Anleitung zur Einrichtung der Zugriffssteuerung - Access Control

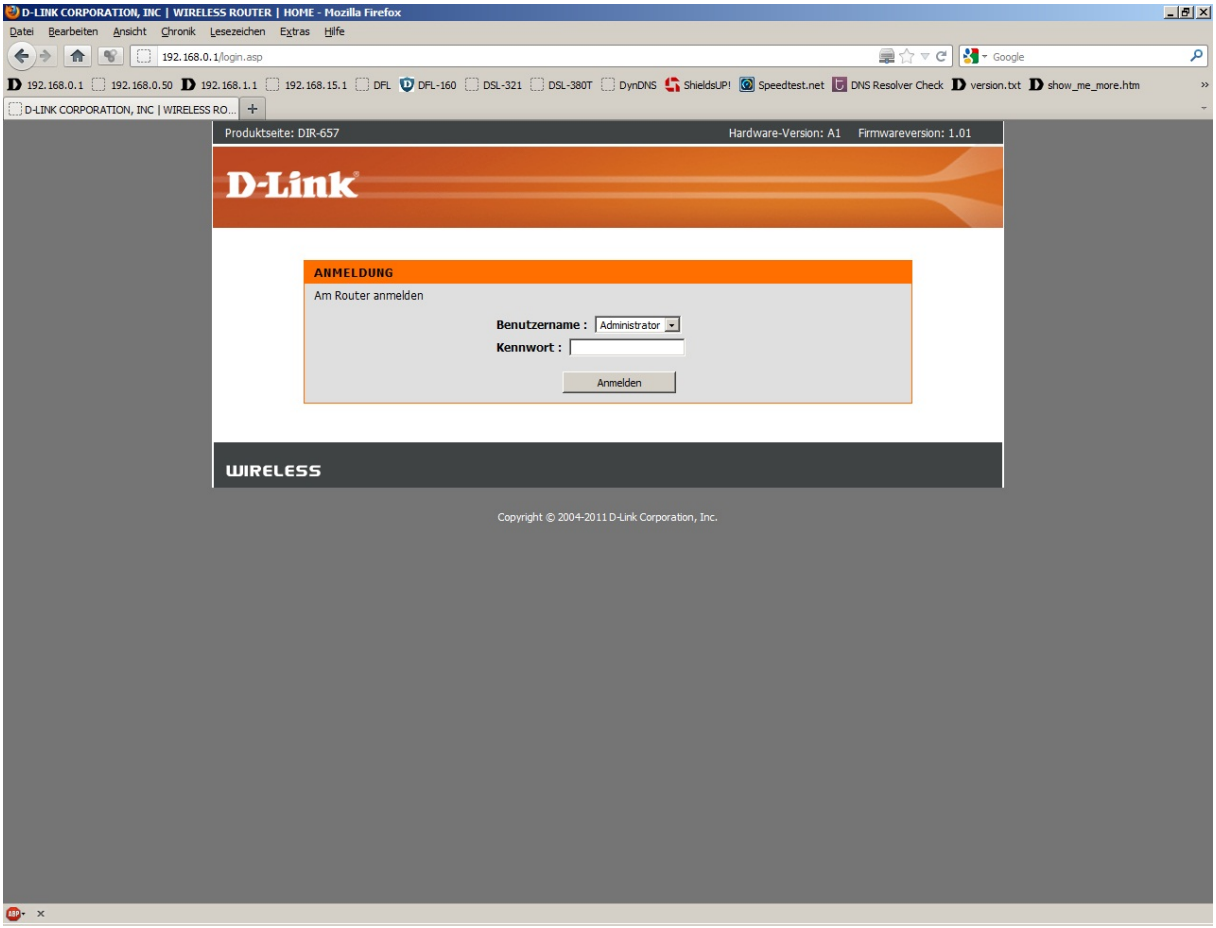
Für DIR-657, DIR-857 und DHP-1565 mit Deutschen Sprachpaket

Um bestimmten Rechnern im LAN den Internetzugang oder den Zugriff auf bestimmte Dienste zu verbieten gibt es im Router die Funktion Zugriffssteuerung.

Beachten Sie auch die Angaben zur Konfiguration der Netzwerkverbindung, in der dem Gerät beiliegenden Anleitung zur Schnellkonfiguration.

