www.zyxel.com

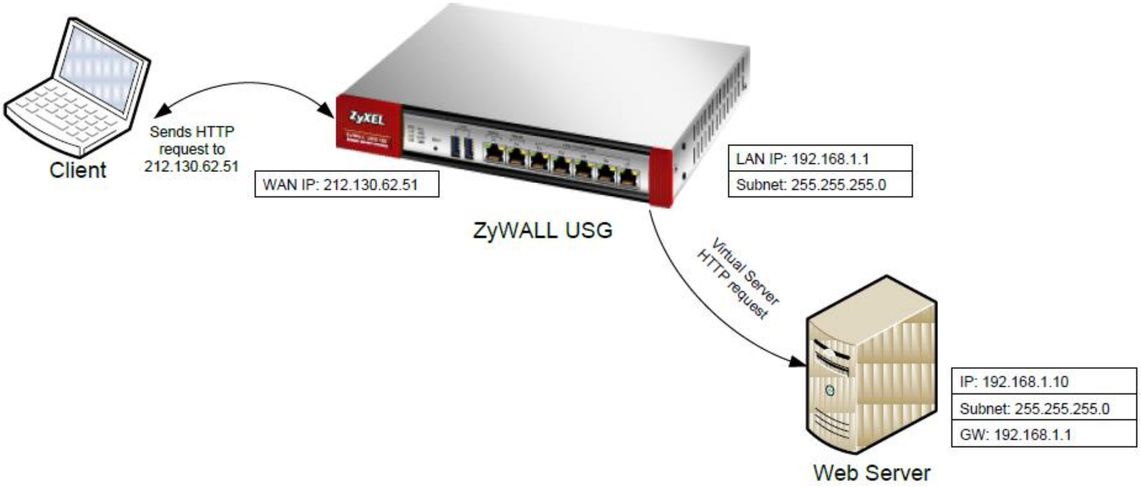
ZLD Series – Port Forwarding (NAT)

Virtual Server (Port Forwarding) Rule(s) Setup for 4.XX Firmware version and higher

Table of Contents

Scenario

With Virtual Server (Port Forwarding) the ZyXEL gateway forwards specific requests to the selected server/client. This guideline shows how to setup a Virtual Server rule.



