

# Report 2

## Switch 3 (Core switch )

interface ethernet0/2	
no switchport	Make the interface Layer 3 (routing mode)
ip address 10.10.10.2 255.255.255.0	Assign IP address
no shutdown	Enable the interface
int vlan10	Create VLAN 10 SVI (Layer 3 interface)
ip address 192.168.10.1/24	Set gateway IP for VLAN 10
int vlan20	Create VLAN 20 SVI
ip address 192.168.20.1/24	Set gateway IP for VLAN 20
ip route 0.0.0.0 0.0.0.0 10.10.10.1	Default route pointing to Fortigate

## Fortigate:

Login: admin	Default login with no password
password:	
new password: 123	Set a new password

config system interface	Enter interface configuration mode
edit port1	Select port1
set mode static 192.168.126.139	Assign static IP to port1
set allowaccess http https ping ssh	Allow management access on port1
end	
config system interface	Enter interface configuration mode again
edit port2	Select port2
set mode dhcp	Receive IP from DHCP server
set allowaccess http https ping ssh	Allow management access on port2
end	

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

Name: LAN (port2)  
Alias: LAN  
Type: Physical Interface  
VRF ID: 0  
Role: LAN

Address:  
Addressing mode: Manual  
IP/Netmask: 10.10.10.1/255.255.255.0  
Create address object matching subnet: port2 address  
Name: port2 address  
Destination: 10.10.10.0/24  
Secondary IP address:

Administrative Access:  
IPv4:  HTTPS,  HTTP,  PING,  SSH,  SNMP,  Security Fabric Connection  
 Speed Test  
Receive LLDP:  Use VDOM Setting,  Enable,  Disable  
Transmit LLDP:  Use VDOM Setting,  Enable,  Disable  
 DHCP Server

OK Cancel

FortiGate  
FGVMEVIBX-KJUQ32  
Status: Up  
MAC address: 0caed1:32:00:01  
Additional Information: API Preview, References, Edit In CLI  
Online Guides: Relevant Documentation, Video Tutorials  
Fortinet Community: AWS Fortigate WAN IP, CHANGED SUBNET FROM LAN TO WAN, External Interface drops every 10 minutes, See More

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:

Name: WAN (port1)  
Alias: WAN  
Type: Physical Interface  
VRF ID: 0  
Role: Undefined

Address:  
Addressing mode: Manual  
IP/Netmask: 192.168.126.139/255.255.255.0  
Secondary IP address:

Administrative Access:  
IPv4:  HTTPS,  HTTP,  PING,  SSH,  SNMP,  Security Fabric Connection  
 Speed Test  
Receive LLDP:  Use VDOM Setting,  Enable,  Disable  
Transmit LLDP:  Use VDOM Setting,  Enable,  Disable  
 DHCP Server

Network:  
Device detection:   
Security mode:

OK Cancel

FortiGate  
FGVMEVIBX-KJUQ32  
Active Administrator Sessions: HTTP  
Status: Up  
MAC address: 0caed1:32:00:00  
Additional Information: API Preview, References, Edit In CLI  
Online Guides: Relevant Documentation, Video Tutorials  
Fortinet Community: AWS Fortigate WAN IP, CHANGED SUBNET FROM LAN TO WAN, External Interface drops every 10 minutes, See More

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

The Fortigate's static routes:

Destination	Gateway IP	Interface	Status	Comments
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	