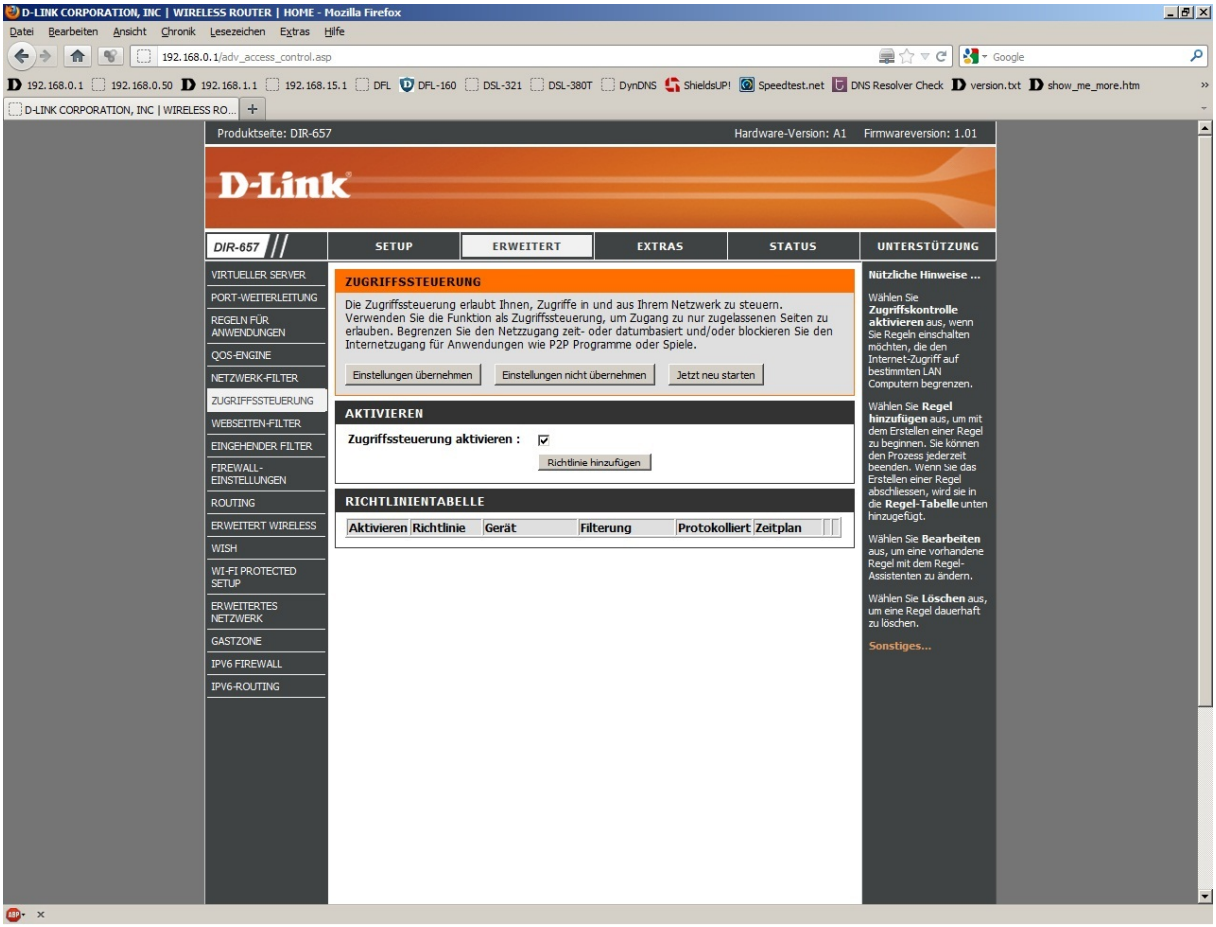
1. Greifen Sie per Webbrowser auf die Konfiguration des DIR-Routers zu.
Die Standard Adresse ist http://192.168.0.1 .

2. Im Auslieferungszustand ist auf die Konfiguration kein Passwort gesetzt.
Als Benutzername wählen Sie **Administrator** aus, lassen das Kennwort Feld leer und klicken auf Anmelden.

