

# **Grundlegende Informationen zur Einrichtung des Portforwardings beim DSR-500N/1000N (FW 202B501C).**

#### 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 1995.)

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

🍘 Status 🎅 Wireless 💂 N	letwork 🏠 VPN 🤮 Security 💇 Maintenance							
Status » System Information » Device » WAN1	0 0							
System LAN WAN1 WAN2 Wireless								
All of your WAN1 network connection details are displayed on t	he Device Status page.							
WAN1 Information								
Description	WAN1 Info							
MAC Address	14:D6:4D:1E:D2:51							
IPv4 Address	192.168.10.120 / 255.255.255.0							
IPv6 Address	N/A							
Status	UP							
IPv6 Connection Type	N/A							
IPv6 Connection State	IPv6 is disabled							
Prefix Obtained	N/A							
NAT (IPv4 Only)	Enabled							
IPv4 Connection Type	Static IP							
IPv4 Connection State	Connected							
Link State	LINK UP							
WAN Mode	Use only single port: WAN1							
Gateway	192.168.10.1							
Primary DNS	192.168.10.1							
Secondary DNS	8.8.8							
Disable								



#### 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.

	🝘 Status	🛜 Wireless	📃 Network	යි VPN	Security	Maintenance					
Security >	> Firewall » Custom	Services				3 6					
When you can creat service wi Custom	(hen 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 an create your own custom services. This page allows creation of custom services against which firewall rules can be defined. Once defined, the new ervice will appear in the List of Available Custom Services table.										
Show 10	♥ entries [Right	t click on record to get m	ore options ]			٩					
Name	🗘 Туре	⊖ Source Port Ran	ge ⇔	ICMP Type / D	estination Port Rang	e e					
			No data ava	ailable in table							
Showing (	Showing 0 to 0 of 0 entries Next > Last >										
Add N	ew Custom Servic	e									

Klicken Sie auf "Add New Custom Service" um einen neuen Service anzulegen.

Name	WebServer_HTTP	
Туре	ТСР	
Port Type	Port Range O Multiple Ports	
Source Start Port	1 [Range : 1 - 65535]	
Source Finish Port	<b>65535</b> [Range : 1 - 65535]	
Destination Start Port	<b>1995</b> [Range: 1 - 65535]	
Destination Finish Port	<b>1995</b> [Range: 1 - 65535]	

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

Der Source Start Port und Source End Port definieren die Quell-Portnummer der TCP/UDP Session des anfragenden Gerätes.

Da gemäß Standard dieser Quellport dynamisch ist, muss hier die komplette Portrange angegeben werden.

Der Destination Start/End Port ist der Port Ihres lokalen Services hinter dem DSR-Gerät.



	🕜 Statı	is 🔹	🛜 Wireless	📃 Network	6	3 VPN	🔒 Security	笷 Maintenance		
Security » Firewall » Custom Services										
			69	Operati	on Suc	ceeded				
When you can create service wi	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.									
Custom	Services Li	st								
Show 10	✓ entries	[Right click	on record to get	t more options ]					٩	
Name		🗘 Туре	e ⊖ Sour	ce Port Range	⇔	ІСМР Тур	pe / Destination Po	ort Range	⇔	
WebServe	r_HTTP	TCP	1-6553	35		1995-1995				
Showing 1	to 1 of 1 entries						KIF	First I Previous 1 Next >	Last 刘	
Add N	ew Custom S	ervice								

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

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

🕜 Status	🛜 Wireless	💻 Network	CB VPN	Security	<b>©°</b> Maintenance				
Security » Firewall » Firewall	Rules » IPv4 Firewall	Rules				00			
IPv4 Firewall Rules IPv	6 Firewall Rules B	ridge Firewall Rules							
A firewall is a security mechan You can use this page to manag firewall rules for this device ar Firewall Rules	ism to selectively blo e the firewall rules t nd allows several ope	ock or allow certain ty that control traffic to rations on the firewall	pes of traffic in acc and from your netw l rules.	cordance with rules spe rork. The List of Availab	cified by network adminis le Firewall Rules table in:	trators. cludes all			
Default Outbound Policy Always	Default Outbound Policy for IPv4 Always O Block								
IPv4 Firewall Rules Lis	Save Cancel IPv4 Firewall Rules List								
Show 10 v entries [Right	nt click on record to ge	t more options ]				٩			
Status <sub>⊕</sub> From <sub>⊕</sub> To Zone⊕ Zone	eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee	lock / ⊖ Source ⊖ Hosts	$\begin{array}{c} \text{Destination} \\ \text{Hosts} \end{array} \\ \end{array} \\ \begin{array}{c} \ominus \end{array}$	Local Server $\ominus$ Internet Destinati	on ⊖ Log <sub>⊖</sub> Rule Pri	<sup>ority</sup> ⊖			
		No data a	vailable in table	16					
Showing 0 to 0 of 0 entries				KI Fi	rst 🔄 Previous Next 🗲	Last 刘			
Add New IPv4 Firewall	Rule								

Klicken Sie auf "Add New IPv4 Firewall Rule" um eine neue Firewall Regel anzulegen.



