Anleitung zur Einrichtung von Outbound und Inbound Filtern

Für DWR-512
(Stand August 2012)

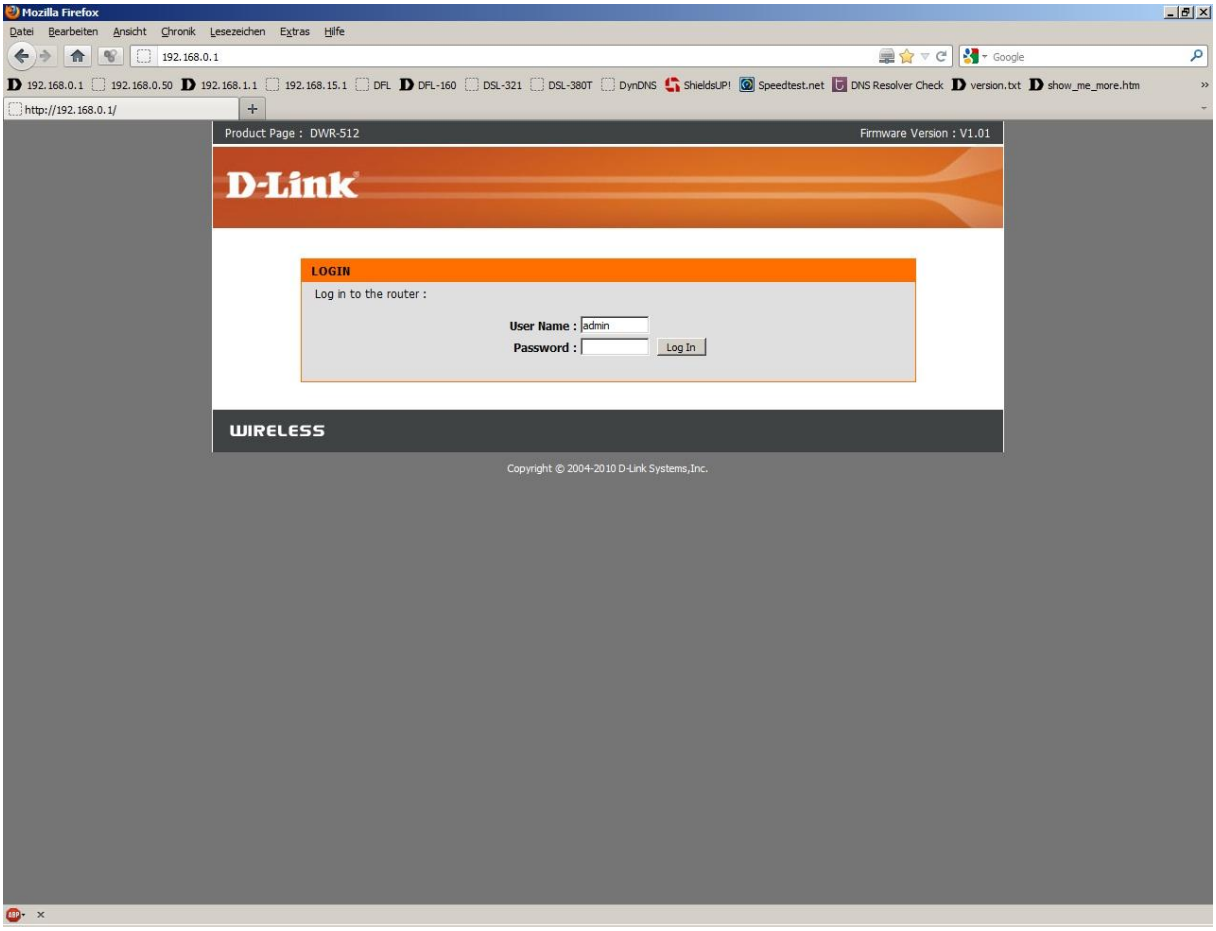
Mittels der Outbound Filter können Sie den Zugriff von Ihrem Lokalen Netzwerk auf bestimmte IP Adressen oder Dienste (TCP/UDP Ports) im Internet beschränken.

Mittels der Inbound Filter können Sie den Zugriff auf eine vorgenommene Portfreigabe (Virtual Server) beschränken.