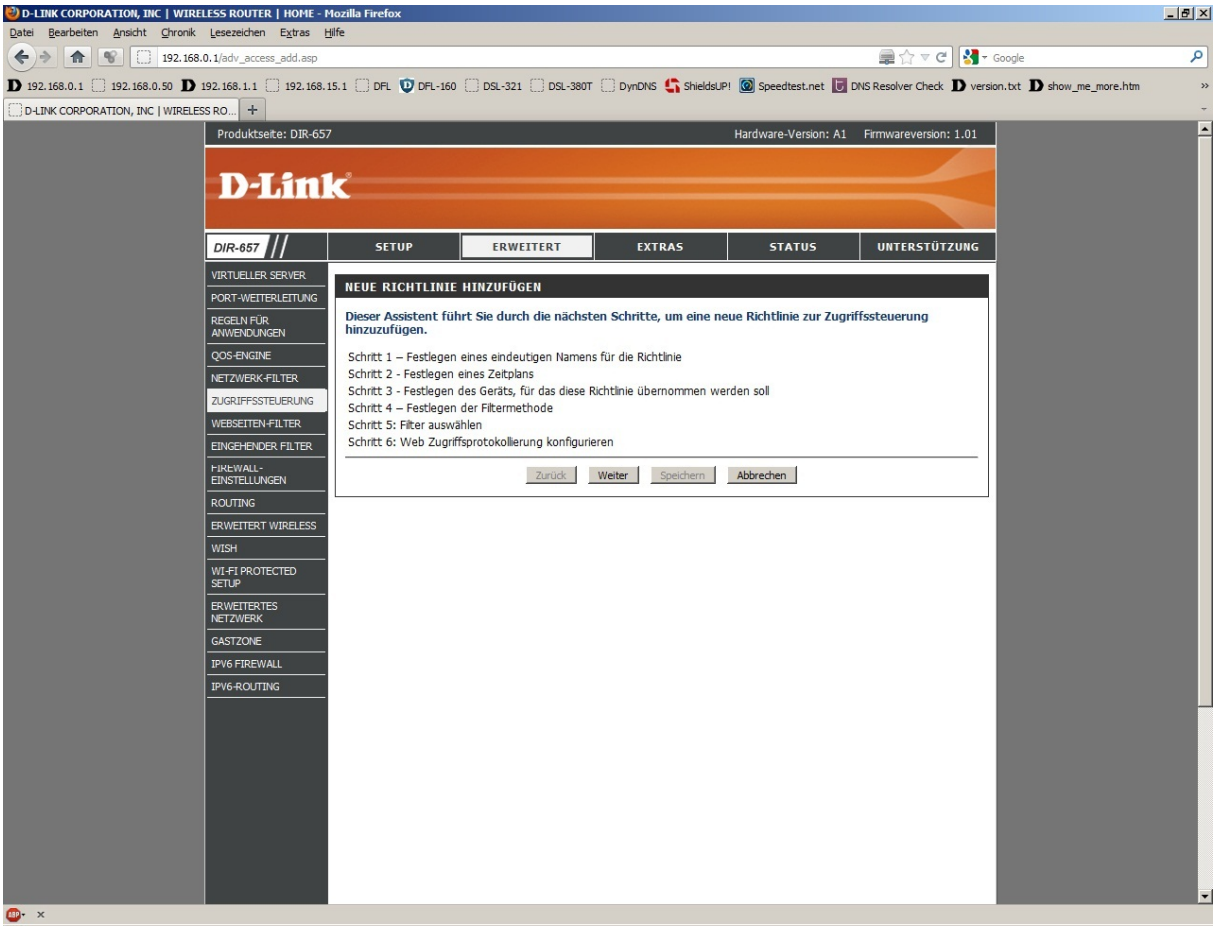


3. Zur Einrichtung der Zugriffskontrolle wählen Sie oben das Menü **Erweitert** und links **Zugriffssteuerung** aus.

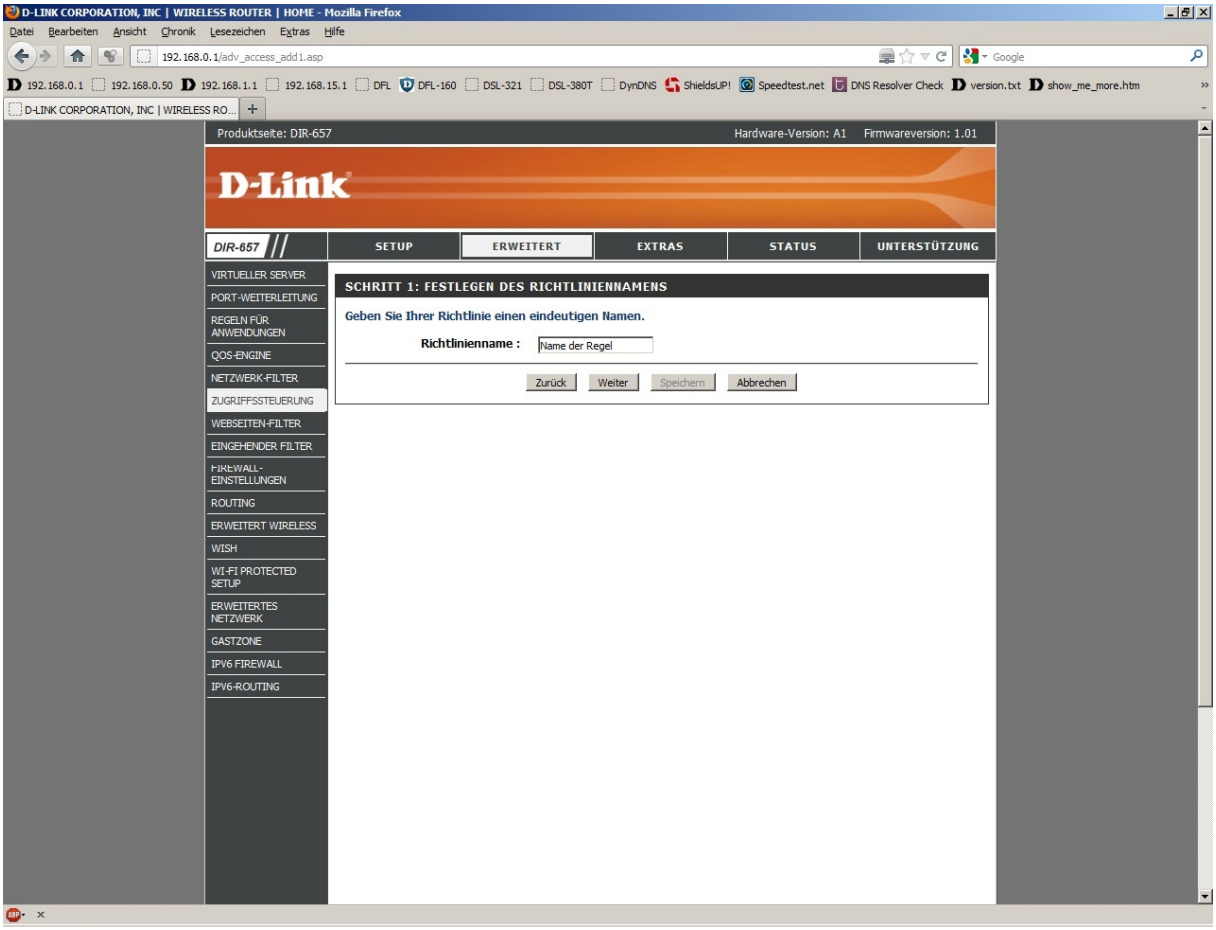
4. Setzen Sie bei **Zugriffssteuerung aktivieren** einen Haken und klicken auf **Richtlinie hinzufügen**.



