

# Grundlegende Informationen zur Einrichtung des Portforwardings beim DSR-1000N (FW 1.04B13).

## Szenario:

*Client/Benutzer aus dem Internet möchte auf einen Server im lokalem Netzwerk hinter einem DSR-1000N zugreifen.*

*(In diesem Beispiel soll auf die HTTP Weboberfläche eines Webservers zugegriffen werden, dieser läuft auf Port 1996 (Standard Port 80).)*

## 1.) WAN Status prüfen und ggfls. Internetverbindung herstellen

### WAN1 Information

<b>MAC Address:</b>	00:18:E7:CD:69:52
<b>IPv4 Address:</b>	192.168.30.2 / 255.255.255.252
<b>IPv6 Address:</b>	fe80::218:e7ff:fe8d:6952 / 64
<b>Wan State:</b>	UP
<b>NAT (IPv4 only):</b>	Enabled
<b>IPv4 Connection Type:</b>	Static IP
<b>IPv6 Connection Type:</b>	Dynamic IP (DHCPv6)
<b>IPv4 Connection State:</b>	Connected
<b>IPv6 Connection State:</b>	Not Yet Connected
<b>Link State:</b>	LINK UP
<b>WAN Mode:</b>	Use only single WAN port: Dedicated WAN
<b>Gateway:</b>	192.168.30.1
<b>Primary DNS:</b>	192.168.30.1
<b>Secondary DNS:</b>	192.168.10.1
<b>Primary DNS(IPv6):</b>	
<b>Secondary DNS(IPv6):</b>	

---

## 2.) „Custom Services“ für die gewünschte Verbindung anlegen

*Anmerkung: Das Anlegen von „Custom Services“ ist nur dann notwendig wenn noch kein Standardservice für die Firewallregeln angelegt wurde.*

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B12\_WW

**DSR-1000N** // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▾

Website Filter ▾

Firewall Settings ▾

Wireless Settings ▾

Advanced Network ▾

Routing ▾

Certificates

Users ▾

IP/MAC Binding

IPv6 ▾

Radius Settings

Switch Settings

**APPLICATION RULES** LOGOUT

Default Outbound Policy

Firewall Rules

Custom Services

Protocol	Interface	Outgoing Ports		Incoming Ports	
		Start Port	End Port	Start Port	End Port

UNIFIED SERVICES ROUTER

**Helpful Hints...**

Application rules are also referred to as port forwarding rules. Devices on the LAN or DMZ can send a request to the Internet along one of the defined outgoing ports, and then the configured rule will open the corresponding incoming port for the specified type of traffic coming from the WAN.

Note that port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.

[More...](#)

Klicken Sie auf Add um einen neuen Service anzulegen.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B12\_WW

**DSR-1000N** // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▾

Website Filter ▾

Firewall Settings ▾

Wireless Settings ▾

Advanced Network ▾

Routing ▾

Certificates

Users ▾

IP/MAC Binding

IPv6 ▾

Radius Settings

Switch Settings

**CUSTOM SERVICES** LOGOUT

This page allows a user to add a user defined custom service.

**Custom Services Configuration**

**Name:**

**Type:**

**ICMP Type:**

**Start Port:**

**Finish Port:**

UNIFIED SERVICES ROUTER

**Helpful Hints...**

You can add custom services from here and use them in your firewall rules.

[More...](#)

Bitte geben Sie wie im Beispiel angegeben, die Werte für den jeweiligen Service ein und klicken Sie zum Speichern auf „Save Settings“.

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B12\_WW

**D-Link**

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▶ Website Filter ▶ Firewall Settings ▶ Wireless Settings ▶ Advanced Network ▶ Routing ▶ Certificates Users ▶ IP/MAC Binding IPv6 ▶ Radius Settings Switch Settings

Operation succeeded

**CUSTOM SERVICES** LOGOUT

When you create a firewall rule, you can specify a service that is controlled by the rule.. Common types of services are available for selection, and you can create your own custom services. This page allows creation of custom services against which firewall rules can be defined. Once defined, the new service will appear in the List of Available Custom Services table.

