

# Report 2

## Switch 3 (Core switch )

```
interface ethernet0/2
no switchport
ip address 10.10.10.2 255.255.255.0
no shutdown
int vlan10
ip address 192.168.10.1/24
int vlan20
ip address 192.168.20.1/24
ip route 0.0.0.0 0.0.0.0 10.10.10.1
```

Make the interface Layer 3 (routing mode)  
Assign IP address  
Enable the interface  
Create VLAN 10 SVI (Layer 3 interface)  
Set gateway IP for VLAN 10  
Create VLAN 20 SVI  
Set gateway IP for VLAN 20  
Default route pointing to Fortigate

## Fortigate:

```
Login: admin
password:
new password: 123
```

Default login with no password

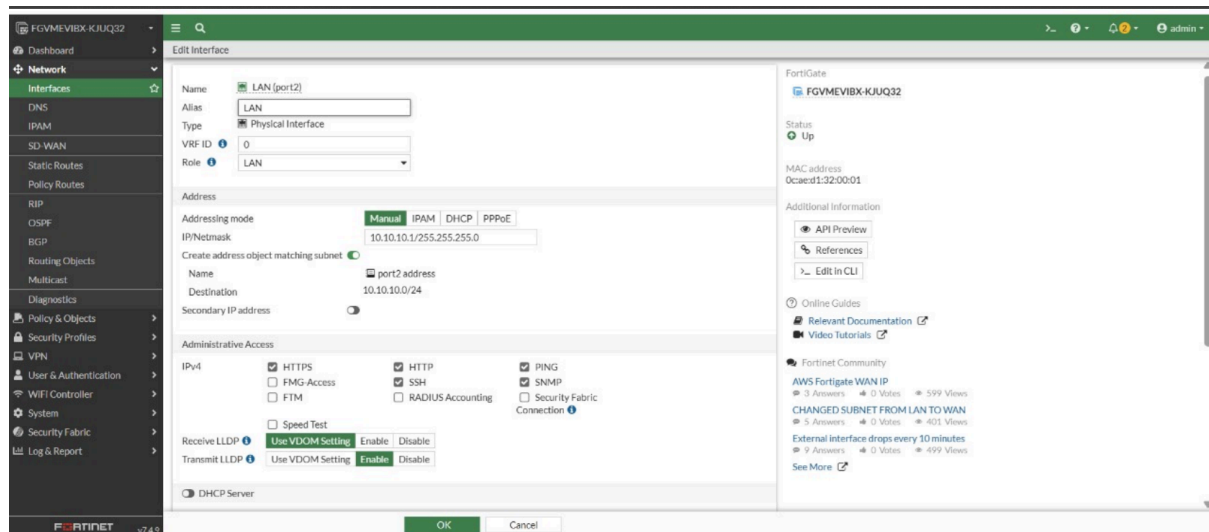
Set a new password

```
config system interface
edit port1
set mode static 192.168.126.139
set allowaccess http https ping ssh
end
config system interface
edit port2
set mode dhcp
set allowaccess http https ping ssh
end
```

Enter interface configuration mode  
Select port1  
Assign static IP to port1  
Allow management access on port1

Enter interface configuration mode again  
Select port2  
Receive IP from DHCP server  
Allow management access on port2

This interface is configured as a LAN port with some settings:



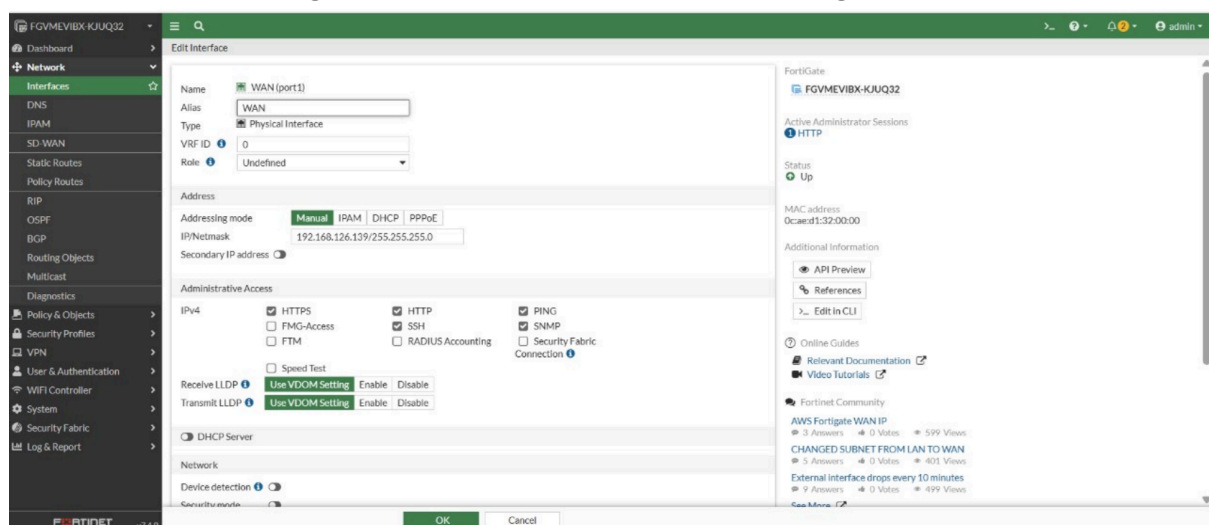
**Addressing Mode:** Manual

**IP:** 10.10.10.1/24 #Gateway for devices in this network

**Role:** LAN #interface is used for internal network traffic

**Administrative access:** include http https ssh ping which enable management and troubleshooting from inside the network

This interface is configured as a WAN port with some settings:



**Addressing Mode:** Manual

**IP:** 192.168.126.139/24 #Gateway for devices in this network

**Role:** WAN #interface is used for external network traffic(Internet)

**Administrative access:** include https ping usually limited for security

Destination	Gateway IP	Interface	Status	Comments
0.0.0.0/0	192.168.126.2	WAN (port1)	Enabled	
192.168.10.0/24	10.10.10.2	LAN (port2)	Enabled	
192.168.20.0/24	10.10.10.2	LAN (port2)	Enabled	

## The Fortigate's static routes:

### 1-default route (0.0.0.0/0)

Gateway: 192.168.126.2

interface WAN (port1)

used for sending all unknown traffic to the internet.

### 2-Route to 192.168.10.0/24

Gateway: 10.10.10.2

interface LAN (port2)

Directs traffic to the 192.168.10.x network through the internal router.

### 3-Route to 192.168.20.0/24

Gateway: 10.10.10.2

interface LAN (port2)

Sends traffic to the 192.168.20.x network through the internal router.

Firewall Addresses:

FGVMEVIBX-KJUQ32

DashboardNetworkPolicy & ObjectsFirewall PolicyDoS PolicyAddressesInternet Service DatabaseServicesSchedulesVirtual IPsIP PoolsProtocol OptionsTraffic ShapingSecurity ProfilesVPNUser & AuthenticationWiFi Controller

Address Address Group

Create newEditCloneDeleteSearch

Name	Type	Interface	Details	IP	Ref.
FABRIC_DEVICE	Subnet			0.0.0.0/0	0
FIREWALL_AUTH_PORTAL_ADDRESS	Subnet			0.0.0.0/0	0
SSLVPN_TUNNEL_ADDR1	IP Range			10.212.134.200-10.212.134.210	1
VLAN10	Subnet			192.168.10.0/24	0
VLAN20	Subnet			192.168.20.0/24	0
all	Subnet			0.0.0.0/0	6
gmail.com	FQDN		gmail.com		1
login.microsoft.com	FQDN		login.microsoft.com		1
login.microsoftonline.com	FQDN		login.microsoftonline.com		1
login.windows.net	FQDN		login.windows.net		1
none	Subnet			0.0.0.0/32	0
port2 address	Interface Subnet	LAN (port2)		10.10.10.0/24	0

Security Rating Issues0% 16

Name

vlan20

Color

Change

Interface

LAN (port2)

Type

Subnet

IP/Netmask

192.168.20.0 255.255.255.0

Static route configuration

Comments

Write a comment...0/255

Name

vlan10

Color

Change

Interface

LAN (port2)

Type

Subnet

IP/Netmask

192.168.10.0 255.255.255.0

Static route configuration

Comments

Write a comment...0/255

The Firewall Policies:

FGVMEVIBX-KJUQ32

DashboardNetworkPolicy & ObjectsFirewall PolicyDoS PolicyAddressesInternet Service DatabaseServicesSchedulesVirtual IPsIP PoolsProtocol OptionsTraffic ShapingSecurity ProfilesVPNUser & AuthenticationWiFi ControllerSystemSecurity FabricLog & Report

Create newPolicy matchSearchExportInterface Pair ViewNew layout

Policy	Source	Destination	Schedule	Service	Action	IP Pool	NAT	Type	Security Profiles	Log	By
LAN (port2) → WAN (port1)	all	all	always	ALL	ACCEPT		NAT	Standard	no-inspection	UTM	2.52
LAN to WAN (1)	all	all	always	PING HTTP	ACCEPT		NAT	Standard	certificate-inspection default	UTM	0 B
VLAN10 (2)	vlan10	all	always	PING HTTP SSH	ACCEPT		NAT	Standard	certificate-inspection default	UTM	0 B
VLAN20 (3)	vlan20	all	always	PING HTTP SSH	ACCEPT		NAT	Standard	certificate-inspection default	UTM	0 B

Implicit

the firewall policies for LAN and VLANs, with allowed services, NAT enabled, and security profiles applied. The rules are organized to manage and secure traffic between the network and the WAN.