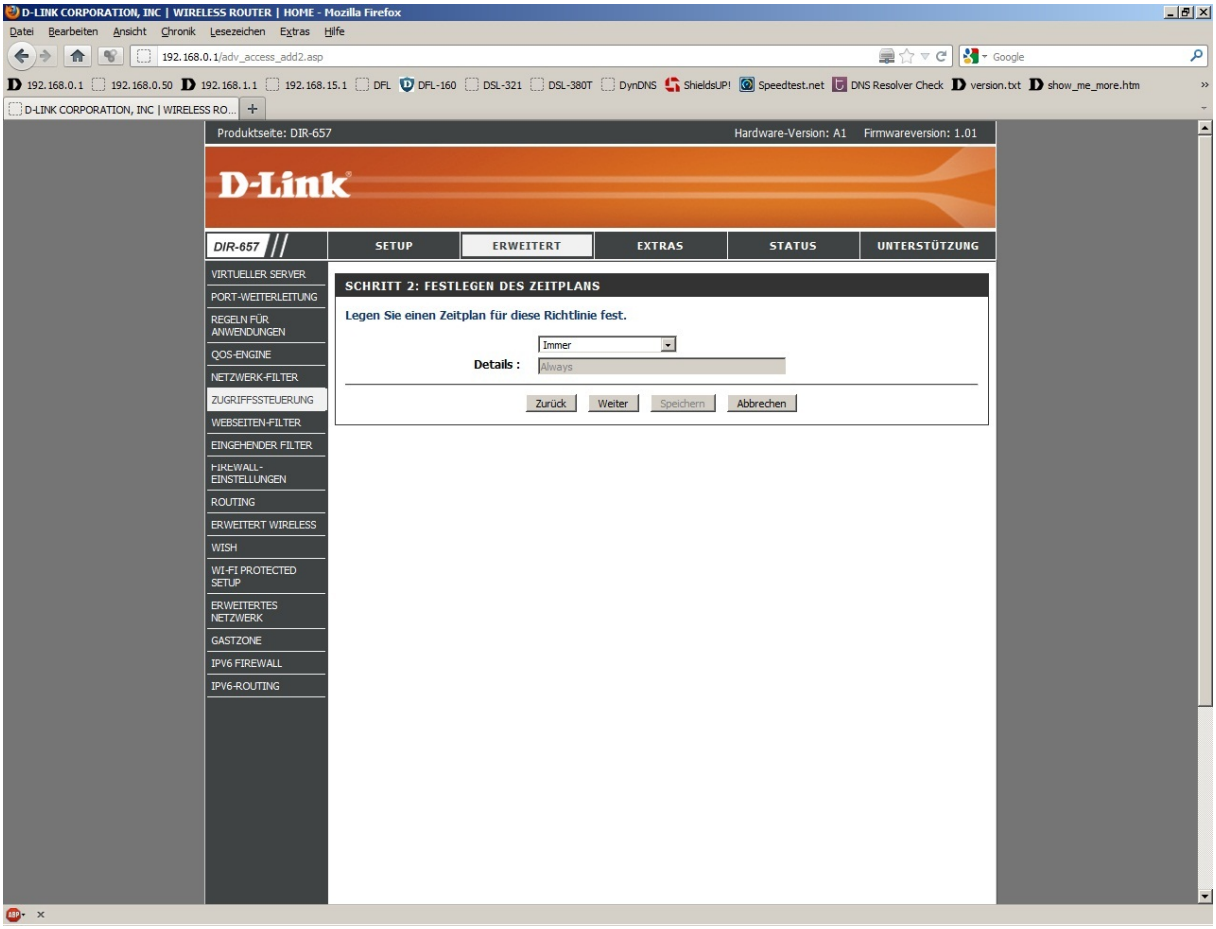
5. Klicken Sie auf **Weiter**.



