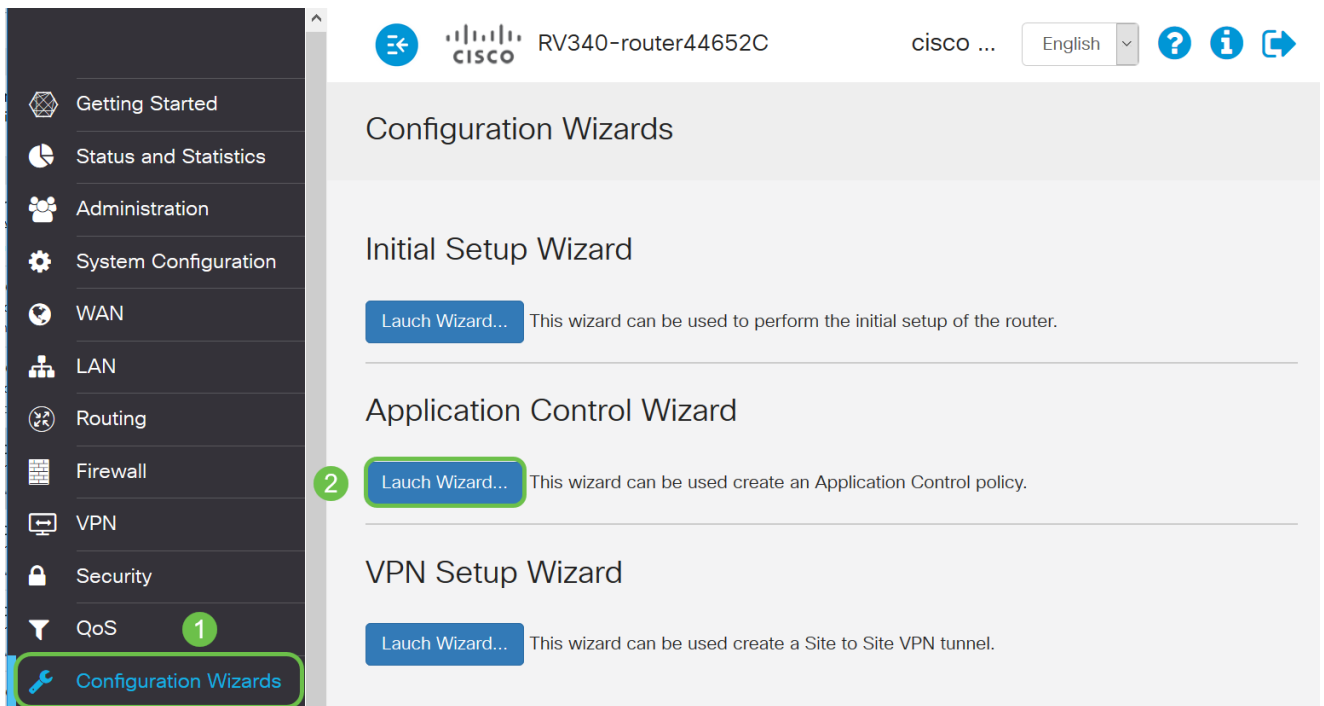
## Versión del software

- 1.0.02.16

## Configurar el control de aplicaciones

### Mediante el Asistente de control de aplicaciones

Paso 1. Inicie sesión en la utilidad basada en Web y elija **Asistente para configuración > Asistente para inicio....**



Paso 2. Haga clic en el botón de opción **On** para habilitar *Application Controller*. Esta función está desactivada de forma predeterminada.

## Application Control Wizard

1. Policy Name

2. Application Name

Application Controller:  On  Off

Enter a name for this policy:

Paso 3. Cree un nombre único para la política en el campo *Policy Name*. Este nombre no debe contener espacios ni caracteres especiales.

**Nota:** Para este ejemplo, se utiliza *MobileControl*.

## Application Control Wizard

1. Policy Name

2. Application Name

Application Controller:  On  Off

Enter a name for this policy:

Paso 4. Haga clic en Next (Siguiete).

Next

Cancel

Paso 5. Haga clic en el botón **Edit** para definir los parámetros y categorías que utilizará el

control de aplicación para filtrar los datos.

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

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

3. Schedule

Category ▾ Application ▾ Behavior ▾

Paso 6. Haga clic en el signo + junto a cualquier categoría para expandir y ver las subcategorías y aplicaciones específicas. Alternativamente, para ver todas las categorías y sus subcategorías, haga clic en **Expandir** en la parte inferior de la página.

