DI-604 Rev.D / DI-707P Rev.C Port öffnen mit Zugriffsbeschränkung

(nur eine IP Adresse aus dem Internet darf auf die Portfreigabe zugreifen) Getestet mit Firmware 3.09

I Port freischalten:

- 1. Greifen Sie auf die Konfiguration des Routers zu.
- 2. Wählen Sie oben Advanced und links Virtual Server aus.

3. Zur Öffnung des oder der entsprechenden Ports aktivieren Sie Enabled.

Geben Sie der Regel einen Namen und tragen die IP Adresse des Rechners im Netzwerk ein, der freigeschaltet werden soll.

Wählen Sie den Protokoll Typ aus (TCP, UDP oder Both für beides) und tragen bei Private und Public Port die freizuschaltenden Ports ein.

Diese sind i.d.R. identisch einzutragen, außer es soll ein Port Redirect stattfinden. Bei Schedule wählen Sie Always aus wenn die Regel immer gelten soll.

Klicken Sie nun auf Apply und dann nachfolgend auf Continue.



II Zugriff auf die Portfreigabe begrenzen:

4. Wählen Sie oben Advanced und links Firewall aus.

5. Aktivieren Sie Enabled und geben der Regel einen Namen.

Bei Action wählen Sie Deny aus.

Bei Source wählen Sie WAN aus und bei IP Start tragen Sie ein Sternchen "*" für alle ein. Bei Destination wählen Sie LAN aus und tragen bei IP Start die IP Adresse des Servers, den Sie zuvor bei Virtual Server freigeschaltet hatten, ein.

Wählen Sie auch hier bei Protocol und Port Range die zuvor unter Virtual Server freigeschalteten Ports aus.

Bei Schedule wählen Sie Always aus und klicken auf Apply und danach auf Continue.

A construction of the construction of	📓 Favoriten 🛞 Medien 🎯 🛛 🕏 🕇	🕘 H				
Adresse 🕘 http://192.168.0.1/						
inks 🝘 192,168.0,1 🖉 192,168,1,1 🛃 192,16	68.0.50 どDCS-1000W 🖉DES-32	50TG 🕘DES-3308TG 🧃	DES-3326 🛛 👸 DES-362	4i 🍓 DES-6000 🏽 🕘 DF	E-100 🕘DI-304	,
	Home Adv	anced Tools	s Status	Help		-
	Firewall Rules Firewall Rules can be used	I to allow or deny traffic fro	om passing through the l	DI-604.		
Virtual Server	• Enabled	C Disabled				
	Action Caller (2.0				
Application	Interface	● Deny IP Start IP End	Protocol I	Port Range		
	Source VVAN -					
Filter	Destination LAN -	192.168.0.144	TCP 💌	1001 -1002		
	Schedule C Alw					
Contraction of the second s		anity .				
Firewall	C Ero	ays m Time 00 🕶 00 🔹	To 00 + 00 +			
Firewall	C Fro	ays m Time 00 ▼:00 ▼ day Sun ▼ to Su				
DDNS	C Fro	ays m Time 00 ♥ 00 ₪ day Sun ♥ to Si				22
DDNS	C Fro	m Time 00 ⊥ 00 ∎ day Sun ⊥ to Si	то 00 • 00 • л •	00		
Firewall DDNS DMZ	C Fro	m Time 00 ▼ 00 ∎ day Sun ▼ to So		Cancel Help		
	C Fro	ays m Time 00 ▼ 00 s day Sun ▼ to S	To OO ▼ OO ▼ Jn ▼ Apply	Cancel Help		
	C Fro Firewall Rules List Action Name	ays m Time 00 ▼ 00 s day Sun ▼ to S Source	To OO Y OO Y	Cancel Help		
	C Fro	m Time 00 ▼ 00 day Sun ▼ to S Source WAN,217.233.231	To 00 Y 00 Y In Y Apply Destination P 28 LAN, 192.168.0.144 T	Cancel Help Trotocol CP,1001- 002 10		
DDNS	C Fro Firewall Rules List Action Name	m Time 00 100 day Sun to S Source WAN,217.233.231	To 00 ▼ 00 ▼ an ▼ Destination P 28 LAN,192.168.0.144 T LAN,192.168.0.144 T	Image: Cancel Help rotocol CP,1001- Image: Transformed to the second to t		
	C Fro	m Time 00 100 day Sun to S Source WAN,217.233.231 WAN,* WAN,*	Destination P 28 LAN,192.168.0.144 LAN,192.168.0.144 LAN,192.168.0.144	Cancel Help rotocol CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- CP,		
DDNS	C Fro	m Time 00 100 day Sun to S Source WAN,217.233.231 WAN,* WAN,* N portWAN,*	Destination P 28 LAN, 192.168.0.144 LAN, 192.168.0.144 LAN, 192.168.0.144 WAN,* U	Image: Constant of the second seco		
DDNS	C Fro	m Time 00 100 day Sun 10 5 Source WAN, 217.233.231 WAN,* WAN,* N port WAN,*	Destination P 28 LAN,192.168.0.144 LAN,192.168.0.144 LAN,192.168.0.144 UAN,192.168.0.144 LAN,192.168.0.144 T	Cancel Help Help CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- CP,100		
DDNS	C Fro	m Time 00 ▼ 00 ▼ day Sun ▼ to S Source WAN,217.233.231 WAN,* WAN,* N port WAN,* *,* LAN,*	Destination P 28 LAN,192.168.0.144 LAN,192.168.0.144 UAN,192.168.0.144 LAN,192.168.0.144 T	Cancel Help Trotocol CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- 002 CP,1001- CP,100-		