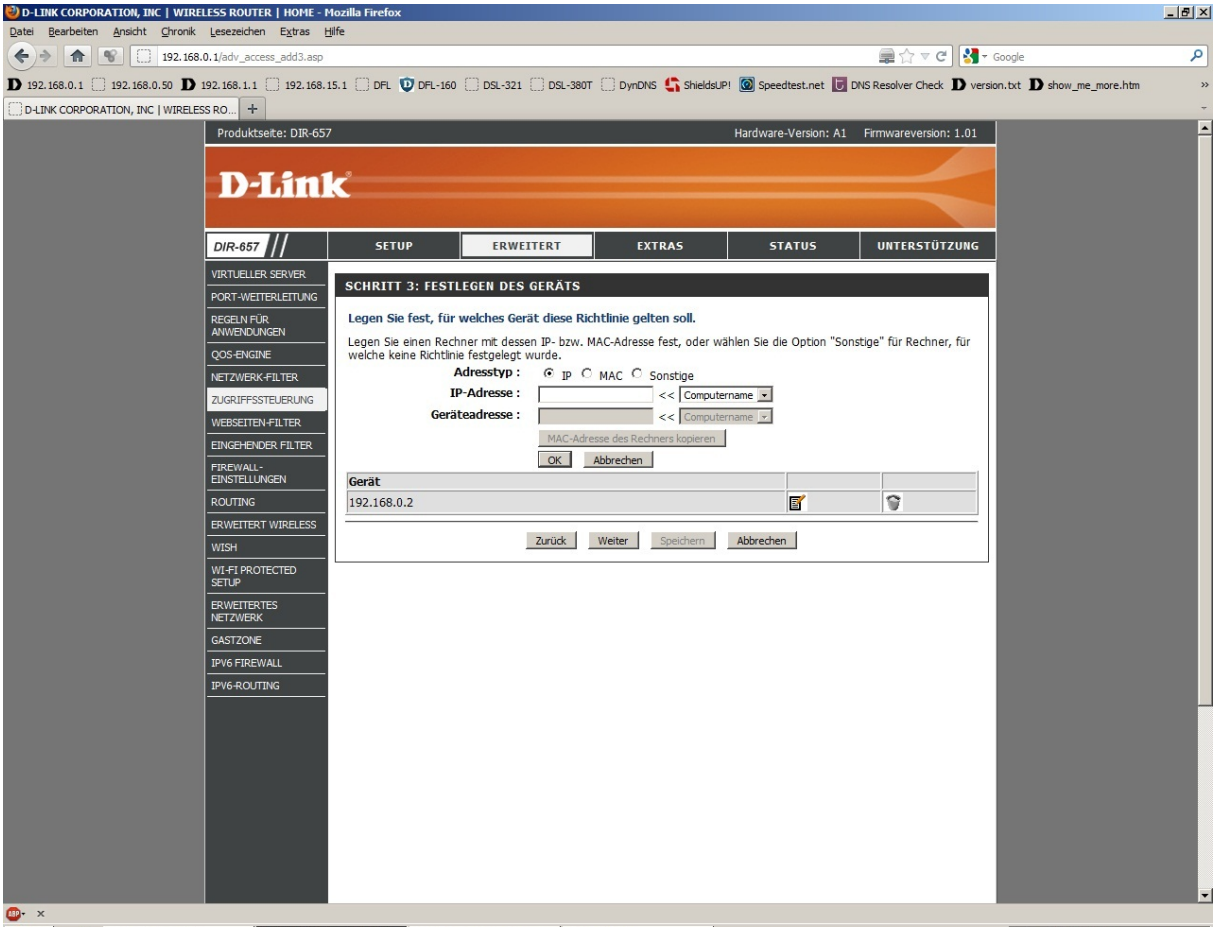
6. Vergeben Sie bei **Richtlinienname** Ihrer Regel einen Namen und klicken auf **Weiter**.



7. Soll die Regel immer gelten, also jeden Tag und rund um die Uhr, muss Immer ausgewählt sein. Andernfalls konfigurieren Sie bitte unter dem Menüpunkt **Extras** – **Zeitpläne** ein Zeitplan-Profil. Beachten Sie dazu die Anleitung **Zeitpläne**.
Klicken auf **Weiter**.



8. Im folgenden Fenster können Sie nun Filter anlegen, um bestimmten Rechnern den Internetzugang zu sperren.



- **Adresstyp**:
 - Wählen Sie **IP** aus um den Rechner mit einer bestimmten IP Adresse zu blockieren.
 - Tragen Sie bei **IP Adresse** die Adresse des zu blockenden Rechners ein, z.B. 192.168.0.22. Beim Aufklappmenue Computer Name können Sie den Rechner auswählen, wenn er vom DHCP Server des Routers seine IP Adresse bezogen hat.

 - Wählen Sie **MAC** aus um den Rechner mit einer bestimmten MAC Adresse zu blockieren.
 - Tragen Sie bei **Geräteadresse** die MAC Adresse des zu blockenden Rechners ein, z.B. 000d8853146c . Beim Aufklappmenue **Computer Name** können Sie den Rechner auswählen wenn er vom DHCP Server des Routers seine IP Adresse bezogen hat.

 - Wählen Sie **Sonstiges** aus um eine Filterregel für alle Rechner zu erstellen.

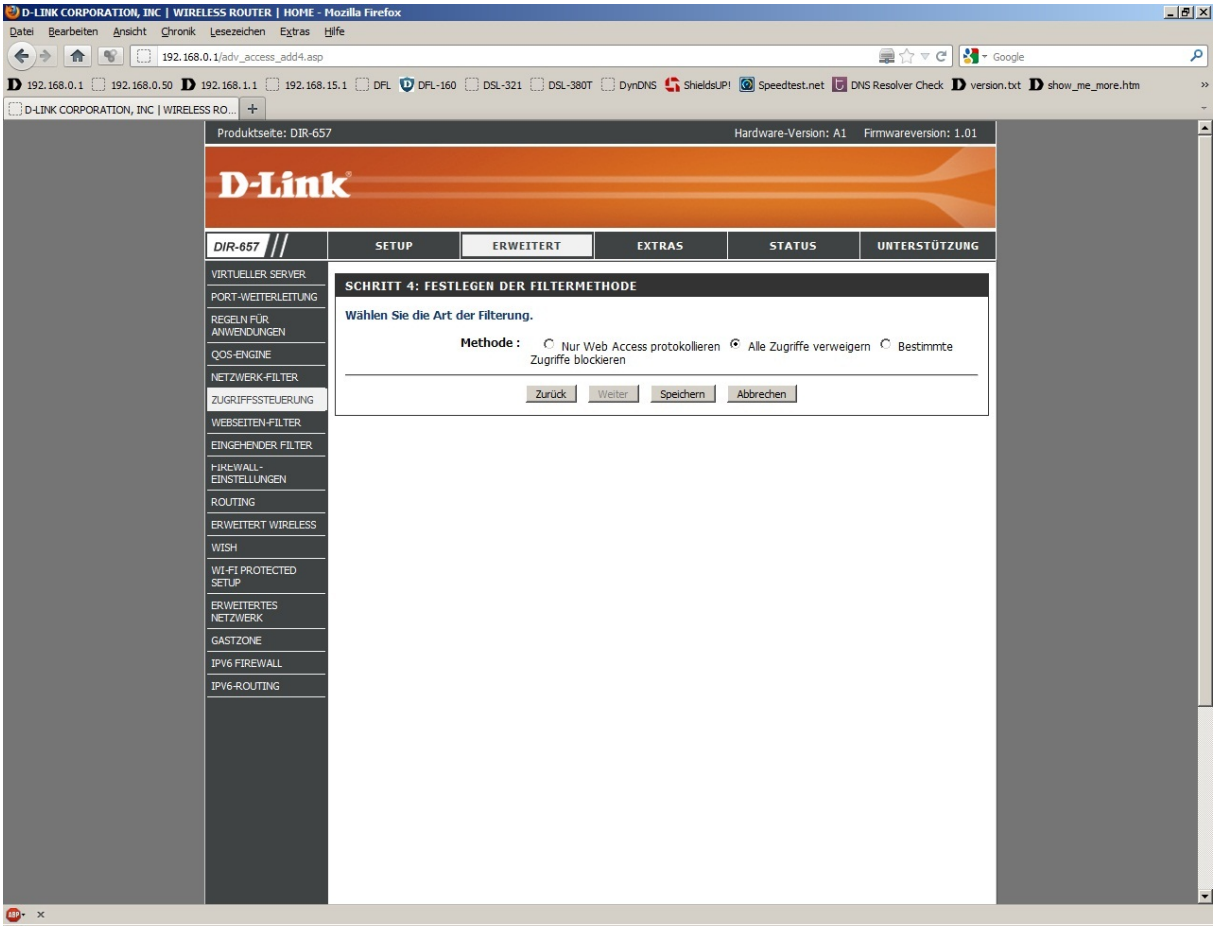
Klicken Sie auf **OK** um das ausgewählte Geräteprofil in der Liste unten aufzunehmen.