### 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.

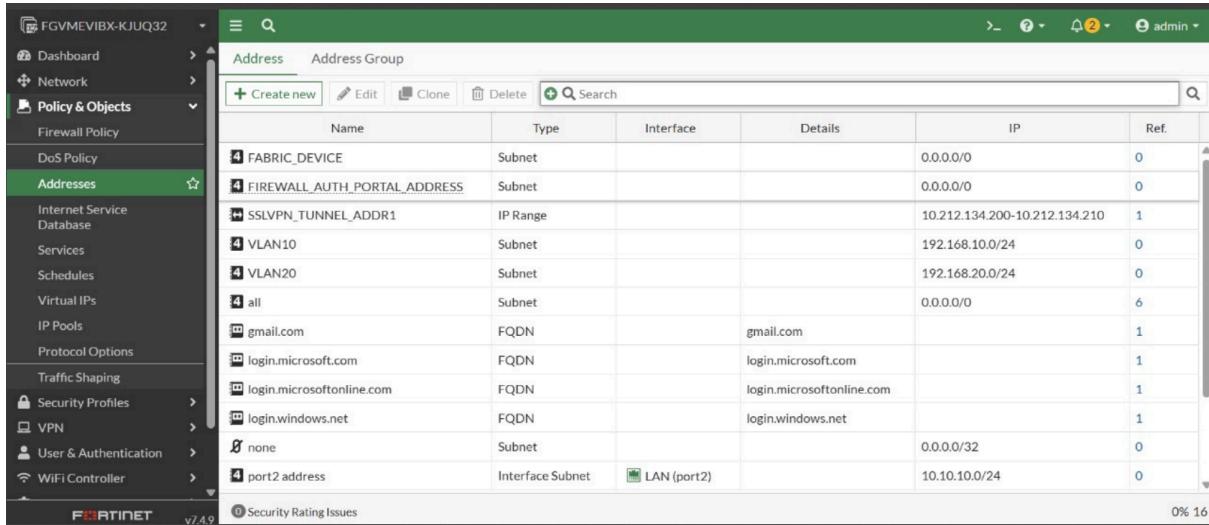
### 3-Route to 192.168.20.0/24

Gateway: 10.10.10.2

interface LAN (port2)

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

## Firewall Addresses:



The screenshot shows the FortiManager interface under the 'Policy & Objects' section, specifically the 'Addresses' tab. The table lists various network addresses and subnets:

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

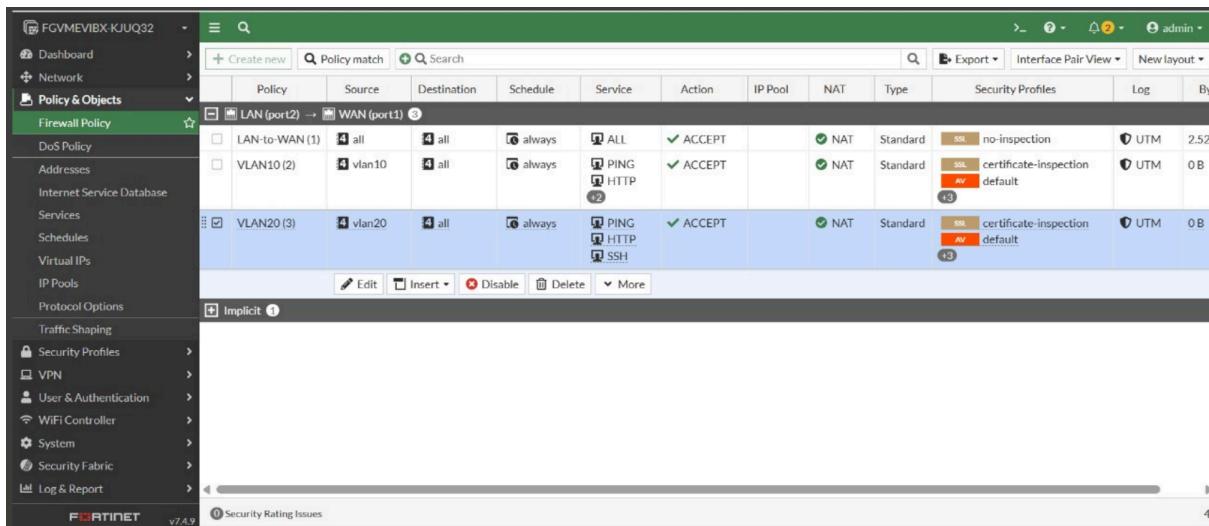
**vlan20**

Name	vlan20
Color	<input type="button" value="Change"/>
Interface	LAN (port2)
Type	Subnet
IP/Netmask	192.168.20.0 255.255.255.0
Static route configuration	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

