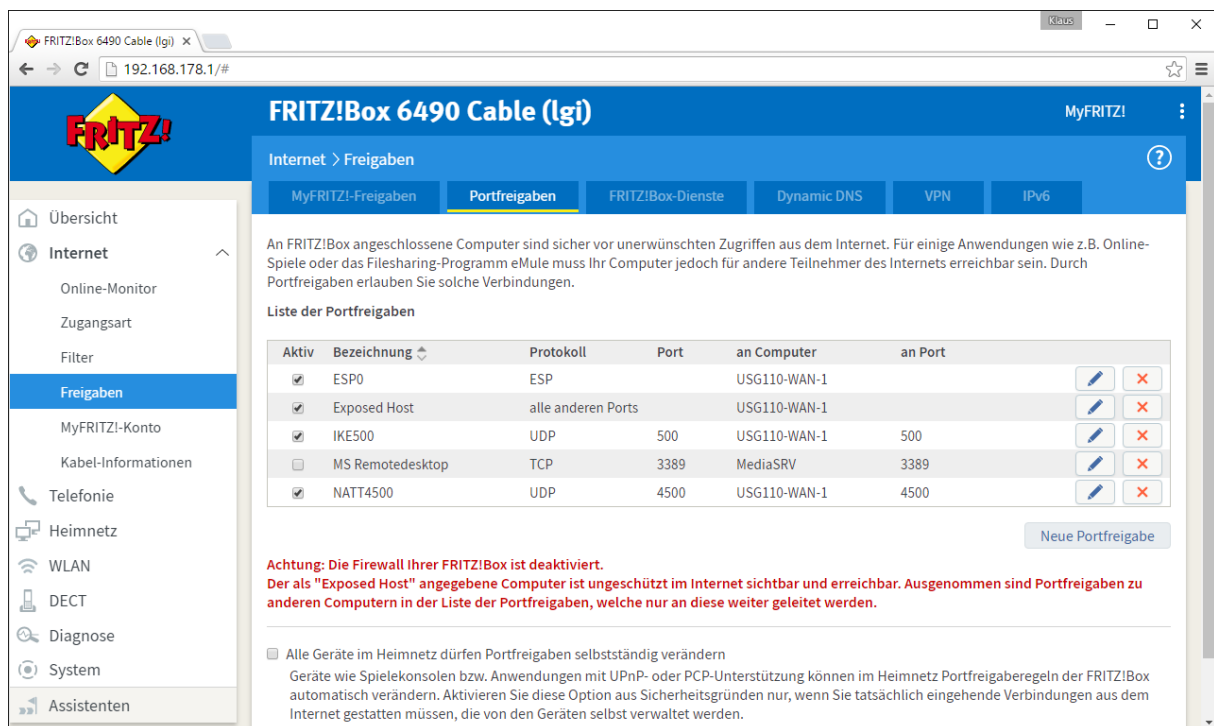


Set WAN-1 USG-IP-Address static DHCP in Fritz!Box, so the WAN USG Interface get every time the same IP from FB as expected.

About NAT incoming to WAN1 IP USG set the following as below:

1. IKE UDP-Port 500 to WAN1-IP USG.
2. NATT UDP-Port 4500 to WAN1-IP USG.
3. ESP0 Protocol-50 to WAN1-IP USG.
4. And the exposed Host for any others to WAN1-IP USG.

So you not need set NATT in the VPN Tunnel of USG, because ESP0 also put in Internet Freigabe.



The screenshot shows the Fritz!Box 6490 Cable (lgi) web interface. The main heading is 'Internet > Freigaben'. Below this, there are tabs for 'MyFRITZ!-Freigaben', 'Portfreigaben', 'FRITZ!Box-Dienste', 'Dynamic DNS', 'VPN', and 'IPv6'. The 'Portfreigaben' tab is selected.

The main content area contains a warning message: 'An FRITZ!Box angeschlossene Computer sind sicher vor unerwünschten Zugriffen aus dem Internet. Für einige Anwendungen wie z.B. Online-Spiele oder das Filesharing-Programm eMule muss Ihr Computer jedoch für andere Teilnehmer des Internets erreichbar sein. Durch Portfreigaben erlauben Sie solche Verbindungen.'

Below the warning is a table titled 'Liste der Portfreigaben' with the following columns: 'Aktiv', 'Bezeichnung', 'Protokoll', 'Port', 'an Computer', and 'an Port'. The table contains five entries:

Aktiv	Bezeichnung	Protokoll	Port	an Computer	an Port
<input checked="" type="checkbox"/>	ESP0	ESP		USG110-WAN-1	
<input checked="" type="checkbox"/>	Exposed Host	alle anderen Ports		USG110-WAN-1	
<input checked="" type="checkbox"/>	IKE500	UDP	500	USG110-WAN-1	500
<input type="checkbox"/>	MS Remotedesktop	TCP	3389	MediaSRV	3389
<input checked="" type="checkbox"/>	NATT4500	UDP	4500	USG110-WAN-1	4500

Below the table is a button labeled 'Neue Portfreigabe'.