**Nota:** En este ejemplo, *IT Resources* es la categoría ampliada.

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  
 ▾

Paso 7. Active la casilla de verificación de las categorías y subcategorías que desea aplicar a la directiva.

**Nota:** Para este ejemplo, *Streaming Media* y *Internet Communications* son las subcategorías de Recursos de TI que se utilizan como ejemplos.

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

Paso 8. (Opcional) Haga clic en la lista desplegable junto a la aplicación que desea aplicar a la política. Repita este paso según sea necesario. Las opciones son:

- Permiso y registro: los datos pueden fluir y se registran.
- Permiso: los datos están permitidos.
- Block (Bloquear): los datos están bloqueados.
- Block & Log (Bloquear y registrar): los datos están bloqueados y registrados.

**Nota:** Asegúrese de que el registro esté habilitado en el router eligiendo **Configuración del sistema > Registro**. Marque la casilla de verificación **Enable** y, a continuación, haga clic en **Apply**.

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

Shareware and Freeware

File Hosting / Storage

**Nota:** Para este ejemplo, *Block* se utiliza para Streaming Media.

Paso 9. Haga clic en Apply (Aplicar). Se le redirigirá de nuevo a la segunda página del asistente de configuración.

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:** La tabla de lista de aplicaciones se rellena con las categorías y aplicaciones seleccionadas.

✓ 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

Paso 10. Haga clic en **Siguiente** para ir a la página Programación.

✓ 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

Paso 11. En la lista desplegable Programación, elija una programación que deba establecer la política. Las opciones pueden variar según las programaciones definidas previamente. Para configurar una programación, vaya a **Configuración del sistema > Programaciones**.

Haga clic en Next (Siguiente).

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

**Nota:** Para este ejemplo, se utiliza *Always On*.

Paso 12. Accederá a la página Resumen. La tabla Políticas de control de aplicaciones se rellena ahora con la política que ha configurado. En la página de resumen, revise los parámetros y haga clic en **Enviar**. Puede volver a hacer clic para modificar los parámetros.

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

Paso 13. Se abrirá una ventana emergente que muestra que la política de control de aplicaciones se ha configurado correctamente. Click OK.

# Success



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

Ok

Paso 14. Para ver la nueva directiva, vaya a **Seguridad > Control de aplicaciones > Configuración**.

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

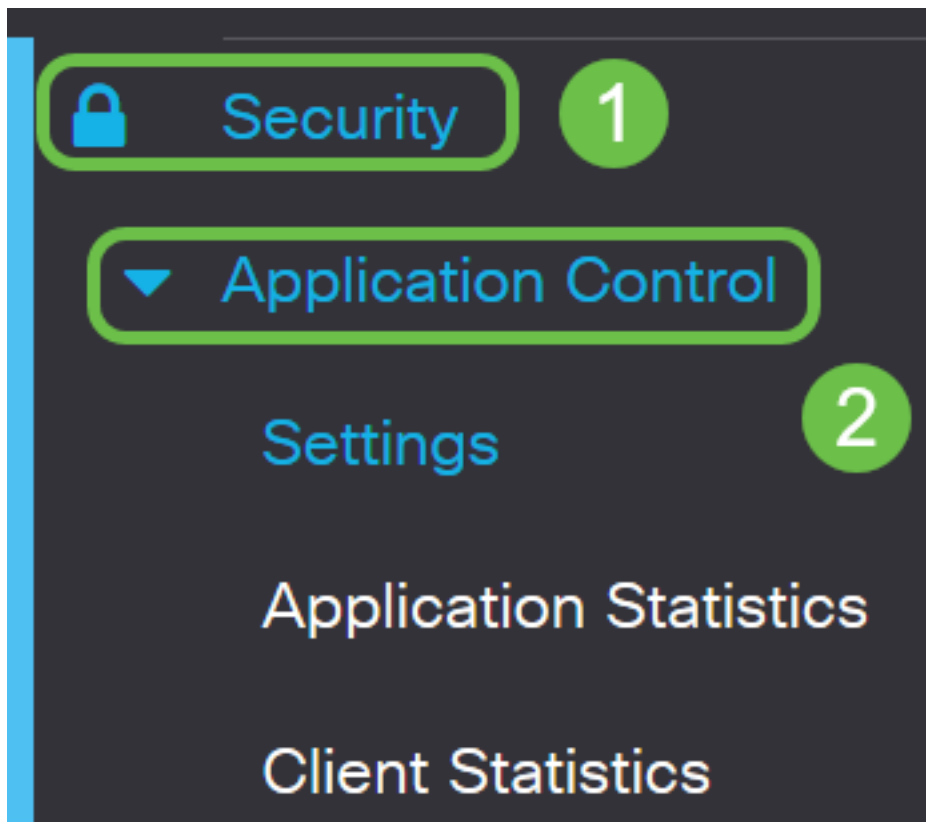
Ahora debería haber configurado correctamente una política de control de aplicaciones a través del Asistente de control de aplicaciones.

