

在RV34x系列路由器上配置網路過濾

目標

Web過濾是路由器的一項功能，它可以根據網路信譽索引中的得分來篩選網站，將關鍵字或域名新增到阻止清單中，以及按伺服器IP地址來增強已安全網路並提高工作場所的工作效率。

管理員或公司可能擁有現有指南，討論一般網路安全、物聯網以及他們希望在網路上實施的規則，但在涉及特定部門時發現這些規則的例外。管理員可以建立計畫規則並將它們繫結到例外清單，以在一天中的某個時間授予對特定網站的訪問，或在網路其餘使用者已拒絕訪問時授予特定使用者對所有網站的訪問。

本文旨在展示如何在RV34x系列路由器上配置Web過濾。

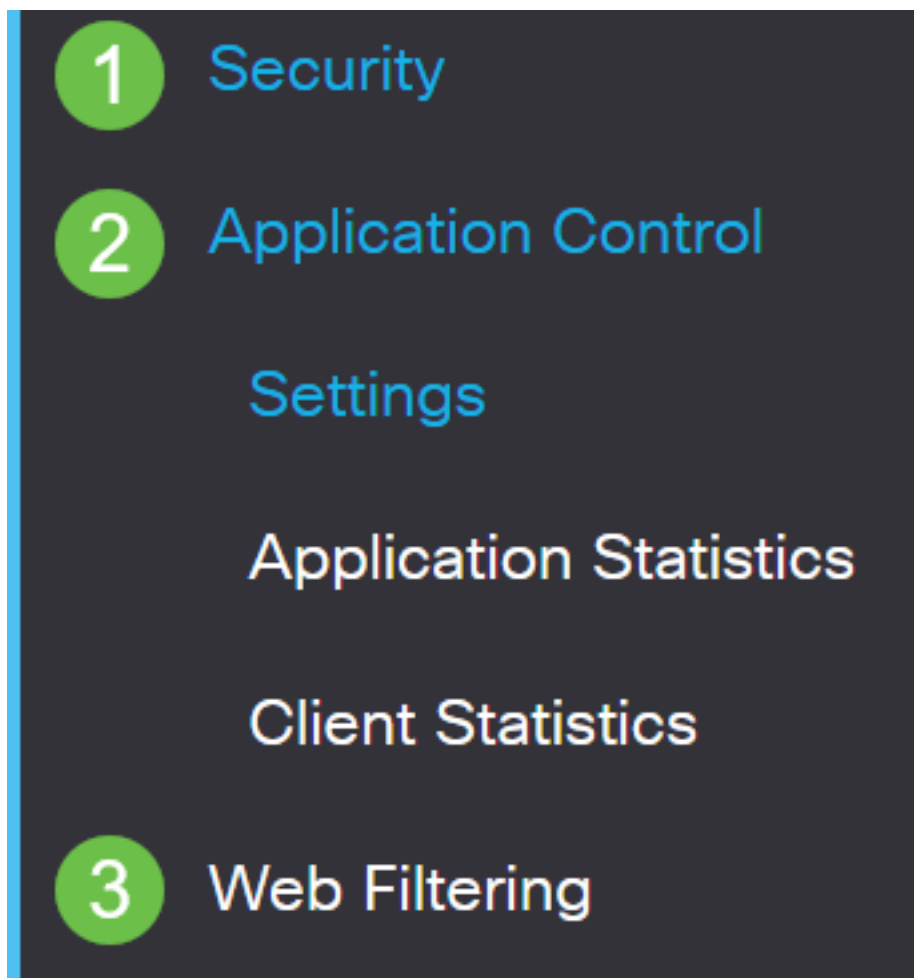
適用裝置 | 軟體版本

- RV34x系列 | 1.0.03.20

配置網路過濾

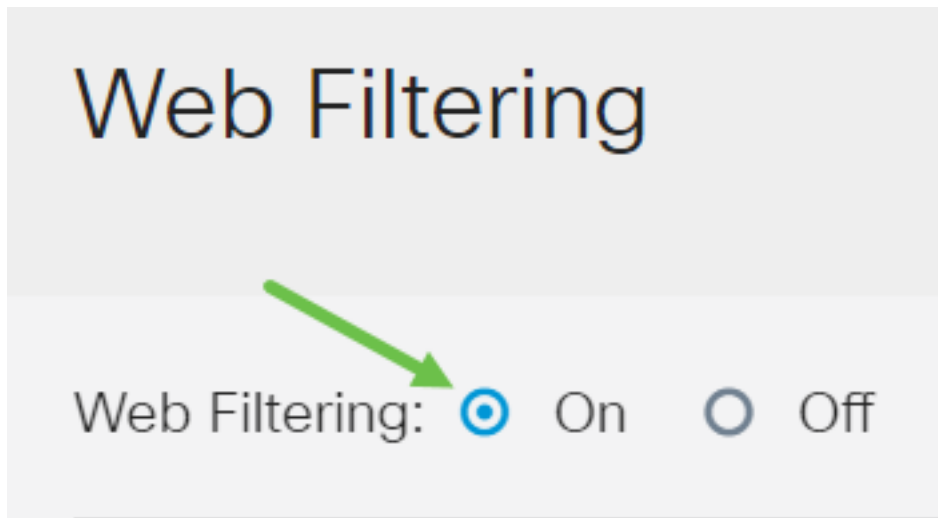
步驟1

登入到基於Web的實用程式，然後選擇Security > Application Control > Web Filtering。