A warning message is displayed: 'Achtung: Die Firewall Ihrer FRITZ!Box ist deaktiviert. Der als "Exposed Host" angegebene Computer ist ungeschützt im Internet sichtbar und erreichbar. Ausgenommen sind Portfreigaben zu anderen Computern in der Liste der Portfreigaben, welche nur an diese weiter geleitet werden.'

At the bottom, there is a checkbox labeled 'Alle Geräte im Heimnetz dürfen Portfreigaben selbstständig verändern' with a sub-note: 'Geräte wie Spielekonsolen bzw. Anwendungen mit UPnP- oder PCP-Unterstützung können im Heimnetz Portfreigaberegeln der FRITZ!Box automatisch verändern. Aktivieren Sie diese Option aus Sicherheitsgründen nur, wenn Sie tatsächlich eingehende Verbindungen aus dem Internet gestatten müssen, die von den Geräten selbst verwaltet werden.'

So the remote Access to Fritz!box might https via 443, it's a good decision to change the Service of USG from 443 to 444 instead (and might handle via exposed Host as well).

1rst add an HTTPS2_444 Service to device:

The screenshot shows the ZyXEL USG110 configuration interface. The 'Service' tab is active, displaying a list of services. The service 'HTTPS_444' is highlighted in blue, indicating it is selected. The list includes various services like CU_SEEME_UDP2, DHCPv6_CLIENT, and others.

Service ID	Service Name	Protocol	Port	Count
15	CU_SEEME_UDP2	UDP	24032	1
16	DHCPv6_CLIENT	UDP	546	2
17	DHCPv6_SERVER	UDP	547	1
18	DNS_TCP	TCP	53	1
19	DNS_UDP	UDP	53	1
20	ESP	Protocol	50	2
21	FINGER	TCP	79	1
22	FTP	TCP	20-21	2
23	FTPS	TCP	990	0
24	GRE	Protocol	47	2
25	H323	TCP	1720	0
26	HPvritGrp	TCP	5223	0
27	HTTP	TCP	80	4
28	HTTPS	TCP	443	8
29	HTTPS_444	TCP	444	3
30	HTTP_8080	TCP	8080	3
31	HTTP_8081	TCP	8081	3
32	HTTP_8082	TCP	8082	3
33	HTTP_8084	TCP	8084	3
34	HTTP_8888	TCP	8888	3
35	Hpvroom_TCP	TCP	5228	1
36	Hpvroom_UDP	UDP	5228	1
37	IBM_Informix_SQL_UDP_9089	UDP	9089	0
38	ICMPv6_Echo	ICMPv6	/echo	1
39	ICMPv6_Echo-Replay	ICMPv6	/echo-reply	1

And add this in Service Group "Default-Allow-WAN-To-ZyWALL":

The screenshot shows the ZyXEL USG110 configuration interface with the 'Edit Service Group Rule Default-Allow-WAN-To-ZyWALL' dialog box open. The dialog box has a 'Configuration' section with 'Name' set to 'Default-Allow-WAN-To-ZyWALL' and 'Description' set to 'System Default Allow From V'. Below this, there are two lists: 'Available' and 'Member'. The 'Member' list contains the 'HTTPS_444' service, which has been added from the 'Available' list.

Family	Reference
1	1
2	0
3	0
4	5
5	0
6	1
7	0
8	0
9	1
10	0
11	1
12	1
13	0
14	2
15	2
16	2
17	2
18	0
19	0
20	1
21	0

Then change in Menu System / WWW at HTTPS the Port from 443 to 444:

The screenshot shows the ZyXEL USG110 configuration interface. The left sidebar contains a 'CONFIGURATION' menu with 'WWW' selected. The main content area is titled 'Service Control' and 'Login Page'. Under 'HTTPS', the 'Enable' checkbox is checked, and the 'Server Port' is set to 444. The 'Server Certificate' is set to 'default'. Below this is the 'Admin Service Control' table.

#	Zone	Address	Action
1	LAN1	LAN1_SUBNET	accept
2	LAN2	LAN2_SUBNET	accept
3	IPSec_VPN	LZTP_Pool	accept
4	IPSec_VPN	ZyXEL_LAN-Addr	accept
5	WAN	ZyXEL_WAN-Addr	accept
6	WAN	DemoUserGRP	accept
7	WAN	RD-Group_and_ZyDE	accept
8	WAN	Demo_185_22_143_18	deny
9	ALL	ALL	deny
-	ALL	ALL	accept

After this is changed, access the USG via <https://USG-IP:444/> from LAN / local or IPsec.
And via Internet by <https://DDNS:444/> depends from domain name / and or IP.