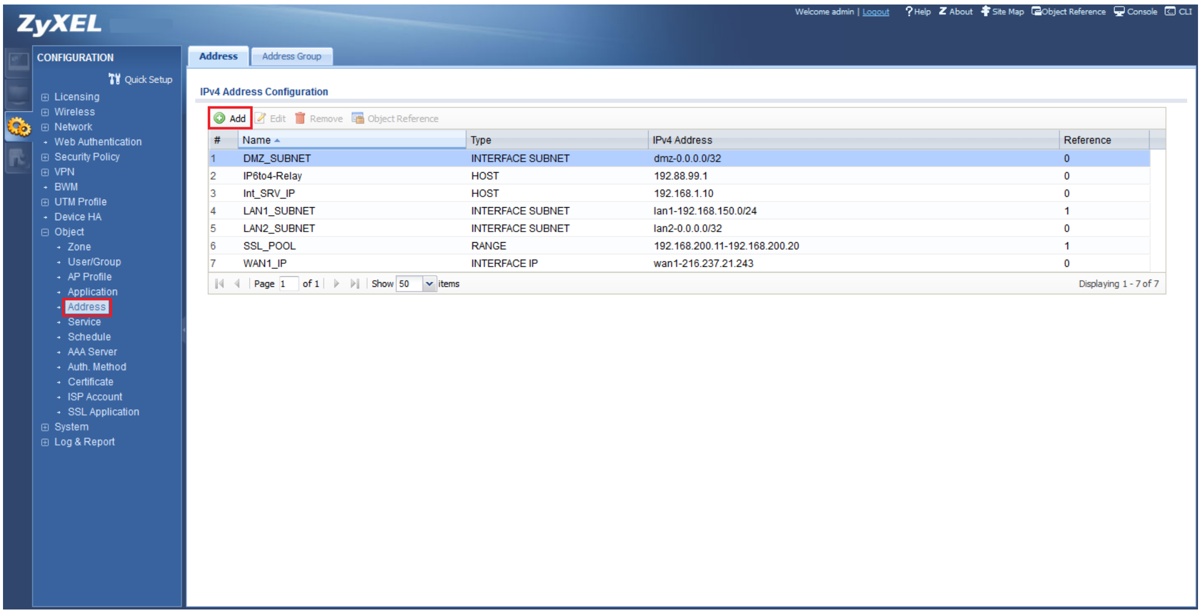
Create Address Objects

To create a Virtual Server rule, the simplest way is to start with creating address objects.

In this tutorial we will create two objects, one for the WAN1 (GE1) Interface IP-address and one for the server's internal IP-address.

To create an address object go to the Configuration menu. Select the **Object → Address** menu.

Click the **Add** button.

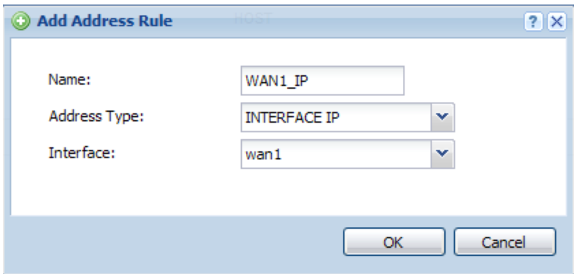


IPv4 Address Configuration

#	Name	Type	IPv4 Address	Reference
1	DMZ_SUBNET	INTERFACE SUBNET	dmz-0.0.0.0/32	0
2	IP6to4-Relay	HOST	192.88.99.1	0
3	Int_SRV_IP	HOST	192.168.1.10	0
4	LAN1_SUBNET	INTERFACE SUBNET	lan1-192.168.150.0/24	1
5	LAN2_SUBNET	INTERFACE SUBNET	lan2-0.0.0.0/32	0
6	SSL_POOL	RANGE	192.168.200.11-192.168.200.20	1
7	WAN1_IP	INTERFACE IP	wan1-216.237.21.243	0

Page 1 of 1 | Show 50 items | Displaying 1 - 7 of 7

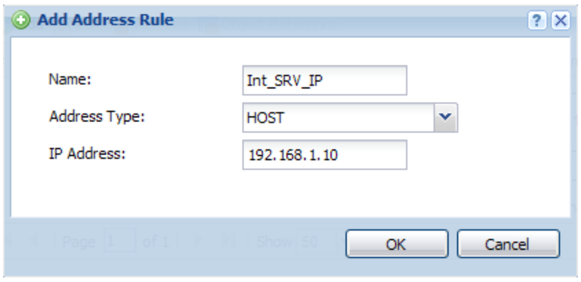
Give the object a name. Choose "Interface IP" as Address Type, as this will dynamically follow the interface IP-address, and select Interface "WAN1" (GE2).



Name:	WAN1_IP
Address Type:	INTERFACE IP
Interface:	wan1

Click the **OK** button

Use the same step for the server's address object. Here you use "Host" as Address Type.   Insert your server’s internal IP-address.