Beispiele zu Outbound Filter finden Sie auf Seite 2 bis 4 dieser Anleitung.
Ein Beispiel zu Inbound Filter finden Sie ab Seite 5 dieser Anleitung.

1. Greifen Sie per Webbrowser auf die Konfiguration des DWR-512 zu.
Die Standard Adresse ist http://192.168.0.1 .

2. Im Auslieferungszustand ist auf die Konfiguration kein Passwort gesetzt.
Als **User Name** geben Sie **admin** ein, lassen das **Password** Feld leer und klicken auf **Log In**.



Outbound Filter

2. Wählen Sie oben das Menü Advanced und links das Menü Outbound Filter aus.

3. Setzen Sie bei Outbound Filter einen Haken.

Soll der Outbound Filter so konfiguriert werden, dass die angegebene Regel dazu dient um zu blocken und alle anderen haben weiterhin freien Zugang zum Internet, aktivieren Sie **Allow all to pass exept those match the following rules**.

Beispiel ID1 (Screenshot auf der folgenden Seite):
Der Rechner im Lokalen Netzwerk 192.168.0.100 soll keinerlei Internetzugriff haben.
Seine IP 192.168.0.100 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist 0.0.0.0 und als Destination Port ist 1-65535 anzugeben.

Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

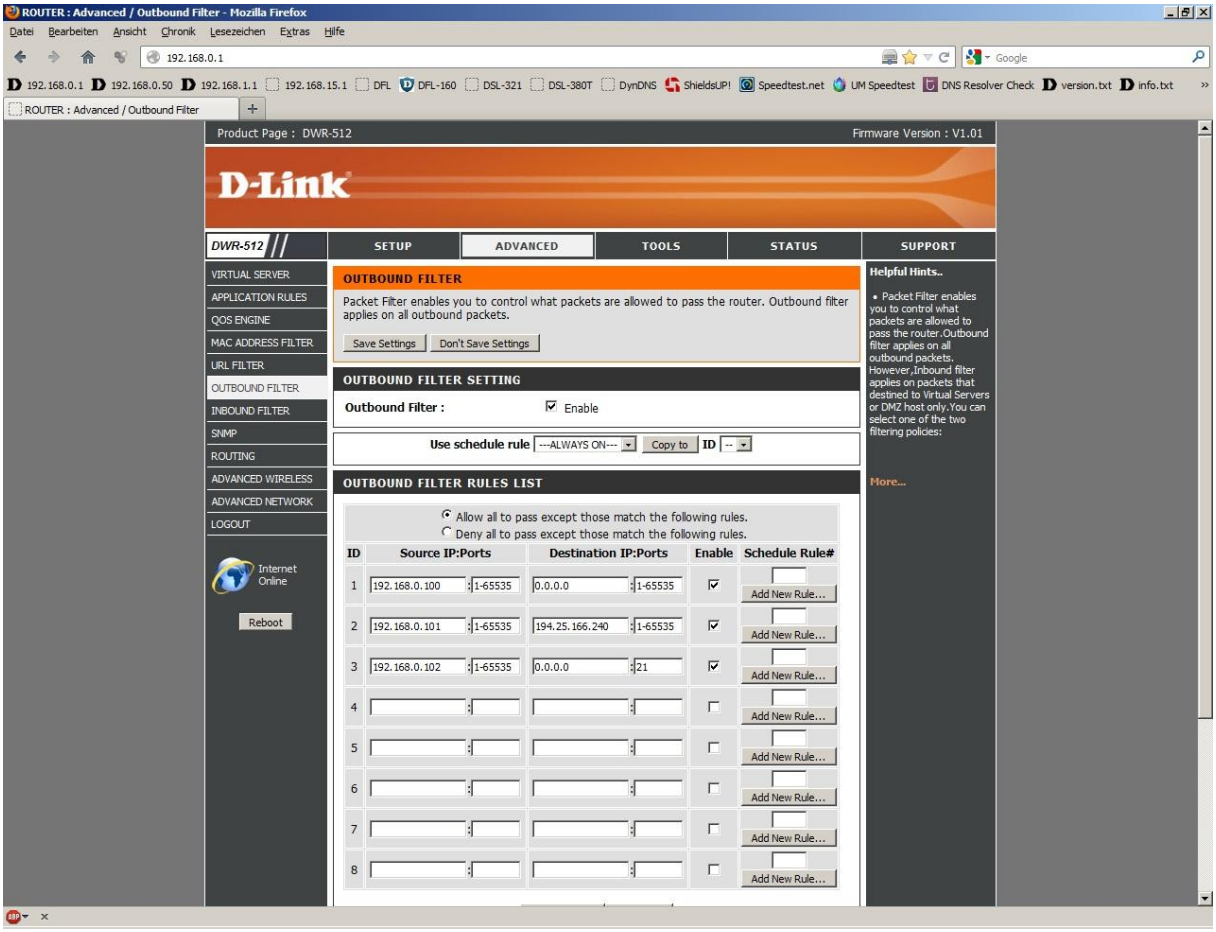
Beispiel ID2 (Screenshot auf der folgenden Seite):
Der Rechner im Lokalen Netzwerk 192.168.0.101 soll keinen Zugriff auf eine bestimmte Zieladresse haben.
Seine IP 192.168.0.101 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist die des Ziels, in Beispiel hier die 194.25.166.240. Als Destination Port ist 1-65535 anzugeben.

Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Beispiel ID3 (Screenshot auf der folgenden Seite):
Der Rechner im Lokalen Netzwerk 192.168.0.102 soll keinen Zugriff irgendeinen FTP Server im Internet haben.
Seine IP 192.168.0.102 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP Als Destination IP ist 0.0.0.0 anzugeben. Als Destination Port ist 21 anzugeben.

Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Um die vorgenommenen Einstellungen zu übernehmen, klicken Sie oben auf **Save Settings**.



Soll der Outbound Filter so konfiguriert werden, dass die angegebene Regel dazu dient um zuzulassen und allen anderen den Zugang zum Internet zu blockieren, aktivieren Sie **Deny all to pass exept those match the following rules**.

Beispiel ID1 (Screenshot auf der folgenden Seite):
Der Rechner im Lokalen Netzwerk 192.168.0.100 soll vollen Internetzugriff haben.
Seine IP 192.168.0.100 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist 0.0.0.0 und als Destination Port ist 1-65535 anzugeben.

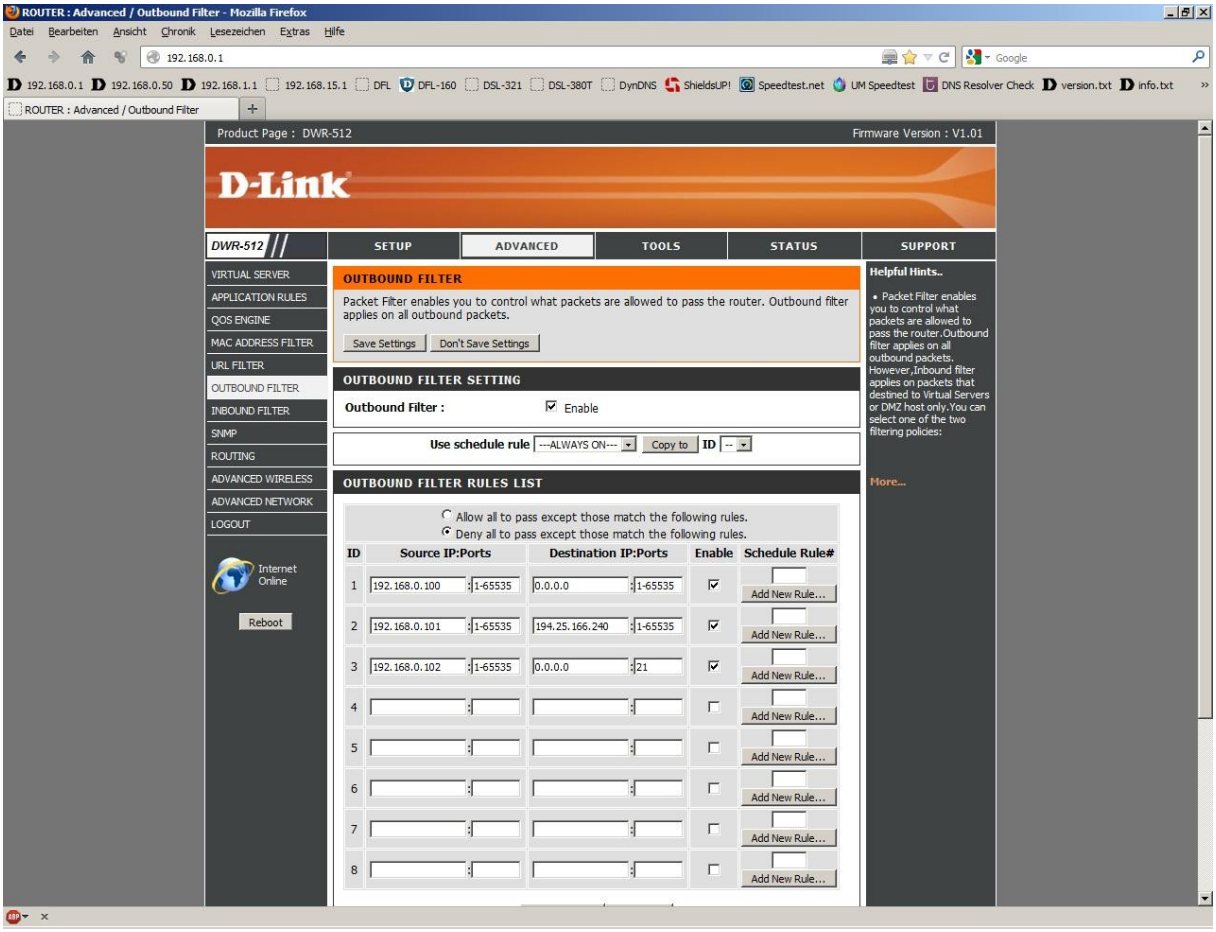
Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Beispiel ID2 (Screenshot auf der folgenden Seite):
Der Rechner im Lokalen Netzwerk 192.168.0.101 soll ausschließlich Zugriff auf eine bestimmte Zieladresse haben.
Seine IP 192.168.0.101 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist die des Ziels, in Beispiel hier die 194.25.166.240. Als Destination Port ist 1-65535 anzugeben.

Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Beispiel ID3:
Der Rechner im Lokalen Netzwerk 192.168.0.102 soll ausschließlich Zugriff auf FTP Server im Internet haben.
Seine IP 192.168.0.102 und der Portbereich 1-65535 ist als Source IP:Port anzugeben. Als Destination IP Als Destination IP ist 0.0.0.0 anzugeben. Als Destination Port ist 21 anzugeben.

Rechts neben der Regel unter Enable setzen Sie noch einen Haken.



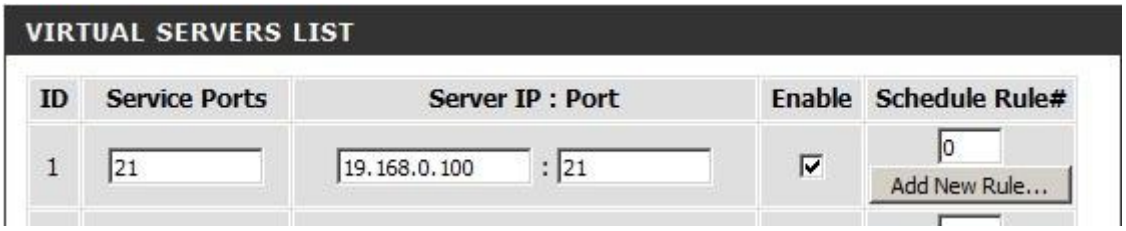
Um die vorgenommenen Einstellungen zu übernehmen, klicken Sie oben auf **Save Settings**.

