

Anleitung zur Einrichtung von Ausgangs- und Eingangsfiltern

Für DIR-506L (Stand April 2013)

Die Eingangs- und Ausgangsfilter stehen im DIR-506L nicht im Repeater- und Accesspoint-Modus zur Verfügung.

Verbinden Sie den Rechner per WLAN auf den DIR-506L. Beachten Sie bitte die Anleitung zur Schnellkonfiguration, die dem DIR-506L beiliegt. Im Router Modus (Voreinstellung) ist der DIR-506L nicht per LAN ansprechbar, da sein Netzwerk-Anschluss in diesem Modus der WAN-Port (Internet-Port) ist.

1. Greifen Sie per Webbrowser auf die Konfiguration des DIR-506L zu. Die Standard Adresse ist <u>http://192.168.0.1</u> .

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

1=1.....

Datei Bearbeiten	Ansicht Chronik Lesezeichen Extras Hilfe			
€ ⇒ ☆	S (@ 192.168.0.1		🚍 🍲 マ 😋 🛃 - Google	2
D 192 168 0 1	192 168 0 50 💆 192 168 1 1 🗌 192 168 15 1 🗍 DEL DEL-160		(A LM Speedtest III DNS Resolver Check D version by D info b	d »
ROLITER	+			
Acced (Produktseite : DIR-506L		Firmware-Version : V2.13(EU)	
	D-Link			
	ANNELDEN			
	Am Router anmelden :		_	
		Providence of the second		
		Kennwort : Anmelden		
		Copyright © 2004-2012 D-Link Systems, Inc.		
@ ▼ ×				



3. Wählen Sie wenn möglich oben rechts die Sprache der Konfigurationsoberfläche des DIR-506L aus.



4. Klicken Sie auf Abbrechen.





Ausgangsfilter

- 1. Wählen Sie oben das Menü **Erweitert** und links das Menü **Ausgangsfilter** aus.
- 2. Setzen Sie bei **Ausgangsfilter** einen Haken.

Soll der Ausgangsfilter so konfiguriert werden, dass die angegebene Regel dazu dient um zu blocken und alle anderen haben weiterhin freien Zugang zum Internet, aktivieren Sie **Alle passieren lassen, außer jene, die den folgenden Regeln entsprechen**.

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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist 0.0.0.0 und als **Ziel-Port** ist 1-65535 anzugeben.

Rechts neben der Regel unter **Aktivieren** 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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist die des Ziels, in Beispiel hier die 194.25.166.240. Als **Ziel-Port** ist 1-65535 anzugeben.

Rechts neben der Regel unter **Aktivieren** 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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist 0.0.0.0 anzugeben. Als **Ziel-Port** ist 21 anzugeben.

Rechts neben der Regel unter **Aktivieren** setzen Sie noch einen Haken.

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



Produktseite : DIR-5	506L					De	eutsch 🗾 Firmw	are-Version : V2.13(EU)
D-I im	1,-							
DIR-506L	SET	UP	ERWEITE	RT	TOOLS		STATUS	SUPPORT
VIRTUELLER SERVER	AUSGAN	GSFILTER						Nützliche Tipps
	Mithilfe ein gelten für	es Paketfilters k alle ausgehende	können Sie ste en Datenpaket	uern, welche P :e.	akete den Rou	ter passieren	dürfen. Ausgangs	filter Mithilfe
URL-FILTER	Einstellung	en speichern	Einstellungen n	icht speichern				Paketfilters können Sie
AUSGANGSFILTER	AUSCAN		NETELLUNG					steuern,
	AUSGAN		norfiltor ·	Z Aktiviaran				Datenpakete den Router passieren
ROUTING		Ausya	ingsnicer .	AKUWETEH				dürfen. Ausgangsfilter
	Z	eitplanregel v	erwenden	-IMMER AKTIV	Kopieren	nach ID	-	gelten für alle ausgehenden
ERWEITERTES	AUSGAN	GSFILTER-RE	GELLISTE					Eingangsfilter gelten
NETZWERK		Alle p	assieren lasser	n, außer jene, d	die den folgend	len Regeln ent	sprechen.	dagegen für Datenpakete,
	Kennung	C A Quell-I	lle ablehnen, a P:Ports	ußer jene, die Ziel-I	den folgenden P:Ports	Regeln entspr Aktivieren	echen. Zeitplanreg	virtuelle virtuelle Server oder
Omine	1	192, 168, 0, 100	: 1-65535	0.0.0.0	:[1-65535	N		DMZ-Hosts bestimmt sind.
Neu starten							Neue Regel hinzu	fügen Sie konnen eine der zwei Filterrichtlinien
	2	192.168.0.101	: 1-65535	194.25.166.24	1-65535		Neue Regel hinzu	fügen
	з	192.168.0.102	:1-65535	0.0.0.0	:21		Neue Regel hinzu	filen
		r		·		_		Fienr
	4	1	1		9		Neue Regel hinzu	fügen
	5	ſ	;		:		Neue Regel hinzu	fügen
	6		:		:		New Read	
							Neue Regel hinzu	
	7	I	;]	1		Neue Decel hinzu	ficen