## Mediante la configuración manual

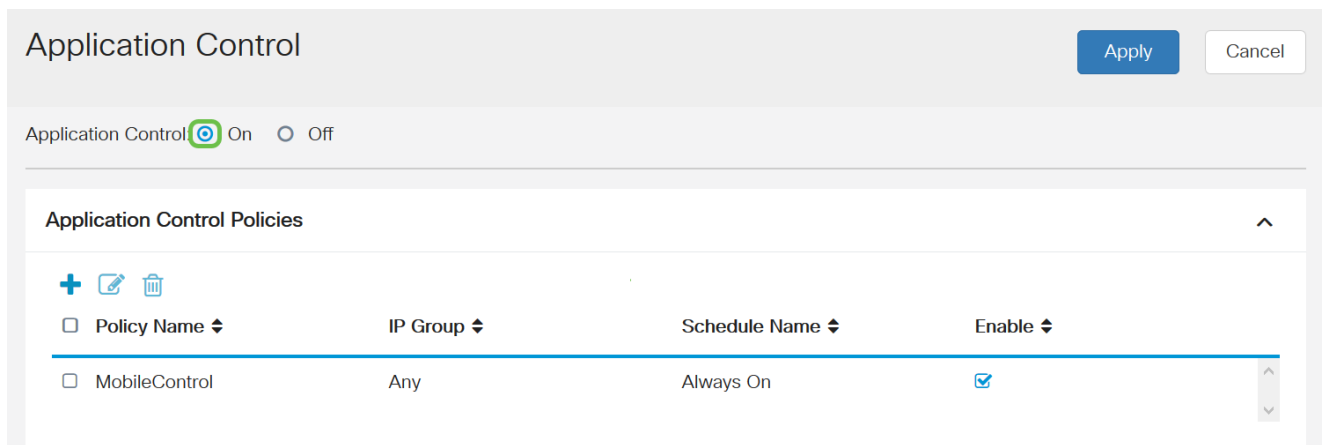
**Nota:** En el caso de las políticas configuradas a través del asistente, este es el área en la que puede definir y ajustar más las políticas.

Paso 1. Inicie sesión en la utilidad basada en Web y elija **Security > Application Control**.

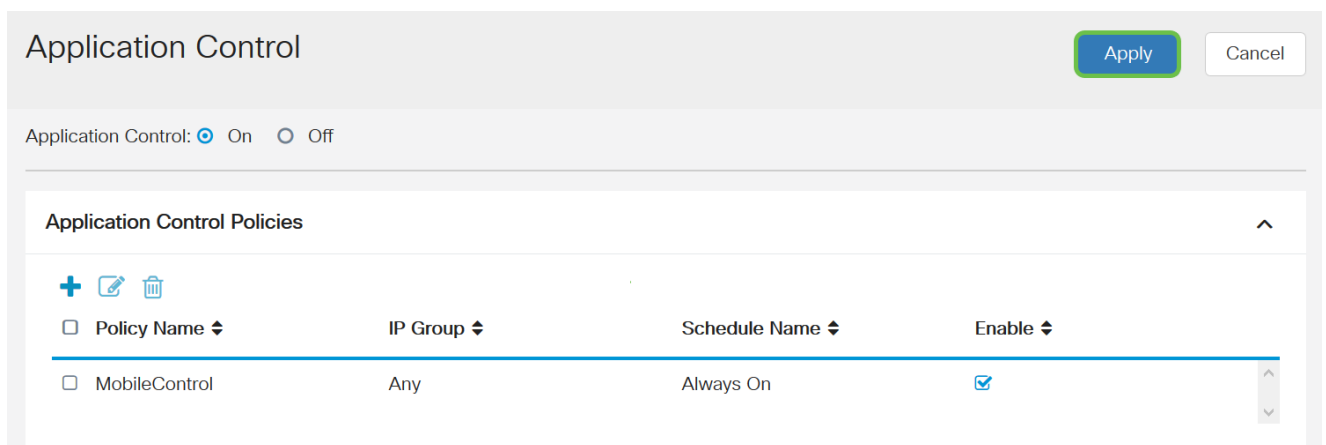




Paso 2. Haga clic en el botón de opción **On** Application Control para habilitar la función Application Control. La función está desactivada de forma predeterminada.



