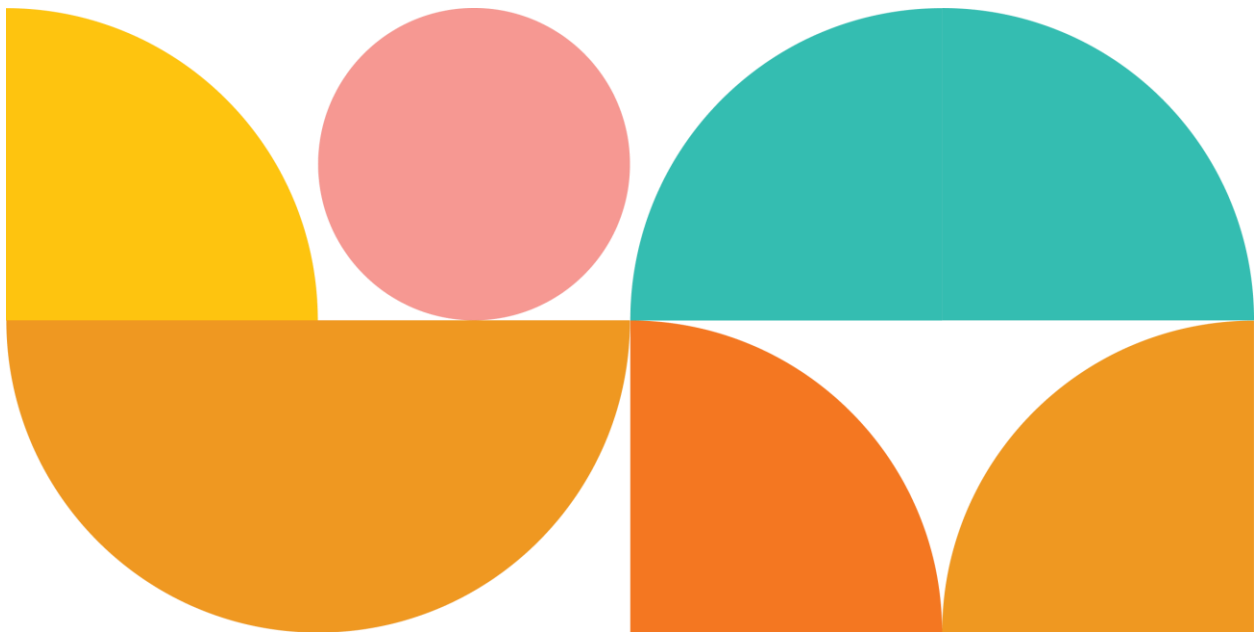


17/01/2025

FireWall

Configuration-Règles-Routages



Jocelin Rey

ByteMeUp

Sommaire

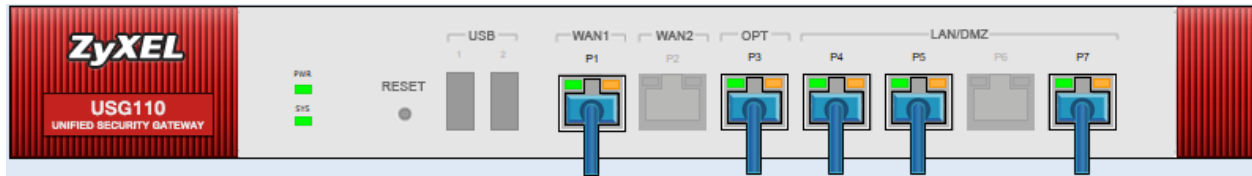
Sommaire	2
1-Configuration-Basic.....	3
2-Configuration-Ports	3
3-Configuration-Routages	4
4-Configuration-VPN.....	6
5-Regle de pare feu.....	9