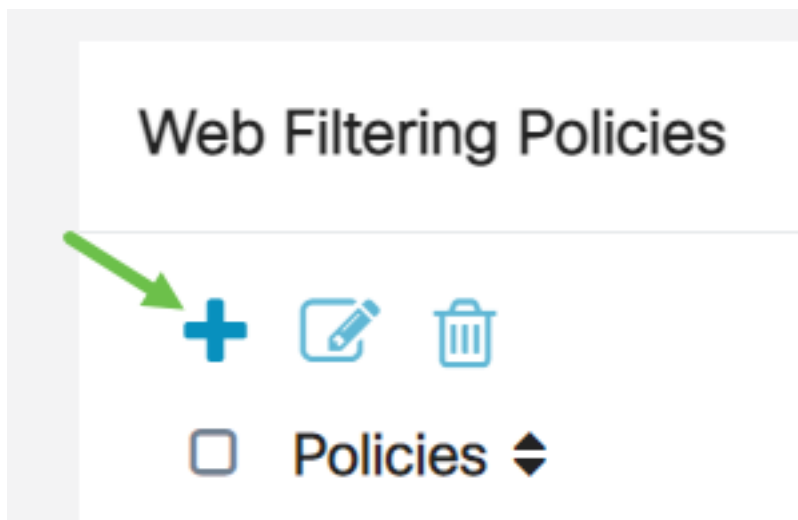
步驟2

選擇 *On* 單選按鈕。



步驟3

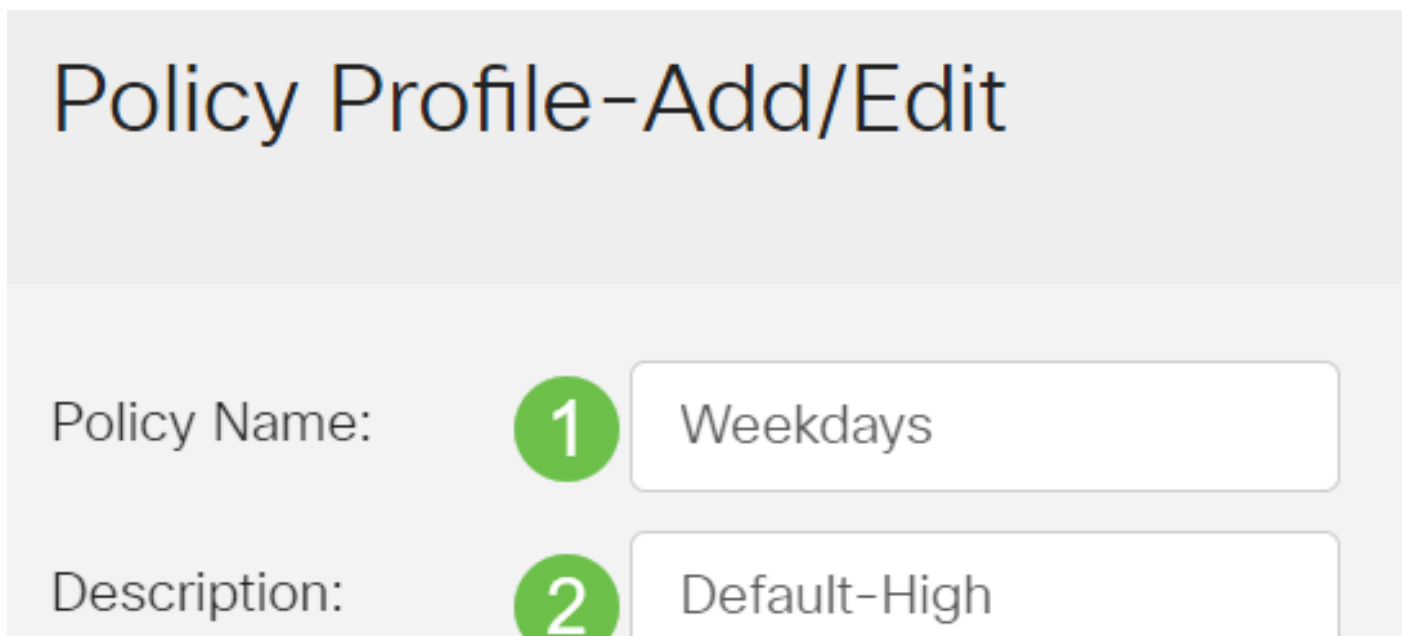
按一下 *add* 圖示。



步驟4

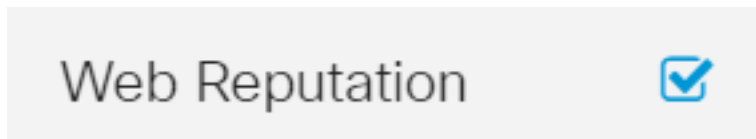
輸入 *Policy Name*、*Description* 和 *Enable* 覈取方塊。