Paso. 3 Haga clic en **Aplicar**.






Paso 4. Haga clic en el icono **más** en la tabla Políticas de control de aplicaciones para crear

una política de control de aplicaciones.

Application Control:  On  Off

---

Application Control Policies ^

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

Paso 5. Cree un nombre para la directiva. Este nombre no debe contener espacios ni caracteres especiales.

**Nota:** Para este ejemplo, se utiliza *SportsPolicy*.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

---

Application:

Paso 6. En el campo *Descripción*, cree una descripción para la política.

**Nota:** Para este ejemplo, se utiliza *Block all Sports*.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Paso 7. Marque la casilla de verificación **Enable** para activar esta política específica.

## Policy Profile-Add/Edit

Policy Name:

Description:

Enable:

Application:

Paso 8. Haga clic en el botón **Editar** aplicación para definir y ajustar los parámetros que se

aplicarán a la política.

Policy Name:

Description:

Enable:

---

Application: [Edit](#)

Paso 9. Active la casilla de verificación de las categorías y subcategorías que desea aplicar a la directiva.

Policy Profile-Add/Edit Categories

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

Paso 10. Haga clic en + junto a cualquier categoría para expandir y ver las subcategorías y aplicaciones específicas. Alternativamente, para ver todas las categorías y sus subcategorías, haga clic en **Expandir** en la parte inferior de la página.

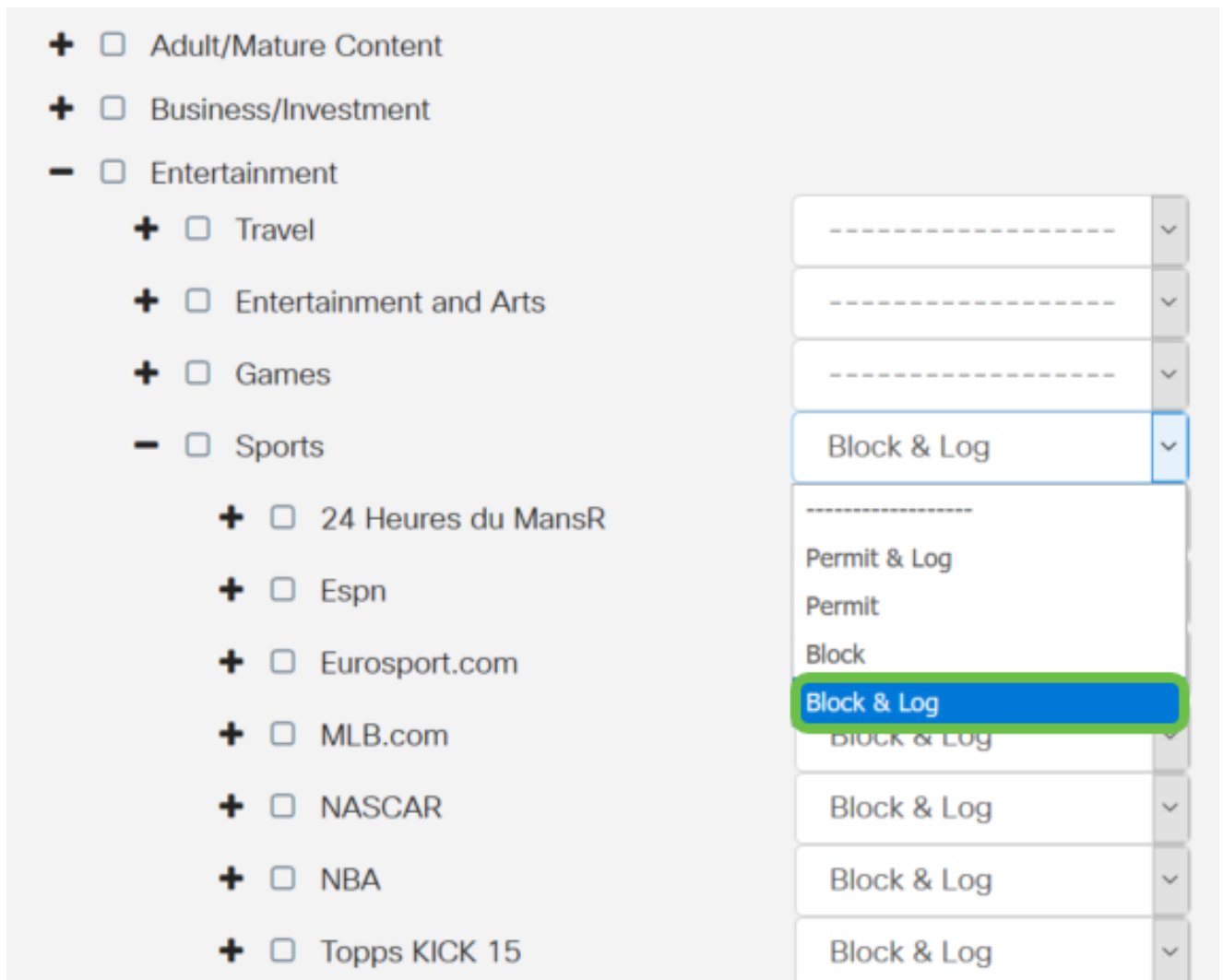
**Nota:** Para este ejemplo, se *eligen* entretenimiento y deportes.