Add Address Rule

Name: Int_SRV_IP

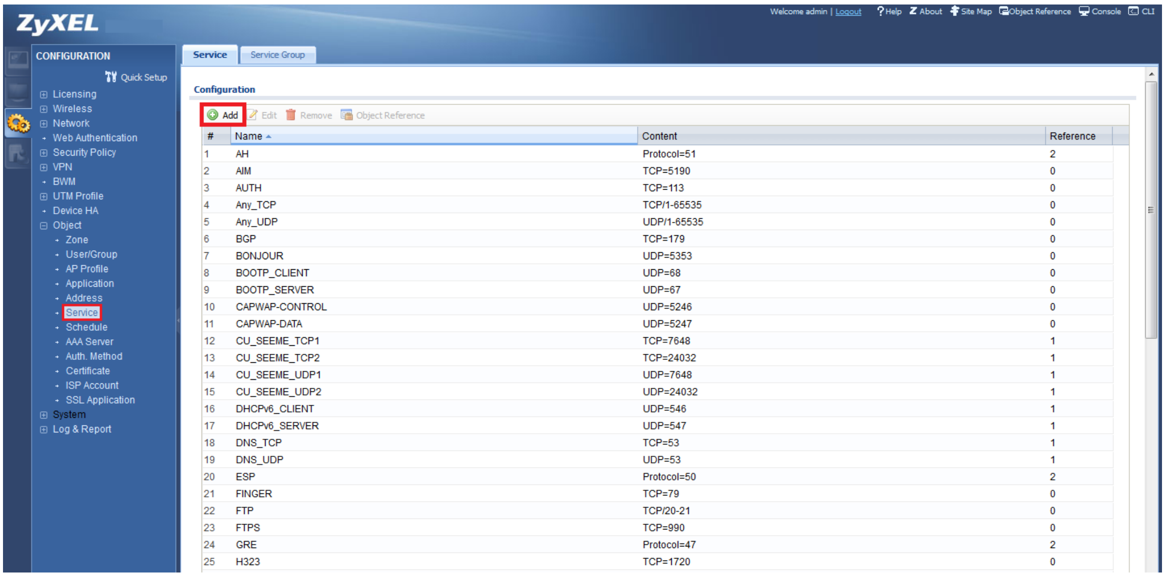
Address Type: HOST

IP Address: 192.168.1.10

Click the **OK** button

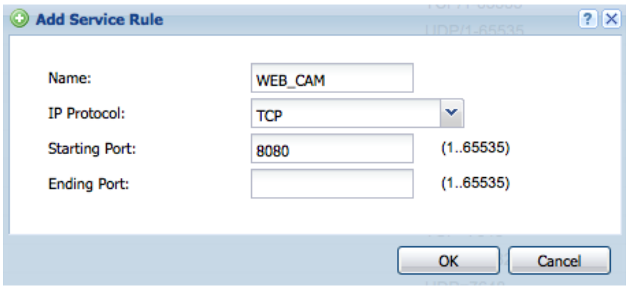
Create Service Object

To create a service object for ports that are not predefined go to **Configuration → Object → Service**. You will be presented with a list of all the service objects on the device, both user created and predefined. If there isn't a service object created for the port number(s) you need please click the **Add** button to insert a service rule.



#	Name	Content	Reference
1	AH	Protocol=51	2
2	AIM	TCP=5190	0
3	AUTH	TCP=113	0
4	Any_TCP	TCP/1-65535	0
5	Any_UDP	UDP/1-65535	0
6	BGP	TCP=179	0
7	BONJOUR	UDP=5353	0
8	BOOTP_CLIENT	UDP=68	0
9	BOOTP_SERVER	UDP=67	0
10	CAPWAP-CONTROL	UDP=5246	0
11	CAPWAP-DATA	UDP=5247	0
12	CU_SEEME_TCP1	TCP=7648	1
13	CU_SEEME_TCP2	TCP=24032	1
14	CU_SEEME_UDP1	UDP=7648	1
15	CU_SEEME_UDP2	UDP=24032	1
16	DHCPv6_CLIENT	UDP=546	1
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	0
22	FTP	TCP/20-21	0
23	FTPS	TCP=990	0
24	GRE	Protocol=47	2
25	H323	TCP=1720	0

- Give the object a name
- Specify protocol "TCP" or "UDP" (if you need both protocols you will need to add multiple service object, one using the TCP protocol and the other with UDP)
- Specify start and end ports (if you only need one port such as the example above just specify the start port and the object will be created for a single port only)