**List OF Available Custom Services**

<input type="checkbox"/>	Name	Type	ICMP Type / Port Range
<input type="checkbox"/>	Webserver_HTTP	TCP	1996 - 1996

**UNIFIED SERVICES ROUTER**

**Helpful Hints...**  
While common services use known TCP/UDP/ICMP ports, many custom or uncommon applications require traffic to be sent through the firewall. This section allows you to define traffic type and static ports for a unique identifier and then create firewall rules for this user-defined service.  
[More...](#)

In der Übersicht sehen Sie den/die von Ihnen angelegten Custom Service(s).

### 3.) Anlegen einer Firewall Regel für den soeben angelegten „Custom Service“

Product Page: DSR-1000N Hardware Version: A1 Firmware Version: 1.03B12\_WW

**D-Link**

DSR-1000N // SETUP ADVANCED TOOLS STATUS HELP

Application Rules ▶ Website Filter ▶ Firewall Settings ▶ Wireless Settings ▶ Advanced Network ▶ Routing ▶ Certificates Users ▶ IP/MAC Binding IPv6 ▶ Radius Settings Switch Settings

**APPLICATION RULES** LOGOUT

Default Outbound Policy: enable port triggering rules and allows several operations on the rules.

**Application Rules**

Protocol	Interface	Outgoing Ports		Incoming Ports	
		Start Port	End Port	Start Port	End Port

**UNIFIED SERVICES ROUTER**

**Helpful Hints...**  
Application rules are also referred to as port forwarding rules. Devices on the LAN or DMZ can send a request to the Internet along one of the defined outgoing ports, and then the configured rule will open the corresponding incoming port for the specified type of traffic coming from the WAN.  
Note that port triggering is not appropriate for servers on the LAN, since there is a dependency on the LAN device making an outgoing connection before incoming ports are opened.  
[More...](#)

Klicken Sie auf Add um eine neue Firewall Regel anzulegen.

<ul style="list-style-type: none"> <li>Application Rules ▶</li> <li>Website Filter ▶</li> <li>Firewall Settings ▶</li> <li>Wireless Settings ▶</li> <li>Advanced Network ▶</li> <li>Routing ▶</li> <li>Certificates</li> <li>Users ▶</li> <li>IP/MAC Binding</li> <li>IPv6 ▶</li> <li>Radius Settings</li> <li>Switch Settings</li> </ul>	<p><b>Helpful Hints...</b></p> <p>If you are not an expert user, we recommend not to configure firewall rules and leave the router into default firewall configuration.</p> <p><a href="#">More...</a></p>
<p><b>FIREWALL RULES</b> <span style="float: right;">LOGOUT</span></p>	
<p>This page allows you to add a new firewall rule or edit the configuration of an existing firewall rule. The details will then be displayed in the List of Available Firewall Rules table on the Firewall Rules page.</p> <p style="text-align: center;"> <input type="button" value="Save Settings"/> <input type="button" value="Don't Save Settings"/> </p>	
<p><b>Firewall Rule Configuration</b></p> <p><b>From Zone:</b> INSECURE (WAN) ▼</p> <p><b>To Zone:</b> SECURE (LAN) ▼</p> <p><b>Service:</b> Webservice_HTTP ▼</p> <p><b>Action:</b> Always Allow ▼</p> <p><b>Select Schedule:</b>   ▼</p> <p><b>Source Hosts:</b> Any ▼</p> <p><b>From:</b> <input type="text"/></p> <p><b>To:</b> <input type="text"/></p> <p><b>Destination Hosts:</b> Any ▼</p> <p><b>From:</b> <input type="text"/></p> <p><b>To:</b> <input type="text"/></p> <p><b>Log:</b> Never ▼</p> <p><b>QoS Priority:</b> Normal-Service ▼</p>	
<p><b>Source NAT Settings</b></p> <p><b>External IP Address:</b> WAN Interface Address ▼</p> <p><b>Single IP Address:</b> <input type="text"/></p> <p><b>WAN Interface:</b> WAN1 ▼</p>	
<p><b>Destination NAT Settings</b></p> <p><b>Internal IP Address:</b> 192.168.20.252</p> <p><b>Enable Port Forwarding:</b> <input checked="" type="checkbox"/></p> <p><b>Translate Port Number:</b> 1996</p> <p><b>External IP Address:</b> Dedicated WAN ▼</p>	