1-Configuration-Basic

Ip : 192.168.30.254

Compte	User	Password
admin	admin	*****
admin	jocelin	*****

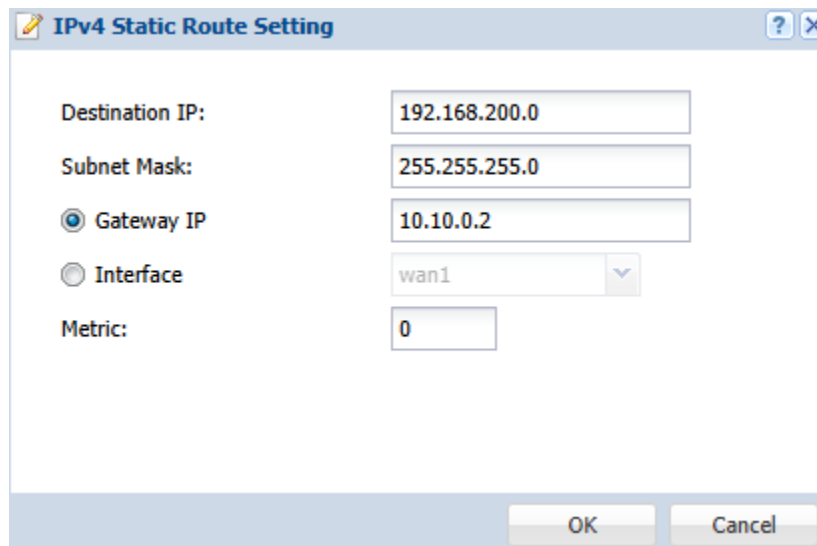
2-Configuration-Ports



Name	Port	IP	Role	Actif
Wan1	P1	172.31.254.178/16	Exterieur	UP
Wan2	P2	0.0.0.0/0.0.0.0	Exterieur	DOWN
OPT	P3	10.30.0.2/16	Liaison-CM	UP
LAN	P4	10.30.0.2	Liaison-PF	UP
LAN	P5	192.168.30.254/24	LAN-BMU	UP
LAN	P6	0.0.0.0/0.0.0.0	LAN-BMU	DOWN
DMZ	P7	192.168.40.254/24	DMZ-Replica	UP

3-Configuration-Routages

Route Static liaison PF DMZ :

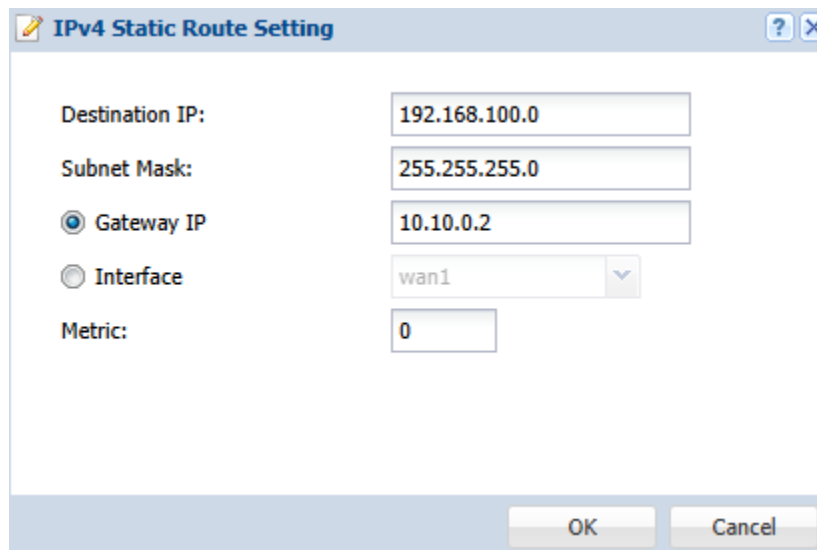


The dialog box titled "IPv4 Static Route Setting" contains the following fields and options:

Destination IP:	192.168.200.0
Subnet Mask:	255.255.255.0
☒ Gateway IP	10.10.0.2
☐ Interface	wan1
Metric:	0

Buttons: OK, Cancel

Route Static PF LAN :



The dialog box titled "IPv4 Static Route Setting" contains the following fields and options:

Destination IP:	192.168.100.0
Subnet Mask:	255.255.255.0
☒ Gateway IP	10.10.0.2
☐ Interface	wan1
Metric:	0

Buttons: OK, Cancel

Route Static LAN MC :

 **IPv4 Static Route Setting**  

Destination IP:	172.16.20.0
Subnet Mask:	255.255.255.0
☒ Gateway IP	10.30.0.1
☐ Interface	wan1 
Metric:	0

4-Configuration-VPN

Configuration VPN Gateway VPN-PF

Edit VPN Gateway VPN-PF

Show Advanced Settings Create New Object

General Settings

☒ Enable

VPN Gateway Name: VPN-PF

IKE Version

☐ IKEv1

☒ IKEv2

Gateway Settings

My Address

☒ Interface wan1 DHCP client -- 172.31.254.178/255.255.0.0

☐ Domain Name / IPv4

Peer Gateway Address

☒ Static Address **Static Address**

Primary 172.31.254.178

Secondary 0.0.0.0

☐ Fall back to Primary Peer Gateway when possible

Fall Back Check Interval: 300 (60-86400 seconds)

☐ Dynamic Address **Dynamic Address**

Authentication

☒ Pre-Shared Key

☐ unmasked

☐ Certificate default (See [My Certificates](#))

☒ Advance

Phase 1 Settings

SA Life Time: 86400 (180 - 3000000 Seconds)

☒ Advance

OK Cancel

Configuration VPN Connection :

General Settings

☐ Enable

Connection Name: VPN

Advance

VPN Gateway

Application Scenario

- ☒ Site-to-site
- ☐ Site-to-site with Dynamic Peer
- ☐ Remote Access (Server Role)
- ☐ Remote Access (Client Role)
- ☐ VPN Tunnel Interface