Soll der Ausgangsfilter so konfiguriert werden, dass die angegebene Regel dazu dient um zuzulassen und allen anderen den Zugang zum Internet zu blockieren, aktivieren Sie **Alle ablehnen, außer jene, die den folgenden Regeln entsprechen**.

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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist 0.0.0.0 und als **Ziel-Port** ist 1-65535 anzugeben.

Rechts neben der Regel unter **Aktivieren** 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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist die des Ziels, in Beispiel hier die 194.25.166.240. Als **Ziel-Port** ist 1-65535 anzugeben.

Rechts neben der Regel unter Aktivieren 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 **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist 0.0.0.0 anzugeben. Als **Ziel-Port** ist 21 anzugeben.

Rechts neben der Regel unter **Aktivieren** setzen Sie noch einen Haken.

Produktseite : DIR-5	506L					De	eutsch 💌 Firmware-V	ersion : V2.13(EU)
D.T.S.to								
DIR-506L	SET	rup	ERWEITE	RT	TOOLS		STATUS	SUPPORT
VIRTUELLER SERVER	AUSGAN	GSFILTER						Nützliche
ANWENDUNGSREGELN	Mithilfe ein	es Paketfilters k	önnen Sie ste	uern, welche Pak	kete den Rou	ter passieren (dürfen. Ausgangsfilter	• Mithilfe
MAC-ADRESSFILTER	gelten für	alle ausgehende	en Datenpaket	ie.				eines Paketfilters
URL-FILTER	Einstellung	gen speichern	Einstellungen n	icht speichern				können Sie steuern,
	AUSGAN	GSFILTER-EI	NSTELLUNG					welche Datenpakete
SNMP		Ausga	ngsfilter : 🖟	Aktivieren				den Router passieren
ROUTING					- 1100 - C			dürfen. Ausgangsfilter
ERWEITERTE DRAHTLOSEINSTELLUNGE	Z	eitplanregel v	erwenden	-IMMER AKTIV	 Kopieren r 	nach ID	•	gelten für alle ausgehenden Datenpakete.
ERWEITERTES	AUSGAN	GSFILTER-RE	GELLISTE					Eingangsfilter gelten
	2	C Alle p	assieren lasser	n, außer jene, die	den folgend	en Regeln ent	sprechen.	dagegen für Datenpakete, die nur für
Internet Offline	Kennung	Quell-I	P:Ports	Ziel-IP:	Ports	Aktivieren	Zeitplanregelnr.	virtuelle Server oder
Neu starten	1	192.168.0.100	:1-65535	0.0.0.0	:1-65535	•	Neue Regel hinzufügen	bestimmt sind. Sie können
	2	192.168.0.101	: 1-65535	194.25.166.240	: 1-65535	N	Neue Regel hinzufügen	Filterrichtlinien wählen:
	3	192.168.0.102	:1-65535	0.0.0.0	:21	•	Neue Regel hinzufügen	··· Mehr
	4		:		:		Neue Regel hinzufügen	
	5		:		:		Neue Regel hinzufügen	
	6	[;		;		Neue Regel hinzufügen	
	7	[:		:		Neue Reael hinzufüaen	

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



Eingangsfilter

- 1. Wählen Sie oben das Menü **Erweitert** und links das Menü **Eingangsfilter** aus.
- 2. Setzen Sie bei **Eingangsfilter** einen Haken.

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

Kennung	Service-Ports	Server-IP: Port		Aktivieren	Zeitplanregelnr.	
1	21	192.168.0.100	:		Neue Regel hinzufügen	

Soll der Eingangsfilter 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

Alle passieren lassen, außer jene, die den folgenden Regeln entsprechen.

Beispiel ID1:

Der im Internet befindliche Rechner 217.6.104.121 soll keinen Zugriff auf die Portfreigabe haben.

Seine IP 217.6.104.112 und der Portbereich 1-65535 ist als **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist die des lokalen FTP Server und als **Ziel-Port** ist 21 anzugeben.