Als Quelle für die Anfragen wird das Interface „Insecure (WAN)“ ausgewählt. Das Ziel für das Portforwarding ist das Interface „Secure (LAN)“. Den vorher angelegten „Custom Service“ hier als „Service“ auswählen. Unter dem Punkt „Action“ wird die Option „Always Allow“ angelegt.

Bei den NAT Einstellungen wird das Ziel und das Portforwarding für das anzusprechende Gerät (hier z.B.: lokale Webserver = 192.168.20.252 und http Port = 1996) eingetragen.

**! ab der Firmware 1.04B13 lassen sich die Portweiterleitungen auch gezielt in vorhandene VLANs legen !**

- Website Filter ▶
- Firewall Settings ▶
- Wireless Settings ▶
- Advanced Network ▶
- Routing ▶
- Certificates ▶
- Users ▶
- IP/MAC Binding ▶
- IPv6 ▶
- Radius Settings ▶
- Captive Portal ▶
- Switch Settings ▶
- Intel® AMT ▶

**FIREWALL RULES**
LOGOUT

This page allows you to add a new firewall rule or edit the configuration of an existing firewall rule. The details will then be displayed in the List of Available Firewall Rules table on the Firewall Rules page.

---

**Firewall Rule Configuration**

**From Zone:** INSECURE (WAN1/WAN2/WAN3 (3G Internet))

**Available VLANs:** Default

**To Zone:** SECURE (VLAN)

**Available VLANs:** 
 TEST\_CP  
 Default  
 TEST\_CP  
 MOBILEHOTSPOT

**Service:** Always Block

**Action:** Always Block

**Select Schedule:** |

**Source Hosts:** Any

**From:**

**To:**

**Destination Hosts:** Any

**From:**

**To:**

**Log:** Never

**QoS Priority:** Normal Service

If you are not an expert user, we recommend not to configure firewall rules and leave the router into default firewall configuration.

[More...](#)

- Application Rules ▶
- Website Filter ▶
- Firewall Settings ▶
- Wireless Settings ▶
- Advanced Network ▶
- Routing ▶
- Certificates ▶
- Users ▶
- IP/MAC Binding ▶
- IPv6 ▶
- Radius Settings ▶
- Switch Settings ▶

Operation succeeded

**FIREWALL RULES**
LOGOUT

A firewall is a security mechanism to selectively block or allow certain types of traffic in accordance with rules specified by network administrators. You can use this page to manage the firewall rules that control traffic to and from your network. The List of Available Firewall Rules table includes all firewall rules for this device and allows several operations on the firewall rules.

**List of Available Firewall Rules**

<input type="checkbox"/>	#	Status	From Zone	To Zone	Service	Action	Source Hosts	Dest Hosts	Local Server	Internet Dest	Log
<input type="checkbox"/>	1	Enabled	WAN	LAN	Webserver_HTTP	ALLOW always	Any		192.168.20.252:1996	WAN1	Never