## VLAN 10 Policy

admin

Edit Policy

Name

VLAN10

Incoming interface

LAN (port2)

Outgoing interface

WAN (port1)

Source

vlan10

+

×

Destination

all

+

×

Schedule

always

Service

PING

×

HTTP

×

SSH

×

DNS

×

+

Action

✓ ACCEPT

✗ DENY

Firewall/Network Options

NAT

ON

IP pool configuration

Use Outgoing Interface Address

Use Dynamic IP Pool

Manage source port

ON

Fixed port

Preserve source port

Protocol options

PROT

default

Security Profiles

AntiVirus

ON

AV

default

Web filter

ON

WEB

default

DNS filter

OFF

Application control

ON

APP

default

IPS

ON

IPS

default

File filter

OFF

SSL inspection

SSL

certificate-inspection

Logging Options

Statistics (since last reset)

ID	2
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B

Current bandwidth 0 bps

Clear Counters

Additional Information

API Preview

Edit in CLI

Online Guides

Relevant Documentation

Video Tutorials

Consolidated Policy Configuration

Fortinet Community

Join the Discussion

OK

Cancel

## VLAN20 Policy

The screenshot shows the 'Edit Policy' configuration page for a policy named 'VLAN20'. The left sidebar contains a navigation menu with options like Dashboard, Network, Policy & Objects, Firewall Policy, DoS Policy, Addresses, Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Protocol Options, Traffic Shaping, Security Profiles, VPN, User & Authentication, WiFi Controller, System, Security Fabric, and Log & Report. The main configuration area is divided into several sections:

- Name:** VLAN20
- Incoming interface:** LAN (port2)
- Outgoing interface:** WAN (port1)
- Source:** 4 vlan20
- Destination:** 4 all
- Schedule:** always
- Service:** PING, HTTP, SSH
- Action:** ACCEPT (checked), DENY
- Firewall/Network Options:**
  - NAT: ☒
  - IP pool configuration: Use Outgoing Interface Address, Use Dynamic IP Pool
  - Manage source port: ☒ Fixed port, ☐ Preserve source port

On the right side, there is a 'Statistics (since last reset)' table and a 'Clear Counters' button.

Statistics (since last reset)	
ID	3
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B

Below the statistics, there is a 'Current bandwidth 0 bps' section with a 'Clear Counters' button. The 'Additional Information' section includes links for 'API Preview', 'Edit in CLI', 'Online Guides', 'Relevant Documentation', 'Video Tutorials', 'Consolidated Policy Configuration', and 'Fortinet Community'.

This screenshot shows the 'Edit Policy' configuration page for the same policy, but with the 'Security Profiles' section expanded. The 'Logging Options' section is also visible.

- Security Profiles:**
  - AntiVirus: ☒ AV default
  - Web filter: ☒ WEB default
  - DNS filter: ☐
  - Application control: ☒ APP default
  - IPS: ☒ IPS default
  - File filter: ☐
  - SSL inspection: ☒ SS certificate-inspection
- Logging Options:**
  - Log allowed traffic: ☒ Security events, ☐ All sessions
  - Generate logs when session starts: ☐
  - Capture packets: ☐
  - Comments: 0/1023
  - Enable this policy: ☒

The right side of the page remains the same, showing the statistics table and additional information links.

# LAN-to-WAN policy

Dashboard

Network

Policy & Objects

Firewall Policy

DoS Policy

Addresses

Internet Service Database

Services

Schedules

Virtual IPs

IP Pools

Protocol Options

Traffic Shaping

Security Profiles

VPN

User & Authentication

WiFi Controller

System

Security Fabric

Log & Report

Create new

Policy match

Policy

Source

LAN (port2) → WAN (port1)

LAN-to-WAN (1) all

VLAN10 (2) vlan10

VLAN20 (3) vlan20

Implicit

LAN-to-WAN

Incoming interface LAN (port2)

Outgoing interface WAN (port1)

Source all

Destination all

Schedule always

Service ALL

ACCEPT DENY

Firewall/Network Options

NAT

IP pool configuration Use Outgoing Interface Address Use Dynamic IP Pool

Manage source port Fixed port Preserve source port

Protocol options PROXY default

Security Profiles

AntiVirus

Web filter

DNS filter

Statistics (since last reset)

ID	1
Last used	23m 39s ago
First used	1h 17m 54s ago
Active sessions	0
Hit count	10
Total bytes	1.68 kB

Current bandwidth 0 bps

Clear Counters

Last 7 Days Bytes IPv4

1.5 kB

1 kB

500 B

0 B

Nov 23 Nov 24 Nov 25 Nov 26 Nov 27 Nov 28 Nov 29 Nov 30

nTurbo SPU Software

Additional Information

API Preview

Edit in CLI

OK

Cancel