

This guide will demonstrate how to configure port forwarding on USG device. By doing this, clients from the Internet will be able to reach the web server on the LAN side by accessing <u>http://192.168.5.127:8090</u>

- 1. Open your web browser and type the IP address of the device into the address bar (default LAN IP address : 192.168.1.1)
- 2. Login (default username : admin Password: 1234)
- 3. Click Configuration > Network > NAT > Add

YXEL USG40				-			Welcome adm	in Liggent ?Help Z About 4	FSta Hisp 🔹 Otgest Reference 🖵
CONFIGURATION	NAT								
TY Quick Setup	Configuration								
Winkess Network Interface Routing Disks	Note: Fyou want to configure SNAT,	please go to <u>Policy Route</u>	the call Marce						
- RUAR	Status Priority	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
ALG L(Ph) L(Ph) L(Ph) L(Ph)MAC Binding DNS Indound LB Nikh Authinstadun Security Policy VPN VPN UTM Prufile Origect System Log & Report	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	U, I star of a	6073						in press

4. Click Create new Object > Address

📀 Add NAT	?	×
Create new Object -		
Address		
Service		
Enable Rule		
Rule Name:		
Port Mapping Type		
Classification:	Virtual Server	
Mapping Rule		
Incoming Interface:	wan1 👻	
Original IP:	User Defined	
User-Defined Original IP:	(IP Address)	
Mapped IP:	User Defined	
User-Defined Mapped IP:	(IP Address)	
Port Mapping Type:	any	
Related Settings		
Enable NAT Loopback	8	
Configure Security Policy		
	OK Cancel	



5. Add the object as shown below

Create Address			?
Name:	WebServerInside		
Address Type:	HOST	~	
IP Address:	192.168.10.10		
	User Defined		ancel

- 6. Click Create new Object > Service and specify the WAN side's service port
- 7. Finish adding the NAT rule as shown below

~
17
OK Cancel

8. Click Apply

INFORMATION	NAT								
TO Quick Setup Licensing	Configuration								
Winkess Network - Interface	Note: If you want to configure SNAT, ;	rease go to Patica Maxim							
- DONS	@ Add (2 tak (2 famore	Adula Q Parties	-Receive						
- HTTP Redrect	Status Priority	Name	Mapping Type	interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port
	Q 1	Web_to_LANside	Virtual Server	<u>*#011</u>	+WAN_INT	«WebServerInside	ka	 WANsideWittPart 	 LANsideWebPort
- ADP Sealtin Control VPH WMM UTH Profile Onject System Lug & Report									

9. Click Configuration > Security Policy > Policy Control > Add

Zywall Port forwarding

Products apply USG20/20W/40/40W/60/60W

E		DY
5/9	Inc	clude

	CONFIGURATION	Policy				and the second								
	T¥ Quick Setup	General Se	ttings											
D	Wireless Network	🔽 Enabl	ie Policy Cor	ntrol										
	- Routing - DDNS	IPv4 Config	guration Asymmetric	al Route										
	NAT HTTP Redirect	() Add	2 6dt. 🍵 A	emove 🤤 Activate. 🤤 In	activate 🦽 Hove									
	 ALG 	Priority -	Status	Name	From	То	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log	UTM Profile
	- UPnP	1	8	LAN1_Outgoing	- LAN1	any (Excluding Zy	any	алу	any	any	none	allow	ne	
	 DNS Inbound LB 	2		LAN2_Outgoing	«LAN2	any (Excluding Zy	any	any	any	any	none	allow	no	
	 Web Authentication 	3	- 9	DMZ_to_WAN	< DM2	< WAN	any	any	any	any	none	allow	no	
	Security Policy	4		IPSec_VPN_Outg	IPSec_VPN	any (Excluding Zy	any	any	any	any	none	allow	no	
	 Poncy control ADP 	5		SSL_VPN_Outgoing	SSL_VPN	any (Excluding Zy	any	апу	any	any	none	allow	no	
	 Session Control 	6		TUNNEL_Outgoing	 TUNNEL 	any (Excluding Zy	any	any	any	any	none	allow	no	
	© VPN	7	9	LAN1_to_Device	LAN1	ZyWALL	any	апу	any	апу	none	allow	no	
	- BWM	8		LAN2_to_Device	LAN2	ZyWALL	any	any	any	any	none	allow	no	
	Object	9		DMZ_to_Device	= DMZ	ZyWALL	any	апу	Default_Allow_D	any	none	allow	no	
	System	10		WAN_to_Device	= WAN	ZyWALL	any	any	Default_Allow_W	any	none	allow	no	
	Log & Report	11		IPSec_VPN_to_D	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
		12		SSL_VPN_to_Devi	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
		13		TUNNEL_to_Device	TUNNEL	ZyWALL	any	апу	any	any	none	allow	no	
		Default			any	any	any	any	any	any	none	deny	log	
		14 4 1	Page 1	of 1 > > Show 50	✓ items									Displaying 1 - 14 of 14

10. Create the firewall rule as shown below

Create new Object 🗸			
_			
C Enable			
Name:	WebInside		
Description:		(Optional)	
From:	WAN	~	
То:	LAN1	*	
Source:	any	*	
Destination:	WebServerInside	~	
Service:	WANsideWebPort	~	
User:	any	~	
Schedule:	none	~	
Action:	allow	~	
Log matched traffic:	no	~	

11. Click Apply to finish

ONFIGURATION	Policy												
1 ¥ Quick Setup	C												
Licensing	Grandical Sec	nu de											
Network	Enable	Policy Cor	lottr										
 Interface 	IPv4 Config	uration											
- Routing			d Decite										
- NAT	Allowy	aymmetric	a Noole										
 HTTP Redirect 	() A55	eat 📲 R	errove 🝟 Activate 👹 37	activate and Nove					harris			1	
+ ALG	Priority	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log	UTM Profile
IP/MAC Binding	-	-	LANI Outering	-1.001	and Control of the To-	any	A TREASE VELTISALE	a module meter on	any	1018	alou	110	
DNS Inbound LB	2		LAN2 Outpoing	aLAN2	any (Excluding Zy	any	30y	any	200	0008	slow		
Security Policy	4		DMZ to WAN	= DMZ	a WAN	any	any	any	any	0000	allow		
 Policy Control 	5		IPSec VPN Outo	IPSec VPN	any (Excluding Zy	any	any	any	any	0008	allow	00	
- ADP Receive Control	6		SSI VPN Outgoing	+ SSI VPN	any (Excluding Zy	env	env	any	any	none	alice	- 00	
VPN	7		TUNNEL Outgoing	TUNNEL	any (Excluding Zy	any	any	any	any	none	allow	no	
BWM	8		LAN1 to Device	LAN1	ZyWALL	any	any	any	any	none	allow	no	
Olim Profile	9		LAN2_to_Device	-LAN2	ZyWALL	any	any	any	any	none	allow	ne	
System	10		DMZ_to_Device	= DMZ	ZyWALL	алу	any	Default_Allow_D	any	none	allow	no	
Log & Report	11		WAN_to_Device	s WAN	ZyWALL	any	any	Default_Allow_W	any	none	allow	no	
	12		IPSec_VPN_to_D	RIPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
	13		SSL_VPN_to_Devi	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
	14	.	TUNNEL_to_Device	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
	Default			any	any	any	any	any	any	none	deny	log	
	13 14 Default	e Page 1	SBL_VPN_16_Device	SSL_VPN TUNNEL any kems	ZyWALL ZyWALL any	any any any	any any any	any any any	any any any	none	allow allow deny	no log	