Klicken Sie dann auf **Weiter**.

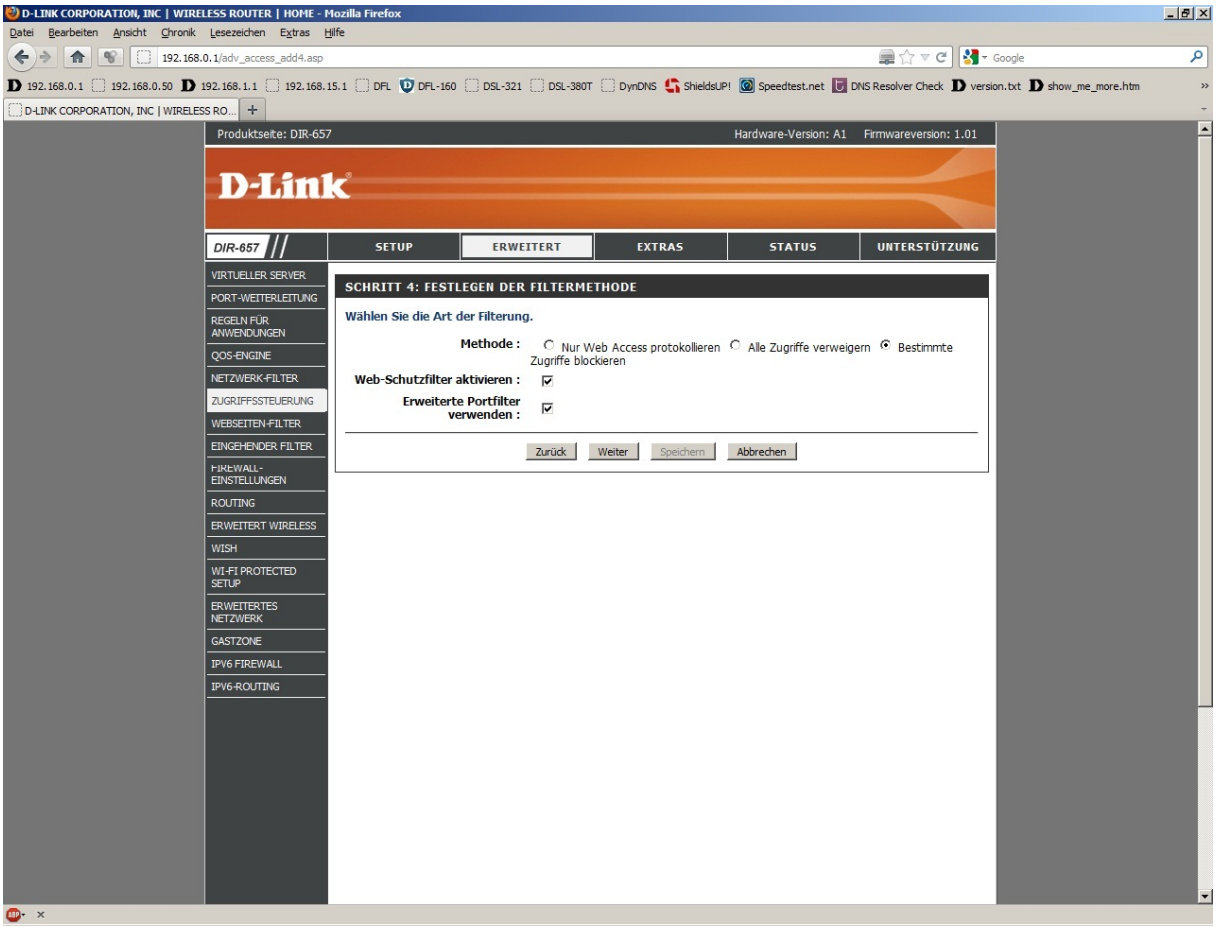
9. Methode:

- Wählen Sie **Nur Web Access protokollieren** aus, um lediglich den Internetzugriff des im Geräteprofil ausgewählten Rechners im Log des Routers zu protokollieren.
Der Zugriff des im Geräteprofil ausgewählten Rechners wird dadurch nicht geblockt.