附註：如果路由器上啟用了內容過濾，將出現一條通知，通知您已禁用內容過濾，且不能同時啟用這兩個功能。按一下「*Apply*」以繼續設定。



步驟5

選中Web Reputation竅取方塊以啟用基於Web信譽索引的過濾。

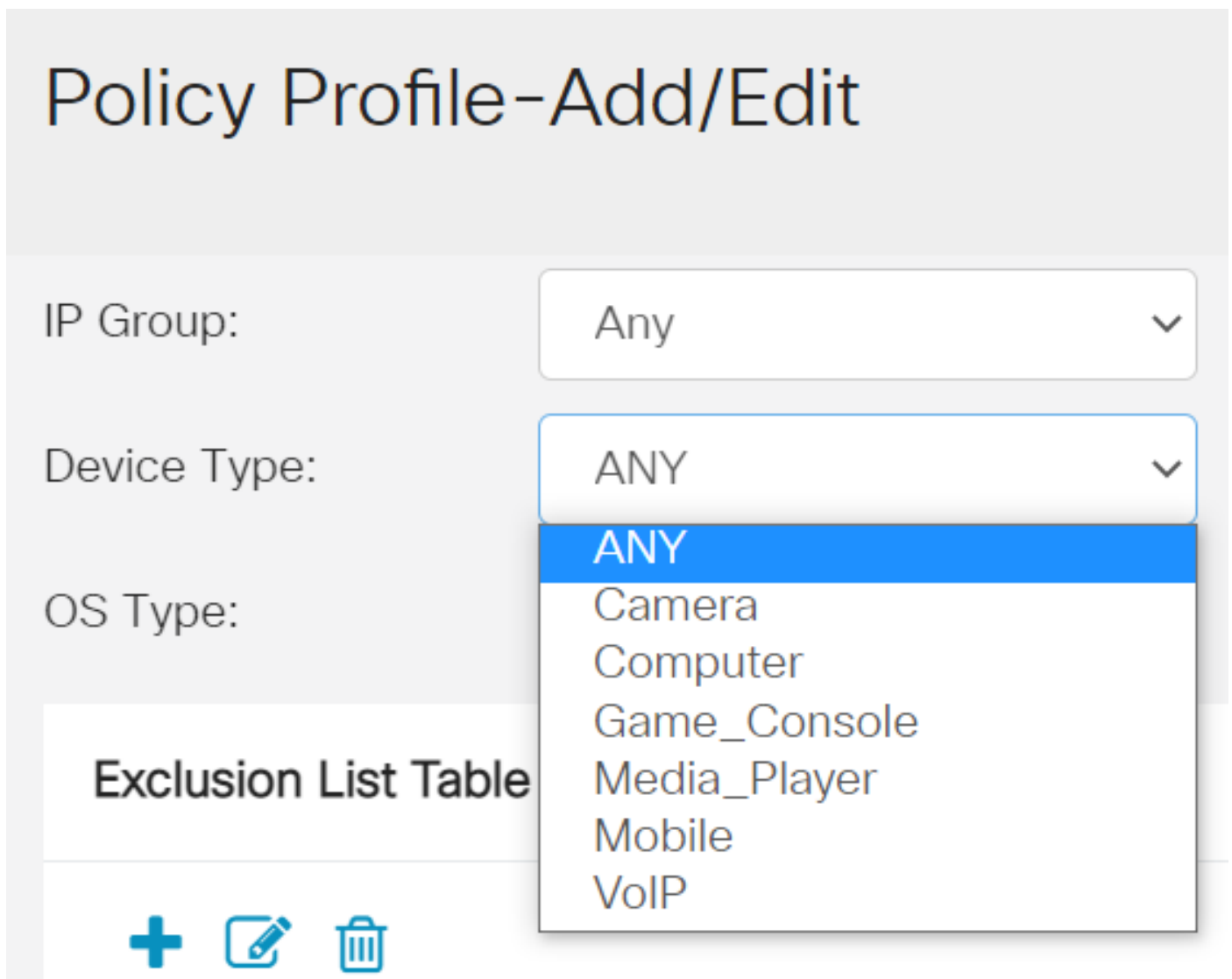


附註：內容將根據網站或URL的惡名基於Web信譽索引進行過濾。如果分數低於40，網站將被阻止。要瞭解有關Web信譽技術的詳細資訊，請按一下[此處](#)瞭解詳細資訊。

步驟6

從Device Type下拉選單中，選擇要過濾的資料包的源/目標。一次只能選擇一個選項。選項包括：

- ANY — 選擇此項可將策略應用於任何裝置。
- 監視器 — 選擇此項可將策略應用於監視器（例如IP安全監視器）。
- 電腦 — 選擇此項可將策略應用於電腦。
- Game_Console — 選擇此項可將策略應用於遊戲控制檯。
- Media_Player — 選擇此項可將策略應用於媒體播放器。
- 移動 — 選擇此項可將策略應用於流動裝置。
- VoIP — 選擇此項可將策略應用於網際網路語音協定裝置。



第7步

在「OS Type」下拉選單中，選擇策略應適用的作業系統(OS)。一次只能選擇一個選項。選項包括：

- ANY — 將策略應用於任何型別的作業系統。這是預設設定。
- Android — 僅將策略應用於Android OS。
- BlackBerry — 僅將策略應用於Blackberry OS。
- Linux — 僅將策略應用於Linux OS。
- Mac_OS_X — 僅將策略應用於Mac OS。
- 其他 — 將策略應用於未列出的作業系統。
- Windows — 將策略應用到Windows作業系統。
- iOS — 僅將策略應用於iOS OS。

The screenshot shows a configuration interface with the following elements:

- Application:** A label with an **Edit** button next to it.
- Application List Table:** A table header.
- Category:** A dropdown menu with a double-headed arrow icon, currently showing a list of options: ANY, Android, BlackBerry, Linux, Mac_OS_X, Other, Windows, and iOS.
- IP Group:** A label.
- Device Type:** A label.
- OS Type:** A dropdown menu with a downward arrow icon, currently showing the selected option: ANY.