**vlan10**

Name	vlan10
Color	<input type="button" value="Change"/>
Interface	LAN (port2)
Type	Subnet
IP/Netmask	192.168.10.0 255.255.255.0
Static route configuration	<input checked="" type="checkbox"/>
Comments	Write a comment... 0/255

## The Firewall Policies:



The screenshot shows the FortiManager interface under the 'Policy & Objects' section, specifically the 'Firewall Policy' tab. The table lists firewall policies for LAN-to-WAN and VLAN-to-WAN connections:

Policy	Source	Destination	Schedule	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	
VLAN10 (2)	vlan10	all	always	PING HTTP SSH ACCEPT		NAT	Standard	certificate-inspection AV default	0 B	
VLAN20 (3)	vlan20	all	always	PING HTTP SSH ACCEPT		NAT	Standard	certificate-inspection AV default	0 B	

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

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

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

Firewall/Network Options

NAT: Use Outgoing Interface Address, Use Dynamic IP Pool

IP pool configuration: Fixed port, Preserve source port

Protocol options: PROT default

Security Profiles

AntiVirus: default

Web filter: WEB default

DNS filter: off

Application control: APP default

IPS: IPS default

File filter: off

SSL inspection: SSL certificate-inspection

Logging Options

OK Cancel

## VLAN20 Policy

**Edit Policy**

**Name:** VLAN20

**Incoming interface:** LAN (port2)

**Outgoing interface:** WAN (port1)

**Source:** vlan20

**Destination:** all

**Schedule:** always

**Service:** PING, HTTP, SSH

**Action:** ✓ ACCEPT

**Firewall/Network Options**

- NAT: Off
- IP pool configuration: Use Outgoing Interface Address
- Manage source port: Fixed port

**Statistics (since last reset):**

ID	3
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B

**Additional Information:**

- API Preview
- Edit in CLI
- Online Guides
- Relevant Documentation
- Video Tutorials
- Consolidated Policy Configuration

Fortinet Community

OK Cancel

**Edit Policy**

**Security Profiles**

- AntiVirus: AV default
- Web filter: wfa default
- DNS filter: Off
- Application control: APP default
- IPS: IPS default
- File filter: Off
- SSL inspection: SSL certificate-inspection

**Logging Options**

- Log allowed traffic: Security events
- Generate logs when session starts: Off
- Capture packets: Off

**Comments:** 0/1023

**Enable this policy:** On

**Statistics (since last reset):**

ID	3
Last used	N/A
First used	N/A
Active sessions	0
Hit count	0
Total bytes	0 B

**Additional Information:**

- API Preview
- Edit in CLI
- Online Guides
- Relevant Documentation
- Video Tutorials
- Consolidated Policy Configuration

Fortinet Community

OK Cancel

## LAN-to-WAN policy

The screenshot shows the Fortinet FortiGate Firewall Policy configuration interface. The left sidebar navigation includes: Dashboard, Network, Policy & Objects (selected), 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 panel displays the 'Edit Policy' dialog for a policy named 'LAN-to-WAN'. The policy details are as follows:

- Name:** LAN-to-WAN
- Incoming interface:** LAN (port2)
- Outgoing interface:** WAN (port1)
- Source:** all
- Destination:** all
- Schedule:** always
- Service:** ALL
- Action:** ✓ ACCEPT (selected)

**Firewall/Network Options:**

- NAT: Enabled
- IP pool configuration: Use Outgoing Interface Address (selected)
- Manage source port: Fixed port (selected)
- Protocol options: PROT default

**Security Profiles:**

- AntiVirus: Enabled
- Web filter: Enabled
- DNS filter: Enabled

**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 (selected) - IPv4

Graph showing traffic over the last 7 days:

Date	Bytes (IPv4)			
Nov 23	1.5 kB			
Nov 24	1 kB			
Nov 25	500 B			
Nov 26	0 B			
Nov 27	Nov 28	Nov 29	Nov 30	1.5 kB

Legend: nTurbo (green), SPU (orange), Software (purple)

**Additional Information:**

- API Preview
- Edit in CLI

Buttons: OK, Cancel