Inbound Filter

2. Wählen Sie oben das Menü Advanced und links das Menü Inbound Filter aus.

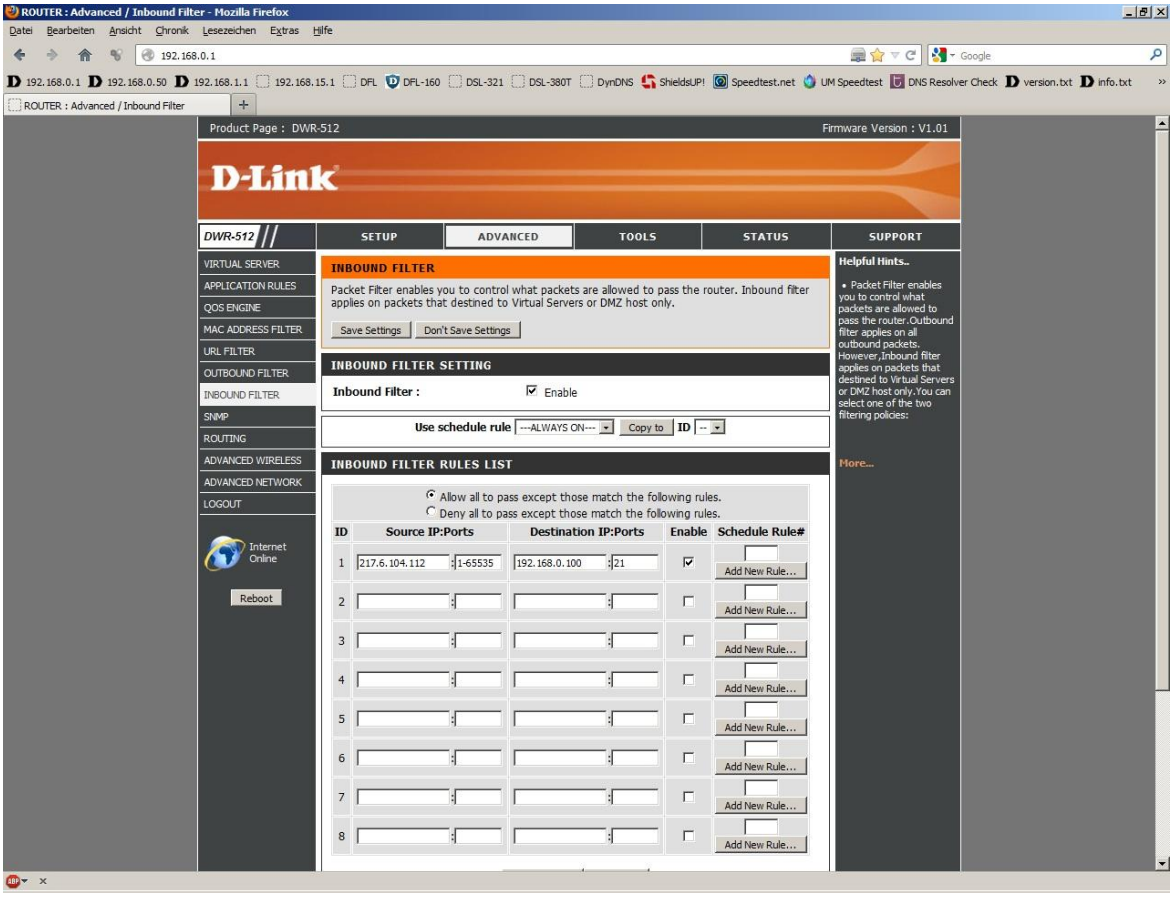
3. Setzen Sie bei Inbound Filter einen Haken.

In dem Beispiel für den Inbound Filter liegt eine Portfreigabe auf einen im lokalen Netzwerk befindlichen FTP Server zugrunde.



Soll der Inbound Filter so konfiguriert werden, dass die angegebene Regel dazu dient um den Zugriff auf eine Portfreigabe zu blocken und alle anderen haben weiterhin Zugriff auf die Portfreigabe, aktivieren Sie
Allow all to pass exept those match the following rules.

Beispiel ID1:
Der im Internet befindliche Rechner 217.6.104.112 soll keinen Zugriff auf die Portfreigabe haben.
Seine IP 217.6.104.112 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist die des lokalen FTP Server und als Destination Port ist 21 anzugeben.