Produktseite : DIR-5	506L			D	eutsch 💌 Firmware	-Version : V2.13(EU)
DIS						
DENIL						
DIR-5061	SETTIP	ERWEITE		<	STATUS	SUPPORT
	JETOT	EKWEITE		-		JULIONI
VIRTUELLER SERVER	EINGANGSFI	LTER				Nützliche Tipps
ANWENDUNGSREGELN	Mithilfe eines Pa	aketfilters können Sie ste	uern, welche Pakete de	n Router passieren	dürfen. Eingangsfilte	T. Nitholfo
MAC-ADRESSFILTER	gelten für Date	npakete, die nur für virtu	ielle Server oder DMZ-Ho	sts bestimmt sind.		eines
URL-FILTER	Einstellungen s	eichern Einstellungen n	icht speichern			Paketfilters können Sie
AUSGANGSFILTER			<i>u</i> :			steuern, welche
EINGANGSFILTER	EINGANGSFI	LTER-EINSTELLUNG				Datenpakete den Pouter
SNMP		Eingangsfilter :	Aktivieren			passieren
ROUTING	7.14.0					Ausgangsfilter
	Zeitp	anregei verwenden [ieren nach ID	×	ausgehenden
ERWEITERTES	EINGANGSFI	LTER-REGELLISTE				Eingangsfilter
NETZWERK		• Alle passieren lasser	n, außer iene, die den fo	laenden Reaeln en	tsprechen.	dagegen für Datenpakete
		C Alle ablehnen, a	ußer jene, die den folge	nden Regeln entspi	rechen.	die nur für
Internet Offline	Kennung	Quell-IP:Ports	Ziel-IP:Ports	Aktivieren	Zeitplanregelr	Server oder
	1 217	.6.104.121 :1-65535	192, 168, 0, 100 :21			bestimmt sind.
Neu starten	- 1	, , , , , , , , , , , , , , , , , , ,	, inclusion of the second		Neue Regel hinzufüg	eine der zwei
	2					Filterrichtlinien wählen:
					Neue Regel hinzufüg	en
	3	:	· · · · · · · · · · · · · · · · · · ·		Neue Degel histofic	en la de
						Mehr
	4	:	:		11 10 10 10 10 10 10 10 10 10 10 10 10 1	



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

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

Soll der Eingangsfilter 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

Alle ablehnen, außer jene, die den folgenden Regeln entsprechen.

Beispiel ID1:

Der im Internet befindliche Rechner 217.6.104.121 soll der einzige sein, der Zugriff auf die Portfreigabe hat.

Seine IP 217.6.104.112 und der Portbereich 1-65535 ist als **Quell-IP:Port** anzugeben. Als **Ziel-IP** ist die des lokalen FTP Server und als **Ziel-Port** ist 21 anzugeben.

Produktseite : DIR-	506L					De	utsch 🛒 Firmware	e-Version : V2.13(EU)		
D-I in	1,-									
DIR-506L	SET	UP	ERWEITE	RT	TOOLS		STATUS	SUPPORT		
IRTUELLER SERVER	EINGANG	EINGANGSFILTER								
NWENDUNGSREGELN	Mithilfe ein	es Paketfilters kö	önnen Sie ste	uern, welche Pa	kete den R	outer passieren d	lürfen. Eingangsfilte	er • Mithilfe		
AC-ADRESSFILTER	geiten für	Datenpakete, di	e nur tur virtu	lelle Server oder	DMZ-HOSTS	Destimmt sind.		eines Paketfilters		
RL-FILTER	Einstellung	en speichern	Einstellungen n	icht speichern				können Sie steuern.		
JSGANGSFILTER	EINGANG	SFILTER-EIN	STELLUNG					welche Datenpakete		
		Eingar	nasfilter : [Aktivieren				den Router passieren		
				- Hitemeren				dürfen. Ausoanosfilt		
RWEITERTE	Z	eitplanregel ve	rwenden	-IMMER AKTIV	 Kopiere 	en nach 🛛 🖬 🗔	•	gelten für all ausgehende		
	EINGANG	SFILTER-REG	ELLISTE					Datenpakete Eingangsfilte		
		C Alle pa	assieren lasser e ablehnen, a	n, außerjene, di ußeriene, die d	e den folge en folgende	nden Regeln ent In Regeln entspr	sprechen. echen.	gelten dagegen für Datenpakete die nur für		
Internet Offline	Kennung	Quell-IP	P:Ports	Ziel-IP	Ports	Aktivieren	Zeitplanregel	nr. Server oder		
Neu starten	1	217.6.104.121	: 1-65535	192.168.0.100	:21		Neue Regel hinzufü	bestimmt sind gen		
	2		:	[:		Neue Regel hinzufü	Filterrichtlinie wählen:		
	3				-:[Neue Regel hinzufü	gen Mehr		
	4	[:		Neue Regel bipzufür	nen.		

Rechts neben der Regel unter **Aktivieren** setzen Sie noch einen Haken.

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