- Wählen Sie **Alle Zugriffe verweigern** aus, um den Internetzugriff für den im Geräteprofil ausgewählten Rechner zu blockieren.



- Wählen Sie **Bestimmte Zugriffe blockieren** aus, um eine Zugriffsregel zu konfigurieren, z.B. um den im Geräteprofil ausgewählten Rechner den Zugriff auf z.B. FTP Server (Port TCP 21) zu verweigern.

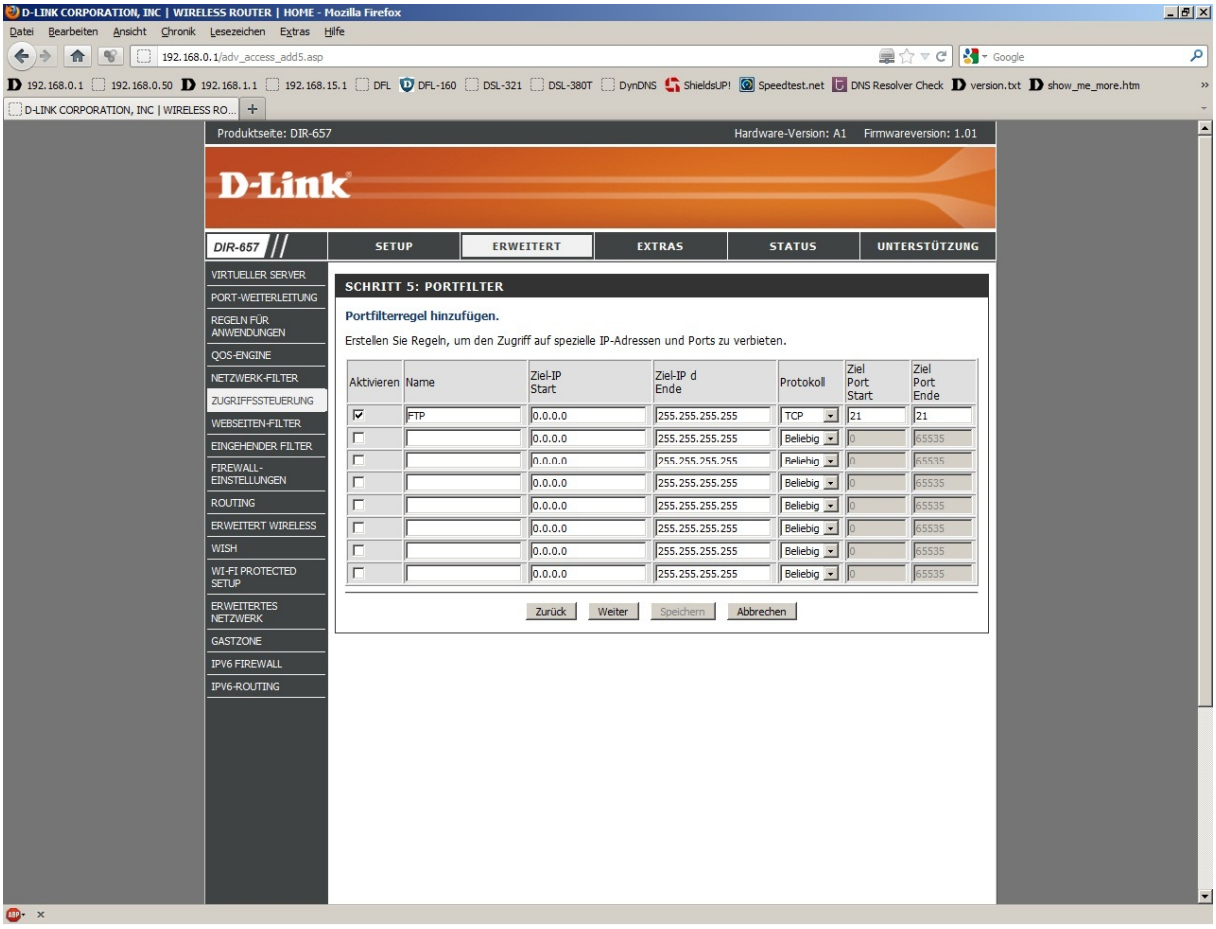


- Markieren Sie **Web-Schutzfilter aktivieren**, um für die im Geräteprofil ausgewählten Rechner den Webseiten-Filter zu nutzen.
Möchten Sie keinen Webseiten-Filter nutzen, markieren Sie Web-Schutzfilter aktivieren **nicht**.

- Markieren Sie **Erweiterte Portfilter verwenden**, um den im Geräteprofil ausgewählten Rechnern den Zugriff auf bestimmte TCP/UDP Ports oder mit ICMP (Pings) zu verweigern.

Klicken Sie auf **Weiter**.

10. Haben Sie **Erweiterte Portfilter verwenden** markiert, können Sie nun Portfilterregeln erstellen.



- Setzen Sie für die nachfolgende Regel einen Haken unter **Aktivieren**.