VPN Gateway: VPN-PF wan1 172.31.254.178, 0.0.0.0

Policy

Local Policy: LAN1_SUBNET INTERFACE SUBNET, 192.168.30.0/24

Remote Policy: reseaupfsrv SUBNET, 192.168.100.0/24

Advance

Advance

☐ Enable GRE over IPSec

☐ Policy Enforcement

Phase 2 Setting

SA Life Time: 28800 (180 - 3000000 Seconds)

Advance

Active Protocol: ESP

Encapsulation: Tunnel

Proposal

Add Edit Remove		
#	Encryption	Authentication
1	AES256	SHA512

Perfect Forward Secrecy (PFS): DH14

Related Settings

Zone: IPSec_VPN

Connectivity Check

☐ Enable Connectivity Check 

Check Method: 

Check Period: (5-600 Seconds)

Check Timeout: (1-10 Seconds)

Check Fail Tolerance: (1-10)

☐ Check This Address (Domain Name or IP Address)

☒ Check the First and Last IP Address in the Remote Policy

☒ Log

 Advance

OK

Cancel

5-Regle de pare feu

Priority	Status	Name	From	To	IPv4 Source	IPv4 Destination	Service	User	Schedule	Action	Log
1		SRV-AD-REPLICA	LAN1	any (Excluding ZyWALL)	SRV-AD-REPLICA	any	PORT-SRV-AD	any	none	allow	no
2		VM-WINDOWS	LAN1	any (Excluding ZyWALL)	any	any	VM-WINDOWS10	any	none	allow	no
3		VM-OMV	DMZ	any (Excluding ZyWALL)	SRV-OMV	any	PORT-OMV	any	none	allow	no
4		VM-APPLI	LAN1	any (Excluding ZyWALL)	SRV-APPLI	any	PORT-SRV-APPLI	any	none	allow	no
5		VM-DC	LAN1	any (Excluding ZyWALL)	SRV-DC	any	PORT-SRV-AD	any	none	allow	no
6		VM-GLPI	LAN1	any (Excluding ZyWALL)	VM-GLPI	any	PORT-GLPI	any	none	allow	no
7		LiaisonPF	LAN2	LAN1	any	any	liaisonPF	any	none	allow	no
8		LiaisonMC	OPT	LAN1	any	any	liaisonMC	any	none	allow	no
9		VM-Zabbix	LAN1	any (Excluding ZyWALL)	VM-Zabbix	any	VM-Zabbix	any	none	allow	no
10		VPN-PF	IPSec_VPN	any (Excluding ZyWALL)	any	any	any	any	none	allow	no
11		VPN-PF2	IPSec_VPN	ZyWALL	any	any	any	any	none	allow	no
12		wifi	LAN1	LAN1	Vlan-10-Wifi	any	any	any	none	allow	log
13		LAN1_Outgoing	LAN1	any (Excluding ZyWALL)	any	any	VM-WINDOWS10	any	none	allow	no
14		DMZ_to_WAN	DMZ	LAN1	SRV-OMV	any	any	any	none	allow	no
15		LAN1_to_Device	LAN1	ZyWALL	any	any	any	any	none	allow	no
16		DMZ_to_Device	DMZ	ZyWALL	any	any	Default_Allow_DMZ_To_ZyWALL	any	none	allow	no
17		WAN_to_Device	WAN	ZyWALL	any	any	Default_Allow_WAN_To_ZyWALL	any	none	allow	no
Default			any	any	any	any	any	any	none	deny	log

NAME	Service
PORT-SRV-AD	Member === Object === DNS_TCP DNS_UDP Kerberos-TCP Kerberos-UDP LDAP-TCP LDAP-UDP LDAPS-TCP LDAPS-UDP MS-RPC NTP NetBIOS_TCP1 NetBIOS_TCP2 NetBIOS_UDP1 NetBIOS_UDP2 SMB3

VM-WINDOWS-10	Member === Object === DNS_TCP DNS_UDP HTTP HTTPS Kerberos-TCP Kerberos-UDP LDAP-TCP LDAP-UDP LDAPS-TCP LDAPS-UDP MS-RPC NetBIOS_TCP1 NetBIOS_TCP2 NetBIOS_UDP1 NetBIOS_UDP2 PING RDP SSH_TCP SSH_UDP
PORT-OMV	Member === Object === HTTP HTTPS NetBIOS_TCP1 NetBIOS_TCP2 NetBIOS_UDP1 NetBIOS_UDP2 SSH_TCP SSH_UDP
PORT-SRV-APPLI	Member === Object === Anydesk Anydesk1 HTTP HTTPS RDP SSH_TCP SSH_UDP
VM-ZABBIX	Member === Object === HTTP SSH_TCP SSH_UDP systemd
PORT-GLPI	Member === Object === HTTP HTTPS LDAP-TCP LDAP-UDP

LIAISONPF	Member === Object === HTTP HTTPS PING SMB3	
LIAISONMC	Member === Object === HTTPS PING SMB3	