步驟8

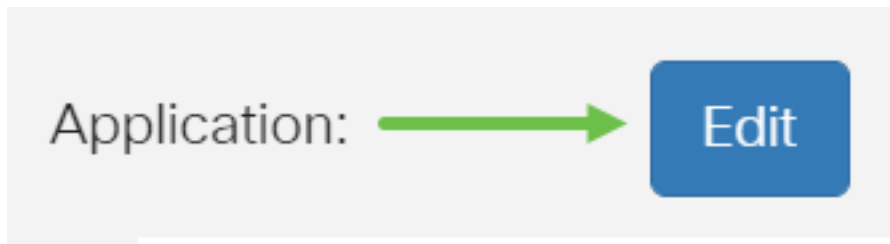
向下滾動到 *Schedule* 部分，然後選擇最符合您需求的選項。

The screenshot shows a configuration interface with the following elements:

- Icons:** A row of three icons: a plus sign (+), a pencil (edit), and a trash can (delete).
- Type:** A dropdown menu with a double-headed arrow icon, currently showing the selected option: Always On.

步驟9

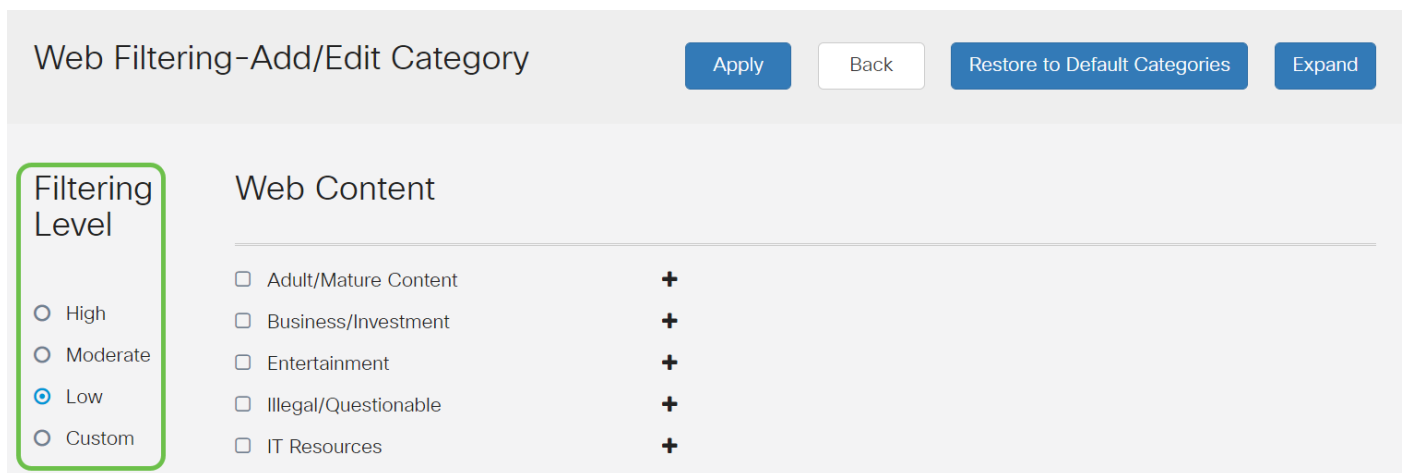
按一下 *Edit* 按鈕。



步驟10

在 Filtering Level 列中，按一下單選按鈕以快速定義最適合網路策略的過濾範圍。選項包括「高」、「中」、「低」和「自定義」。按一下以下任何過濾級別，瞭解過濾到每個已啟用的 Web 內容類別的特定預定義子類別。預定義的過濾器不能再更改，將呈灰色顯示。