	IPv4 Firewall	l Rules C	onfiguratio	on						×	
	From Zone				ISECURE (WAN)						
Securit	To Zone	To Zone				SECURE (LAN)					
	Service			WebSe	WebServer_HTTP						
IP	Action			Always	Allow	~					_
A firev	Source Hosts			• An	y O Sing	le Address O A	ddress range				s. s.all
irewa	Log			• Ne	ever O Al	ways					
Firew	Destination I	NAT Setti	ngs								
Def	Internal IP /	Address		192.1	68.0.3						
AI	Enable Port	Forwardin	g		OFF						
	External IP	Address		Dedica	ated WAN	$\checkmark$					
IPv										0	
Sho										Save	
St	atus <sub>⊕</sub> From <sub>⊕</sub>	To 7000 ⊕	Service <sub>⊖</sub>	Block / ↔	Source 😝	Destination 🕀	Local ⊖	Internet	Log <sub>⇔</sub>	Rule Priority	/ ⇔
	Zone	Zone		Allow	No data a	available in table	Server	Descination			
Showing 0 to 0 of 0 entries Next > Last >											
A	dd New IPv4 Fi	rewall Rul	e								

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 für das anzusprechende Gerät (hier z.B.: lokale Webserver = 192.168.0.3) eingetragen. Der Zielport wird über die vorher angelegte Custom Rule definiert (z.B. 1995)

Security » Firewall » Firewall Rules » IPv4 Firewall	Rules			00					
IPv4 Firewall Rules IPv6 Firewall Rules	Bridge Firewall Rules								
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. Firewall Rules									
Default Outbound Policy for IPv4									
Always	● Allow ○ Block								
IPv4 Firewall Rules List	Save Cancel								
Show 10 entries [Right click on record to ge	et more options ]			٩					
$\begin{array}{c c} Status & From \\ Zone & Zone \\ \end{array} \begin{array}{c} To \\ Zone \\ \end{array} \begin{array}{c} Service \\ e \\ \end{array}$	Block / $\ominus$ Source Destination	n⊖ Local ⊖ Inter Server ⊖ Dest	rnet ination <sup>⊕</sup> Log <sub>⊕</sub>	Rule Priority $_{\ominus}$					
Enabled WAN LAN WebServer_HTTP	Allow Always Any	192.168.0.3 WAN1	Never	1					
Showing 1 to 1 of 1 entries		🕅 Fir	st Previous 1	Next > Last >					
Add New IPv4 Firewall Rule									



Sollten Sie eine Port Translation durchführen, so müssen Sie die Firewall Rule entsprechend anpassen.

	IPv4 Firewall Rules Configuration		
	From Zone	INSECURE (WAN)	
ecurity	To Zone	SECURE (LAN)	
	Service	WebServer_HTTP_R	
	Action	Always Allow	
IPv	Source Hosts	Any O Single Address O Address range	
firew	Log	O Never O Always	irs.
irewall	Destination NAT Settings		es att
irewa	Internal IP Address	192.168.0.3	- 10
	Enable Port Forwarding		
Defa	anslate Port Number	10000	
Au	External IP Address	Dedicated WAN	
IPv4		Save	

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 für das anzusprechende Gerät (hier z.B.: lokale Webserver = 192.168.0.3) eingetragen. Der Zielport wird über die "Translate Port Number" neu definiert. (z.B. 10000)

	IPv4 Fire	ewall Rule	es IPv6	Firewall Rules	Bridge Firewall	Rules					
A Yc fii Fi	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. Firewall Rules										
	Default Outbound Policy for IPv4         Always       Image: Allow O Block         Save       Cancel										
	IPv4 Fire	wall Ru	les List es [Right	t click on record to g	et more options ]						٩
	Status	From Zone	To Zone <sup>⊕</sup>	Service 😜	Block / OR Allow	Source Hosts	Destination <sub>0</sub> Hosts	Local Server ⊖	Internet Destination <sup>⊕</sup>	Log <sub>⇔</sub>	Rule Priority
	Enabled	WAN	LAN	WebServer_HTTP	Allow Always	Any		192.168.0.3	WAN1	Never	1
Ŀ	Enabled	WAN	LAN	WebServer_HTTP_R	Allow Always	Any		192.168.0.3	WAN1	Never	2
	Showing 1 to 2 of 2 entries										
	Add New IPv4 Firewall Rule										

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



#### 4.) Testen der Verbindung:

z.B.: im IE11 eingeben: http://192.168.10.120:1995





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-Gerätes zugreift.