

ZyWALL USG-Series

Setup of One-to-One NAT





Table of contents

Scenario	. 3
Start with address objects	4
Create NAT rule	. 5
Create Firewall rule	. 6



Scenario

This guideline describes how to setup 1:1 NAT in ZyWALL USG-series.

ZyWALL USG has some extra IP-addresses available. With 1:1 NAT all requests to e.g. 212.130.62.52 will be directly forwarded to the selected internal client.





Start with address objects

To create a NAT One-to-One rule, the simplest way is to start with creating address objects.

In this tutorial we will create two objects, one for the secondary WAN IP-address and one for the server's internal IP-address.

To create an address object go to the Configurations menu. Select the Object -> Address menu. Click the Add button.



Give the object a name. Choose Host as Address Type, and insert the secondary WAN IP-address.

Add Address Rule	Type ? 🗙
Name:	Ext_WAN_IP
Address Type:	HOST 👻
IP Address:	212.130.62.52
	OK Cancel

Use the same step for the server's host object.

Add Address Rule	Objed Reference	? ×
Name:	Int_SRV_IP	
Address Type:	HOST	
IP Address:	192.168.1.10	
	OK Cancel	



Create NAT rule

To create the NAT rule, go to Network -> NAT menu, and click the Add button.



Enable rule. Insert a rule name. Select 1:1 NAT.

Choose the incoming interface (usually WAN1 or ge2).

Select the new Ext_WAN_IP object as Original IP, select Int_SRV_IP as Mapped IP. Set Port Mapping Type as Any.

Click the OK button.

O Add NAT				? X
🔚 Create new Object 🗸				
General Settings	SERVER			_
Port Mapping Type				
Classification:	Virtual Server	1:1 NAT	Many 1:1 NAT	
Mapping Rule				
Incoming Interface:	wan1	~		
Original IP:	Ext_WAN_IP	👻 🔶 WAN IP		
Mapped IP:	Int_SRV_IP	SERVER IP		
Port Mapping Type:	any	*		
Related Settings				
Enable NAT Loopback Configure Firewal				
			ОКСа	ncel

Note: NAT Loopback can be activated, so internal clients can contact server on its public IP-address.





Create Firewall rule

As the final step, we need to create a Firewall Rule, to allow traffic pass through to the server.

Go to the Firewall menu, and press the Add button.

	CONFIGURATION	Firew	all Ses	sion Limit									
	T∰ Quick Setup ⊕ Licensing	Gene	eral Setting	5									_
>	 Network Interface Routing 	V	Enable Firew	all symmetrical	Route								
	Zone DDNS NAT	Firev	rall Rule Su m Zone:	mmary any		~	То 2	Zone:	any		~	Refresh	כ
	HTTP Redirect ALG IP/MAC Binding	S) Add 📝 Edi Priority 🔺	t 👕 Remo	ve 🥥 Activ To	vate 🎧 Ina Schedule	octivate 🤿 User	Move Source	Destinat	Service	Access	Log	
	+ Auth. Policy + <mark>Firewall</mark>	9) 1	R WAN	ZyWALL	none	any	any	any	■Defaul	allow	no	
			3	R WAN	any (Ex	none	any	any	any	any	deny	log	
	 Anti-X ⊕ Object ⊕ Curters) 4) 5		ZyWALL ZyWALL	none	any any	any any	any any	■Defaul any	allow deny	no log	
	 ↔ System 	ę	6	■ DMZ	R WAN	none	any	any	any	any	allow	no	
			8		any (Ex	none	any any	any any	any any	any any	deny allow	log no	
		9	9	NULAN	ZyWALL	none	any	any	any	■Defaul	allow	no	
		<	, 10	4 WLAN	ZYWALL	none	any	any	any	any	deny	iog	>

Select from WAN to LAN1. Insert your server's 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.

Click the OK button.

O Add Firewall Rule		? 🗙
🔚 Create new Object 🗸		
🔽 Enable		
From:	WAN	¥
To:	LAN1	*
Description:		(Optional)
Schedule:	none	~
User:	any	~
Source:	any	~
Destination:	Int_SRV_IP	*
Service:	НТТР	~
Access:	allow	*
Log:	no	*
	ZyWALL none a	OK Cancel