- **低** — 這是預設選項。此選項啟用安全性。
- **Moderate** — 使用此選項可啟用「成人/成熟內容」、「非法/可疑」和「安全」。
- **高** — 通過此選項啟用成人/成熟內容、業務/投資、非法/可疑、IT資源和安全。
- **自定義** — 沒有預設值設定為允許使用者定義的篩選器。



Web Filtering-Add/Edit Category

Apply Back Restore to Default Categories Expand

Filtering Level

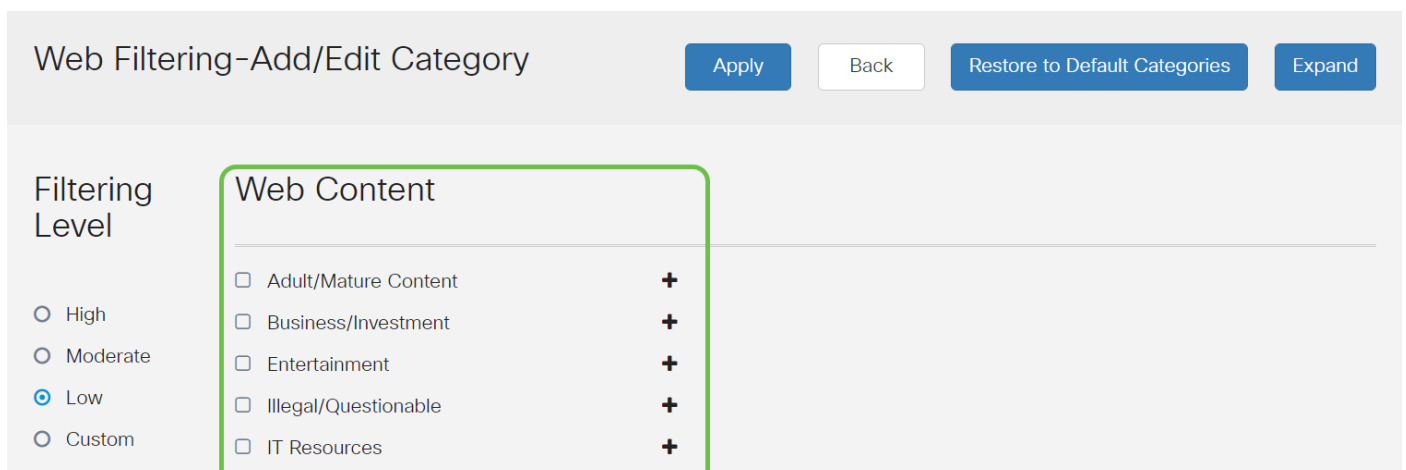
- High
- Moderate
- Low
- Custom

Web Content

<input type="checkbox"/> Adult/Mature Content	+
<input type="checkbox"/> Business/Investment	+
<input type="checkbox"/> Entertainment	+
<input type="checkbox"/> Illegal/Questionable	+
<input type="checkbox"/> IT Resources	+

步驟11

輸入要篩選的 Web 內容。如果您想瞭解某一部分的更多詳細資訊，請按一下 *plus* 圖示。



Web Filtering-Add/Edit Category

Apply Back Restore to Default Categories Expand

Filtering Level

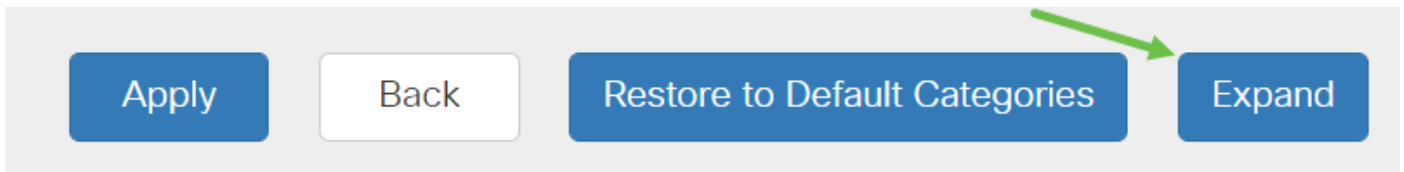
- High
- Moderate
- Low
- Custom

Web Content

<input type="checkbox"/> Adult/Mature Content	+
<input type="checkbox"/> Business/Investment	+
<input type="checkbox"/> Entertainment	+
<input type="checkbox"/> Illegal/Questionable	+
<input type="checkbox"/> IT Resources	+