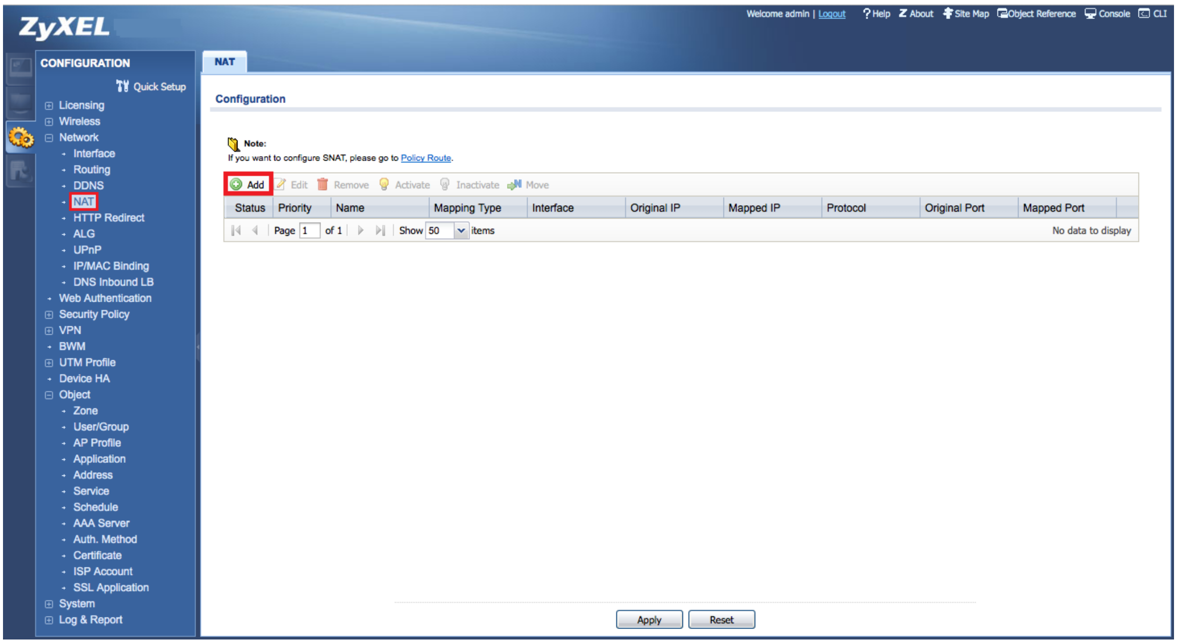


Name:	WEB_CAM	
IP Protocol:	TCP	
Starting Port:	8080	(1..65535)
Ending Port:		(1..65535)

Click the **OK** button

Create Virtual Server Rule

To create a Virtual Server rule go to, **Configuration → Network → NAT** menu.   Click the **Add** button to insert a rule.

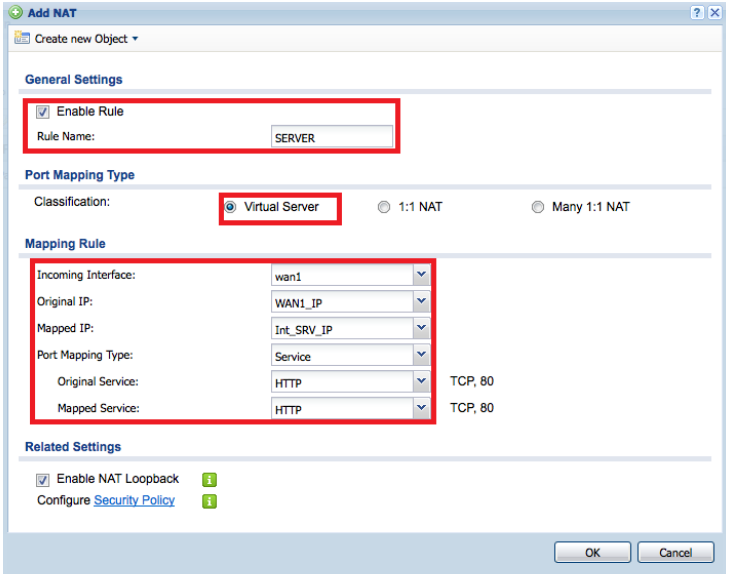


Note:
If you want to configure SNAT, please go to Policy Route.