6. Als letztes benötigen Sie noch eine weitere Regel, auch hier weiterhin unter Advanced – Firewall, um letztendlich festzulegen, welche IP Adresse auf die Portfreigabe zugreifen darf.

Aktivieren Sie Enabled und geben auch dieser Regel einen Namen.

Bei Action wählen Sie Allow aus.

Bei Source wählen Sie WAN aus und bei IP Start tragen Sie die IP Adresse des Rechners ein, der als einziger auf die Portfreigabe zugreifen darf.

Bei Destination wählen Sie LAN aus und tragen bei IP Start die IP Adresse des Servers, den Sie zuvor bei Virtual Server freigeschaltet hatten ein, so wie auch bei der Firewall Regel zuvor.

Wählen Sie auch hier bei Protocol und Port Range wie zuvor die Ports aus.

Bei Schedule wählen Sie Always aus und klicken auf Apply und danach auf Continue.

Zurück 🔹 🔿 🖉 🖄 🖄 Suchen 🖪	Eavoriten Medien					
	ardionical Quincian C					
@102168.0.1 @102168.1.1 @10216	8 0 50 and 50 and 50		5.3308TC SDE5.33	226 ADES.3624	@DES-6000 @DB	a.100 SDT-304
Strendon Strendonn Strend						
	Home	Advanced	Tools	Status	нер	
	Firewall Rules Firewall Rules can	be used to allow or d	eny traffic from pass	ing through the D	ŀ604.	
	•	Enabled O Disable	d			
Virtual Server	Name 3					
(and the second	Action 📀 ,	Allow C Deny				
Application	Inter	face IP Start	IP End	Protocol P	ortRange	
Filter	Source WA	N 🗾 217.233.231.2	8			
	Destination LAN	1 192.168.0.144		TCP 🗾 1	001 - 1002	
Firewall	Schedule	Always				
		C From Time	00 💌 : 00 💌 To 00			
DDNS		day S	un 💌 to Sun 💌			
				S	🖸 🕻 🕻	
DMZ				Apply	Cancel Help	
	Action Name	st Source	e Dest	ination Pr	otocol	
	Allow 3	WAN,2	17.233.231.28 LAN,	192.168.0.144 TC	P,1001-	
	E Dawy 2	lazahi +	1.0.01	1024000444	P,1001-	
	M Deny 2	WAN,"	LAN,	192.168.0.144	02	
	Allow 1	WAN,*	LAN,	192.168.0.144 10 10	02	
	🔽 Allow Allow to F	Ping WAN port WAN,*	WAN	l,* IC	MP,*	
	Deny Default	*,*	LAN,	* *,*	s -	
	Allow Default	1 AN *	* *	* *	n 🛛	