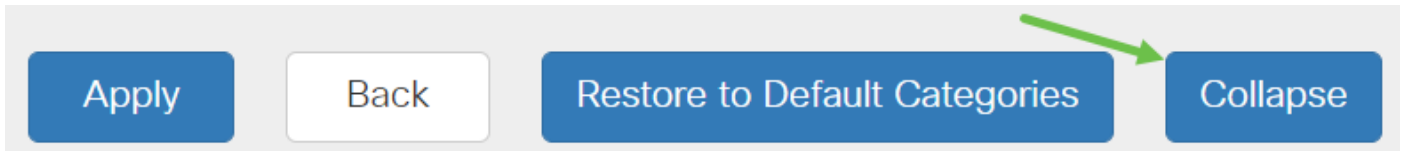
第12步 (可選)

要檢視所有Web內容子類別和說明，可以按一下**Expand**按鈕。



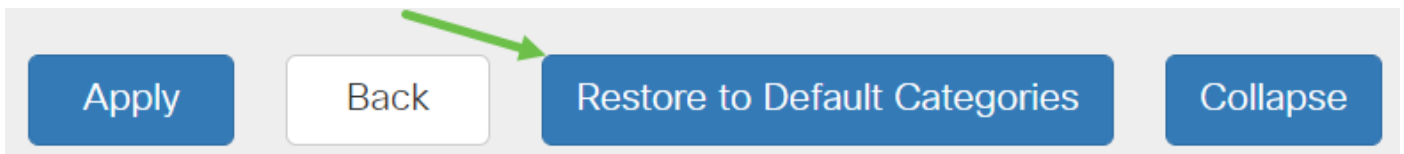
第13步 (可選)

按一下**摺疊**可摺疊子類別和說明。



第14步 (可選)

要返回到預設類別，請按一下**Restore to Default Categories**。



步驟15

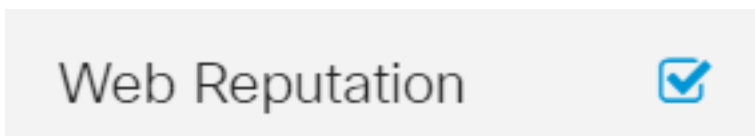
按一下**Apply**以儲存配置，並返回「篩選器」頁以繼續設定。



附註：在「應用程式清單表」中，將填充基於所選篩選級別的相應子類別。

步驟16

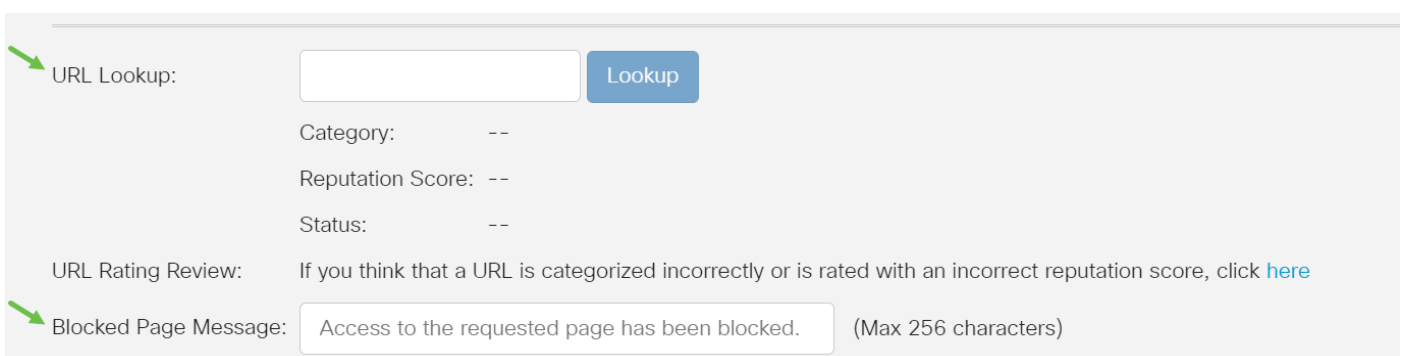
選中 *Web Reputation* 覆取方塊以啟用基於Web信譽索引的過濾。