<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="-----"/> ▾

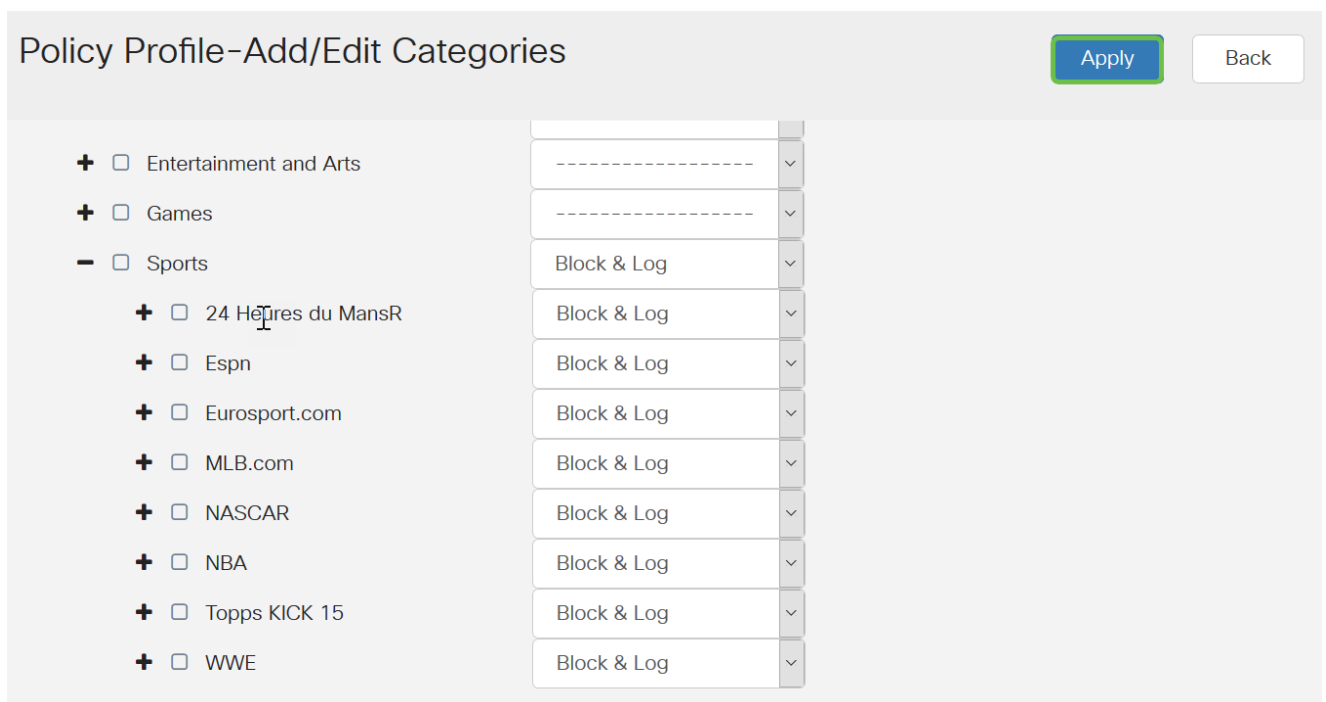
Paso 11. (Opcional) Haga clic en la lista desplegable junto a la aplicación que desea aplicar a la política. Repita este paso según sea necesario. Las opciones son:

- Permiso y registro: los datos pueden fluir y se registran.
- Permiso: los datos están permitidos.
- Block (Bloquear): los datos están bloqueados.
- Block & Log (Bloquear y registrar): los datos están bloqueados y registrados.