Status	Priority	Name	Mapping Type	Interface	Original IP	Mapped IP	Protocol	Original Port	Mapped Port

No data to display

- Enable rule
- Insert a rule name
- Select Virtual Server
- Choose the incoming interface (usually WAN1 or GE1)
- Select the “WAN1_IP” object for Original IP
- select “Int_SRV_IP” for Mapped IP
- Select Service for the Port Mapping Type
- In Original and Mapped Service select the service object you created for the port(s) that need to open



General Settings

☑ Enable Rule

Rule Name: SERVER

Port Mapping Type

Classification: ● Virtual Server ○ 1:1 NAT ○ Many 1:1 NAT

Mapping Rule

Incoming Interface:	wan1	
Original IP:	WAN1_IP	
Mapped IP:	Int_SRV_IP	
Port Mapping Type:	Service	
Original Service:	HTTP	TCP, 80
Mapped Service:	HTTP	TCP, 80

Related Settings

☑ Enable NAT Loopback

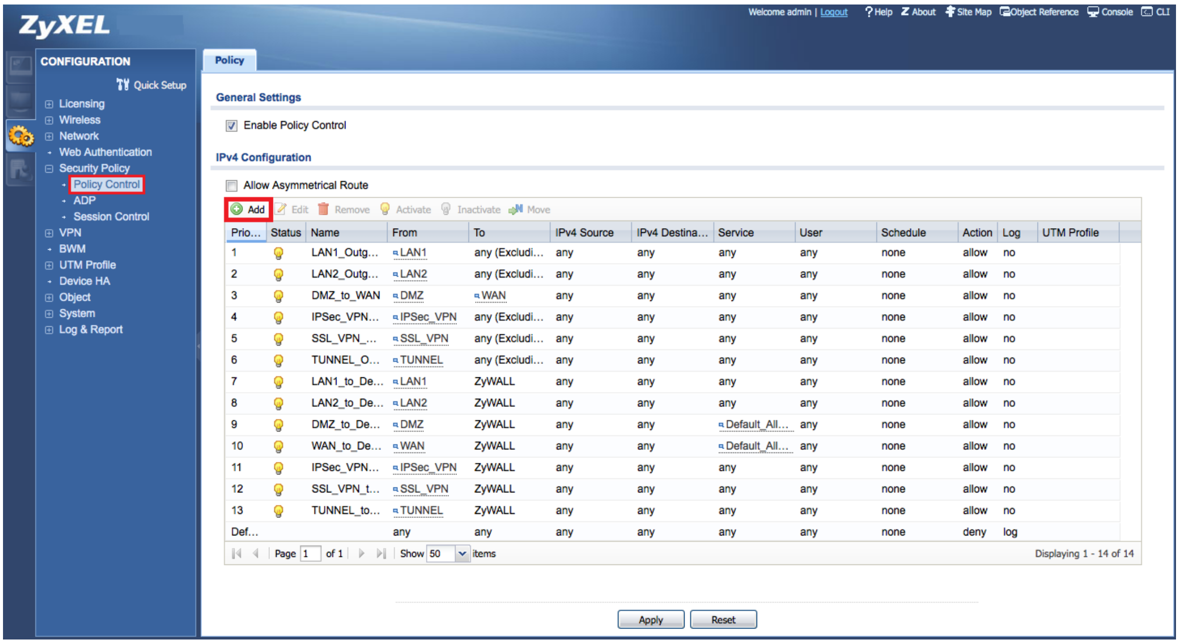
Configure Security Policy

Click the **OK** button

Note: NAT Loopback can be activated so internal clients can contact the server based on public info (WAN IP, DDNS hostname, Domain Name, etc.), only if Original IP is not set to ANY.

Create Policy Control Rule

As the final step, we need to create a Policy Control rule, to allow traffic to pass through to the server. Go to the **Configuration → Security Policy → Policy Control** menu and press the **Add** button to insert a rule.