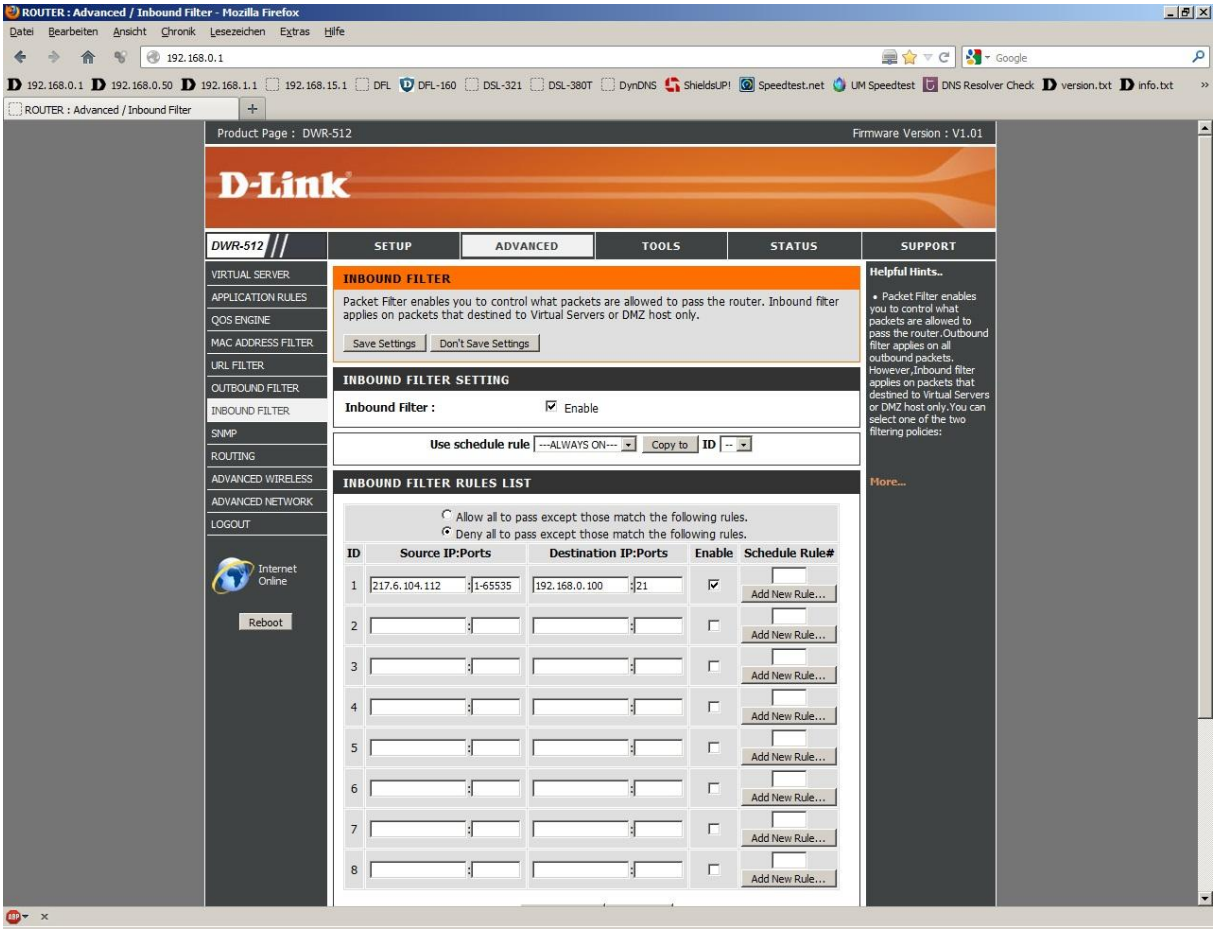


Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Um die vorgenommenen Einstellungen zu übernehmen, klicken Sie oben auf **Save Settings**.

Soll der Inbound Filter so konfiguriert werden, dass die angegebene Regel dazu dient um den Zugriff auf eine Portfreigabe zu blocken und alle anderen haben weiterhin Zugriff auf die Portfreigabe, aktivieren Sie
Deny all to pass exept those match the following rules.

Beispiel ID1:
Der im Internet befindliche Rechner 217.6.104.112 soll der einzige sein, der Zugriff auf die Portfreigabe hat.
Seine IP 217.6.104.112 und der Portbereich 1-65535 ist als Source IP:Port anzugeben.
Als Destination IP ist die des lokalen FTP Server und als Destination Port ist 21 anzugeben.



Rechts neben der Regel unter Enable setzen Sie noch einen Haken.

Um die vorgenommenen Einstellungen zu übernehmen, klicken Sie oben auf **Save Settings**.