**Nota:** Para este ejemplo, *Block & Log* se elige para Sports.



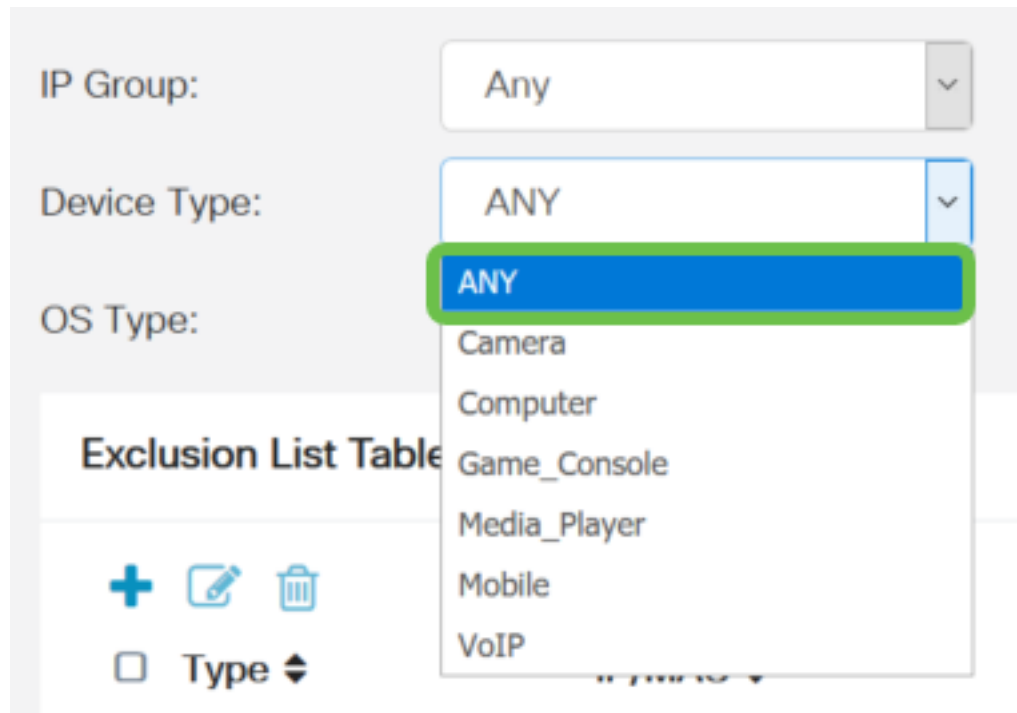
Paso 12. La tabla de lista de aplicaciones se rellena con las categorías y aplicaciones seleccionadas. Haga clic en Apply (Aplicar).



Paso 13. En la lista desplegable Tipo de dispositivo, seleccione el origen o el destino de los paquetes que se filtrarán. Solo se puede seleccionar una opción cada vez. Las opciones son:

- ANY: elija esta opción para aplicar la política a cualquier dispositivo.
- Cámara: seleccione esta opción para aplicar la política a las cámaras (como las cámaras de seguridad IP).
- Equipo: seleccione esta opción para aplicar la directiva a los equipos.
- Game\_Console: elija esta opción para aplicar la política a las consolas de juegos.
- Media\_Player: seleccione esta opción para aplicar la política a los reproductores multimedia.
- Móvil: seleccione esta opción para aplicar la política a los dispositivos móviles.
- VoIP: seleccione esta opción para aplicar la política a los dispositivos del protocolo de voz sobre Internet .