**Move To:** First

**Helpful Hints...**

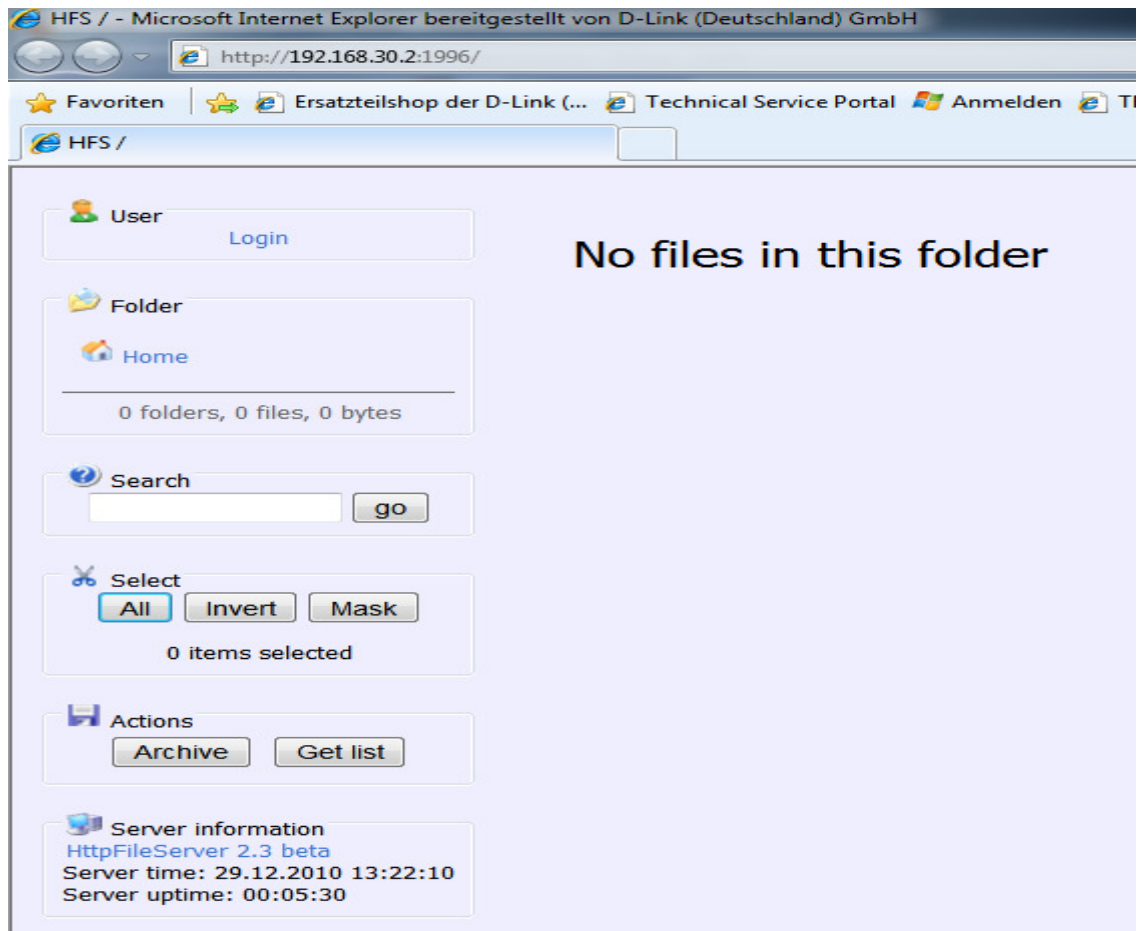
Inbound rules govern access from the WAN to the LAN or DMZ. Using firewall rules allow you to specify which local resources can be accessed from the internet. By default all access from the internet blocked from accessing the secure LAN, except in response to requests from the LAN or DMZ. Outbound (LAN/DMZ to WAN) rules restrict access to traffic leaving your network, selectively allowing only specific local users to access outside resources. Firewall rules are applied in the order listed. As a general rule, you should move the strictest rules (those with the most specific services or addresses) to the top of the list.

[More...](#)

In der Übersicht sehen Sie die von Ihnen angelegte(n) Firewall Regel(n).

#### 4.) Testen der Verbindung:

z.B.: im IE8 eingeben: <http://192.168.30.2:1996>



*Beachten Sie bitte, daß dieser Test von einem Rechner ausgeführt werden sollte, der nicht innerhalb des lokalen LANs verbunden ist, sondern von extern über die WAN Schnittstelle des DSR-1000N zugreift.*