附註：內容將根據網站或URL的惡名基於Web信譽索引進行過濾。如果分數低於40，網站將被阻止。要瞭解有關Web信譽技術的詳細資訊，請按一下[此處](#)瞭解詳細資訊。

第17步 (可選)

其他選項包括URL查詢以及顯示請求的頁面被阻止時間的消息。



步驟18

按一下「Apply」。



步驟19

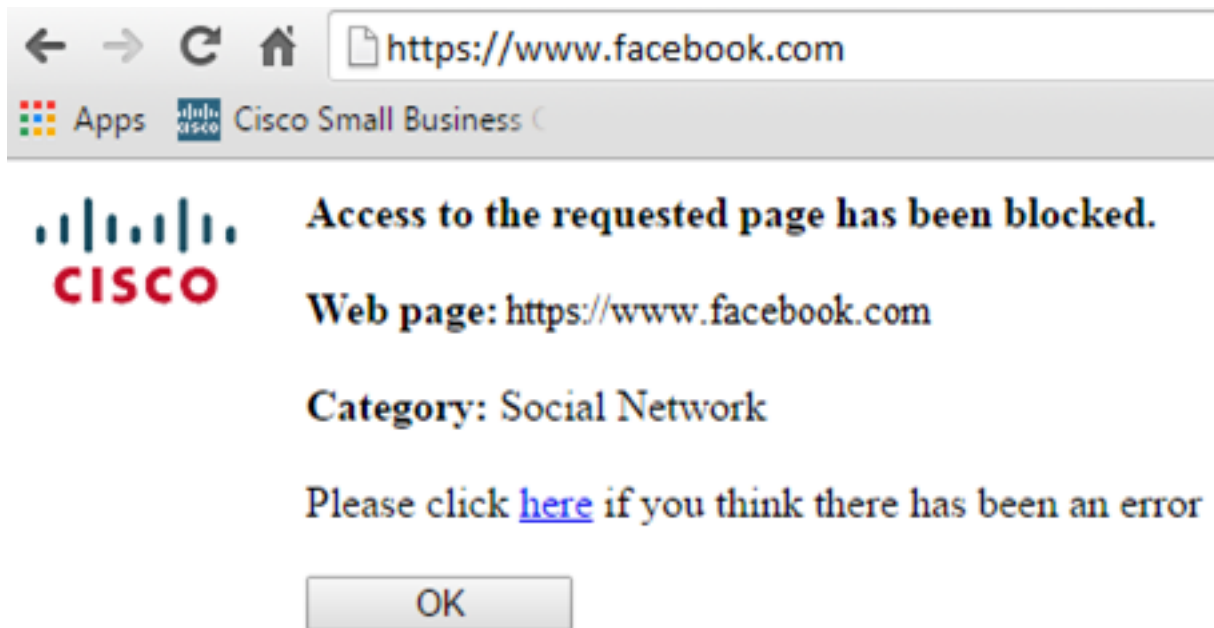
要永久儲存配置，請轉到「複製/儲存配置」頁，或按一下該頁上方的save圖示。



第20步（可選）

要驗證網站或URL是否已被過濾或阻止，請啟動Web瀏覽器或在瀏覽器中開啟一個新頁籤。輸入您已阻止或過濾為被阻止或拒絕的域名。

在本例中，它是www.facebook.com。



您現在應該已經在RV34x路由器上成功配置網路過濾。