- Vergeben Sie dem Portfilter einen **Name**n.

- Falls Sie den Zugriff auf eine bestimmte Ziel-IP Adresse oder einen Bereich (IP Range) verbieten möchten, tragen Sie diese bei **Ziel-IP Start** und **Ziel-IP Ende** ein. Andernfalls belassen Sie die vorkonfigurierten Werte.

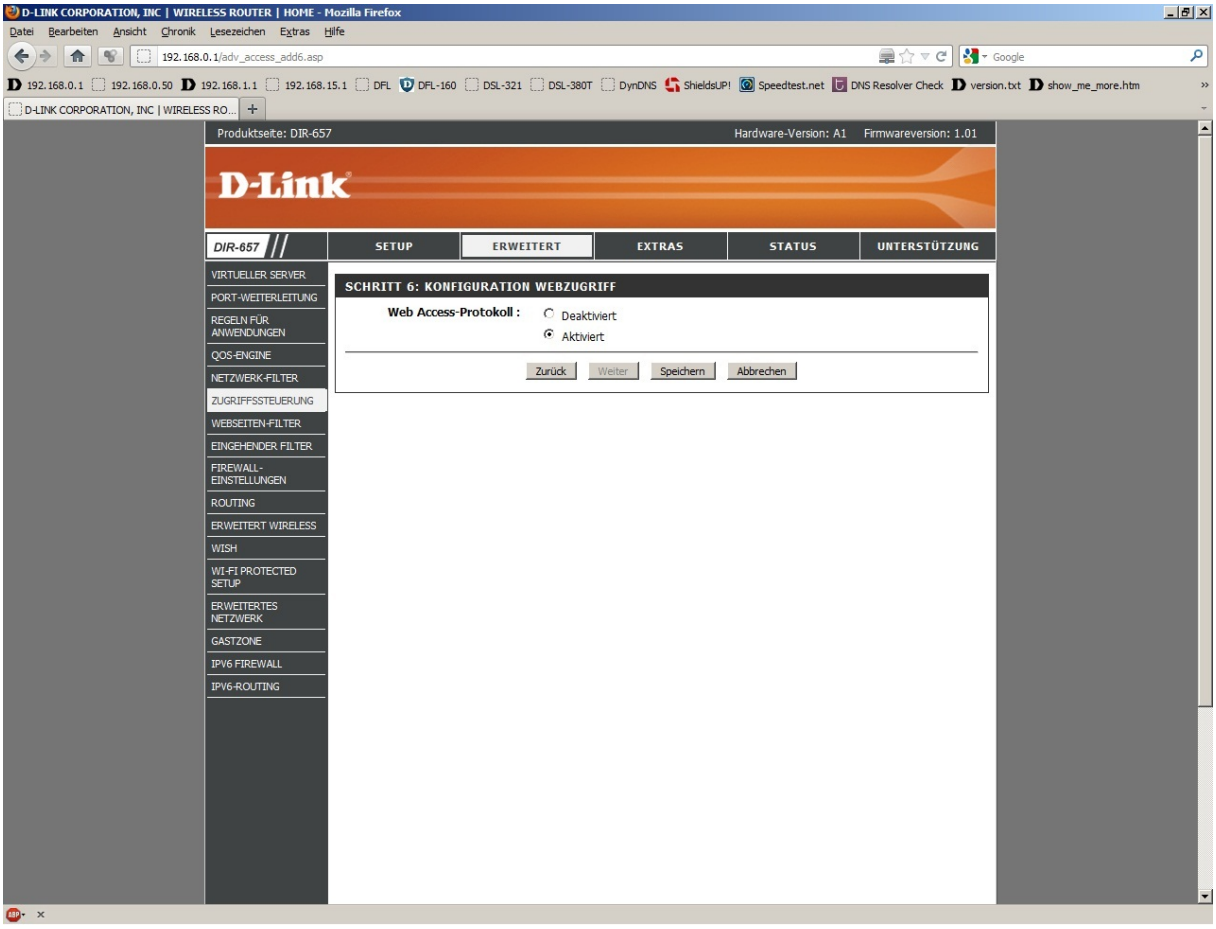
- Wählen Sie den Protokolltyp **TCP, UDP, ICMP oder Any** aus. **Any** steht für alle Protokolltypen.

- Möchten Sie den Zugriff auf einen bestimmten Ziel Port oder einen Bereich (Port Range) verbieten, tragen Sie den entsprechenden Port unter **Ziel Port Start** und **Ziel Port Ende** ein.

- Hatten Sie im vorangegangenen Fenster **Web-Schutzfilter aktivieren** angehakt, klicken Sie nun auf **Weiter**.

Ansonsten klicken Sie auf **Speichern** um die Einstellungen zu übernehmen.

11. Sie können nun den die Protokollierung des Web-Schutzfilter mittels **Aktiviert** ein- oder **Deaktiviert** ausschalten.



Klicken Sie auf **Speichern** um die Einstellungen zu übernehmen.

Hinweis: Haben Sie den **Web-Schutzfilter** konfiguriert?
Damit ein Webseitenfilter funktionieren kann, muss der Router als DNS-Relay arbeiten. In der Konfiguration des Router unter Setup – Netzwerk-Einstellungen muss dazu das **DNS-Relay aktivieren** aktiviert sein.
Das **DNS-Relay aktivieren** ist standardmäßig eingeschaltet.