General Settings

☑ Enable Policy Control

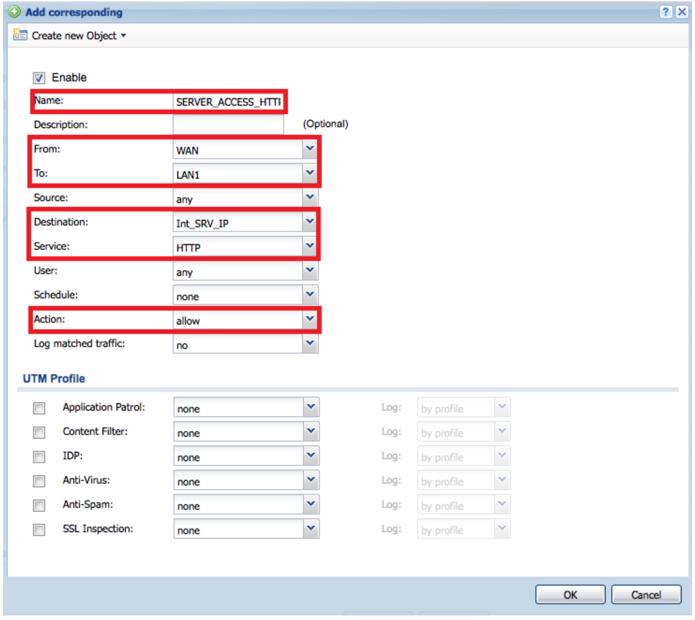
IPv4 Configuration

□ Allow Asymmetrical Route

Prio...	Status	Name	From	To	IPv4 Source	IPv4 Destina...	Service	User	Schedule	Action	Log	UTM Profile
1	●	LAN1_Outg...	LAN1	any (Excludi...	any	any	any	any	none	allow	no	
2	●	LAN2_Outg...	LAN2	any (Excludi...	any	any	any	any	none	allow	no	
3	●	DMZ_to_WAN	DMZ	WAN	any	any	any	any	none	allow	no	
4	●	IPSec_VPN...	IPSec_VPN	any (Excludi...	any	any	any	any	none	allow	no	
5	●	SSL_VPN_...	SSL_VPN	any (Excludi...	any	any	any	any	none	allow	no	
6	●	TUNNEL_O...	TUNNEL	any (Excludi...	any	any	any	any	none	allow	no	
7	●	LAN1_to_De...	LAN1	ZyWALL	any	any	any	any	none	allow	no	
8	●	LAN2_to_De...	LAN2	ZyWALL	any	any	any	any	none	allow	no	
9	●	DMZ_to_De...	DMZ	ZyWALL	any	any	Default_All...	any	none	allow	no	
10	●	WAN_to_De...	WAN	ZyWALL	any	any	Default_All...	any	none	allow	no	
11	●	IPSec_VPN...	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no	
12	●	SSL_VPN_t...	SSL_VPN	ZyWALL	any	any	any	any	none	allow	no	
13	●	TUNNEL_to...	TUNNEL	ZyWALL	any	any	any	any	none	allow	no	
Def...			any	any	any	any	any	any	none	deny	log	

Page 1 of 1 | Show 50 items | Displaying 1 - 14 of 14

- Provide a name to the Policy Control rule.
- Select FROM WAN TO LAN1.
- Insert your servers IP-address object as Destination.
- Select your preferred Service or Service Group (in this case HTTP is selected).
- Set Access as Allow.
- Enable Log if needed.



☑ Enable

Name:	SERVER_ACCESS_HTTI
Description:	(Optional)
From:	WAN
To:	LAN1
Source:	any
Destination:	Int_SRV_IP
Service:	HTTP
User:	any
Schedule:	none
Action:	allow
Log matched traffic:	no

UTM Profile

□	Application Patrol:	none	Log:	by profile
□	Content Filter:	none	Log:	by profile
□	IDP:	none	Log:	by profile
□	Anti-Virus:	none	Log:	by profile
□	Anti-Spam:	none	Log:	by profile
□	SSL Inspection:	none	Log:	by profile

Click the **OK** button