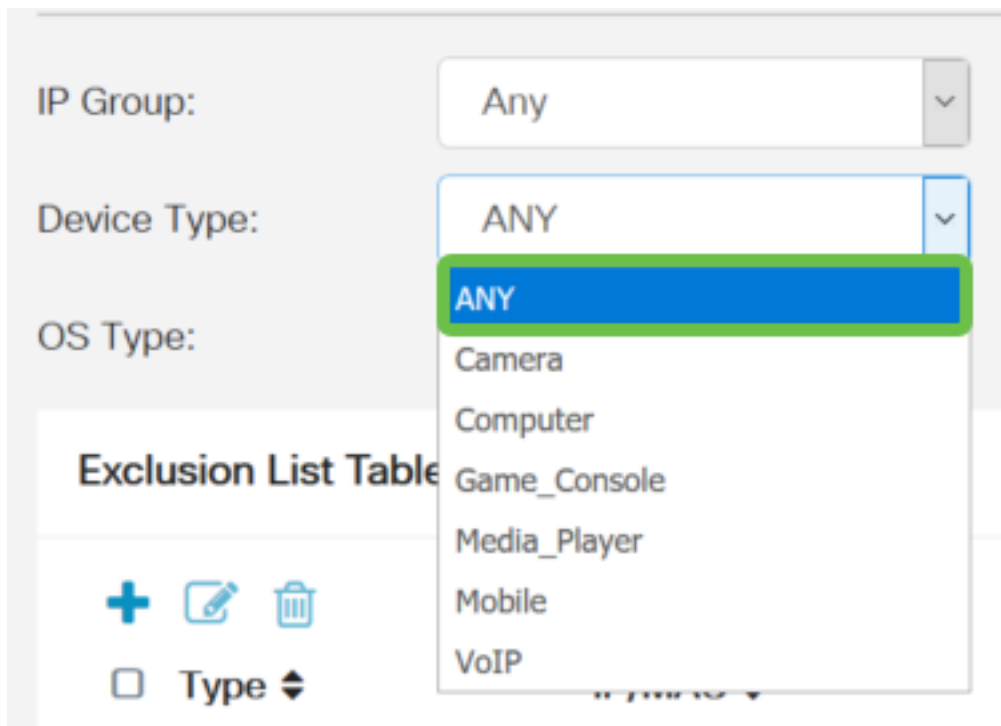
**Nota:** Para este ejemplo, se elige ANY.



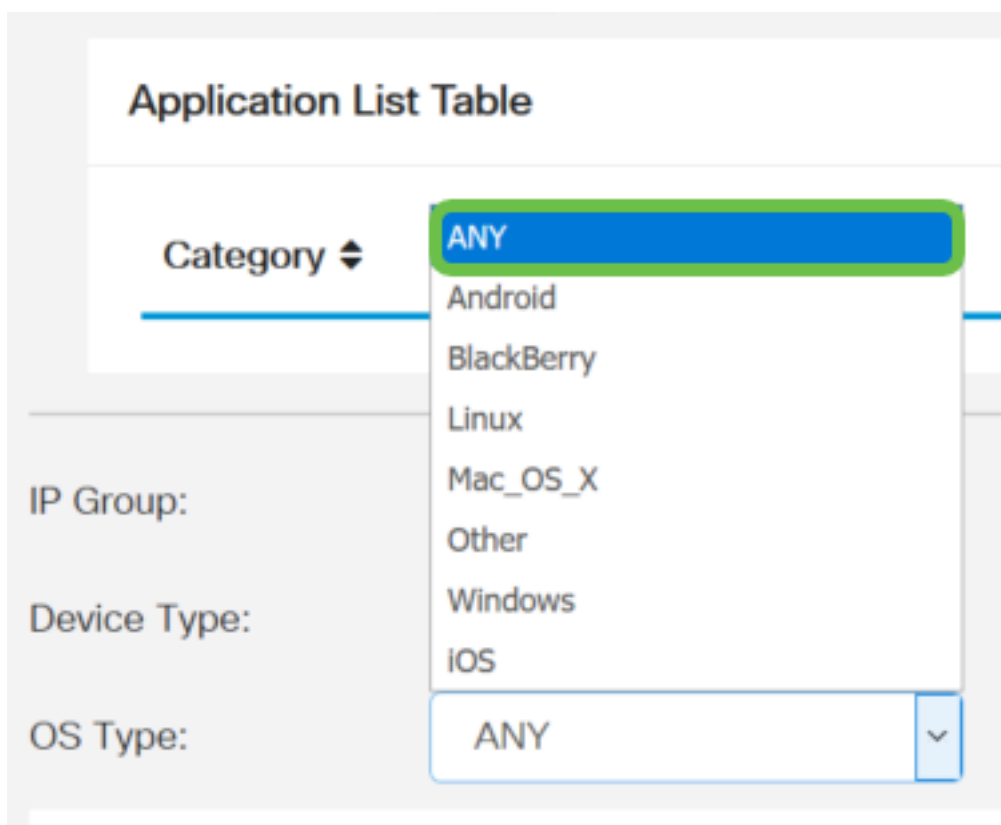
Paso 14. En la lista desplegable Tipo de sistema operativo, elija un sistema operativo (OS) al que deba aplicarse la política. Sólo se puede elegir uno a la vez. Las opciones son:

- ANY: aplica la política a cualquier tipo de sistema operativo. Este es el valor predeterminado.
- Android: aplica la política únicamente al sistema operativo Android.
- BlackBerry: aplica la política únicamente al sistema operativo Blackberry.
- Linux: aplica la política sólo al sistema operativo Linux.
- Mac\_OS\_X: aplica la política sólo al sistema operativo Mac.
- Otro: aplica la política a un SO que no aparece en la lista.
- Windows: aplica la directiva al sistema operativo Windows.
- iOS: aplica la política sólo al sistema operativo iOS.

**Nota:** Para este ejemplo, se elige ANY.



Paso 15. Elija un grupo IP de la lista desplegable *Grupos IP*. Las opciones pueden variar dependiendo de si se ha configurado previamente algún grupo IP. El valor predeterminado es Any (Cualquiera).



Paso 16. (Opcional) Haga clic en el icono **más** bajo la tabla de lista de exclusión para excluir usuarios específicos de la política.



IP Group:

Device Type:

OS Type:

**Exclusion List Table**

+ ✎ 🗑

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

Paso 17. En la lista desplegable Tipo, elija el tipo de dirección que se excluirá de la política. Las opciones son:

- MAC: especifique una dirección MAC para excluir de la política.
- Dirección IPv4: especifique una única dirección IPv4 que se excluya de la política.
- IPv4 IP Range: especifique un rango de hosts de direcciones IPv4 que se excluirán de la política. Introduzca una dirección IP inicial y una dirección IP final en los campos correspondientes.
- IPv6 IP Address: especifique una única dirección IPv6 para excluir de la política.
- IPv6 IP Range: especifique un rango de hosts de direcciones IPv6 que se excluirán de la política. Introduzca una dirección IP inicial y una dirección IP final en los campos correspondientes.

**Nota:** Para este ejemplo, se utiliza *IPv4 IP Address*.

**Exclusion List Table**

+ ✎ 🗑

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

Schedule:

Paso 18. Introduzca una dirección IPv4 en el campo *IP*.

**Nota:** En este ejemplo, se utiliza 192.168.1.114.

**Exclusion List Table**

+ ✎ 🗑

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

Paso 19. Elija un tipo de dispositivo que se excluirá de la política.

**Nota:** Para este ejemplo, se elige ANY.

OS Type: ANY

Exclusion List Table

+ ✎ 🗑

Type IP/MAC OS Type

IPv4 IP Address 192.168.1.114 ANY ANY

Paso 20. Elija un tipo de sistema operativo que se excluirá de la política.

**Nota:** Para este ejemplo, se elige ANY.

OS Type: ANY

Exclusion List Table

+ ✎ 🗑

Type IP/MAC OS Type

IPv4 IP Address 192.168.1.114 ANY ANY

Paso 21. En la lista desplegable Programación, elija una programación que deba establecer la política. Las opciones pueden variar según las programaciones definidas previamente. Para configurar una programación, vaya a **Configuración del sistema > Programaciones**.

**Nota:** Para este ejemplo, se elige *Always On*.

Exclusion List Table

+ ✎ 🗑

Type IP/MAC Device Type OS Type

IPv4 IP Address 192.168.1.114 ANY ANY

Schedule: Always On

Paso 22. Haga clic en Apply (Aplicar).

Apply Cancel

Paso 23. (Opcional) Para guardar la configuración permanentemente, haga clic en el icono **Guardar**.

**Nota:** Si desea guardar permanentemente esta configuración, asegúrese de guardar la configuración en ejecución en la configuración inicial.

Ahora debería haber configurado correctamente la función de control de aplicaciones en el router serie RV34x.

También puede encontrar este artículo informativo: [Preguntas frecuentes \(FAQ\) sobre el router serie RV34x](#)

Este sitio ofrece varios enlaces a otros artículos que pueden resultar interesantes: [Página del producto del router serie RV34x](#)

## Ver un vídeo relacionado con este artículo...

[Haga clic aquí para ver otras charlas técnicas de Cisco](#)