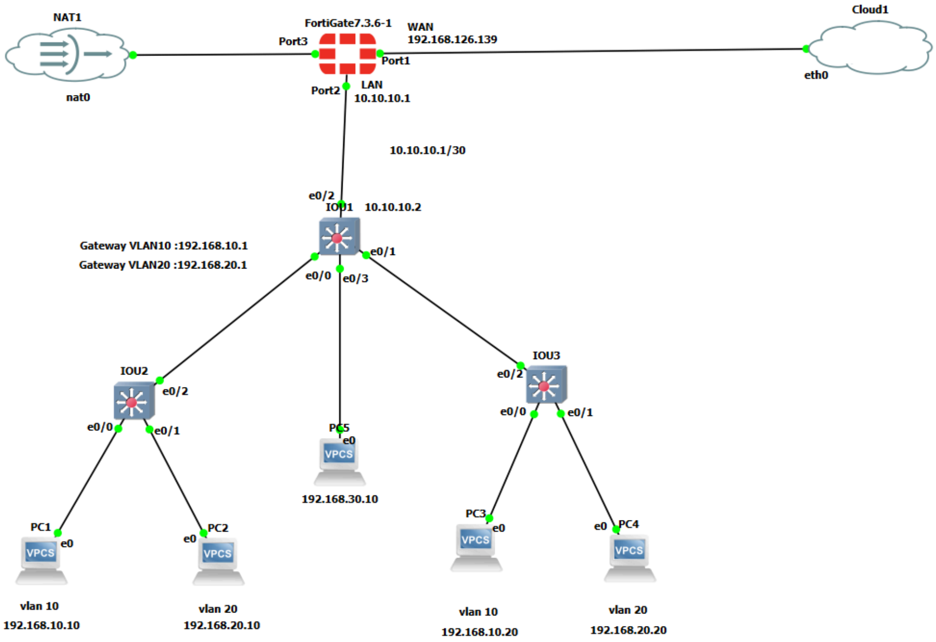
Report 4


NAT1
nat0
FortiGate7.3.6-1
Port3
WAN
192.168.126.139
Port1
Cloud1
eth0
Port2
LAN
10.10.10.1
10.10.10.1/30
e0/2
IOU1
10.10.10.2
Gateway VLAN10 :192.168.10.1
Gateway VLAN20 :192.168.20.1
e0/1
e0/0
e0/3
IOU2
e0/2
e0/0
e0/1
PC5
e0
VPCS
192.168.30.10
IOU3
e0/2
e0/0
e0/1
PC1
e0
VPCS
vlan 10
192.168.10.10
e0
PC2
VPCS
vlan 20
192.168.20.10
PC3
e0
VPCS
vlan 10
192.168.10.20
e0
PC4
VPCS
vlan 20
192.168.20.20

1. Access Switch Configuration (Switch1/IOU1 and Switch2/IOU2)

The two access layer switches (Switch1 and Switch2) were configured identically to support the two internal VLANs (HR and IT) and to establish a trunk link to the Core Switch.

- **VLAN Creation and Naming:**
  - VLAN 10 was created and named **HR**.
  - VLAN 20 was created and named **IT**.
- **Access Port Configuration:**
  - Interface Ethernet0/0 was set as an access port and assigned to **VLAN 10**.
  - Interface Ethernet0/1 was set as an access port and assigned to **VLAN 20**.
- **Trunk Port Configuration (Uplink to Core):**
  - Interface Ethernet0/2 was configured for **802.1Q** trunk encapsulation.
  - The port was set to **trunk mode**.
  - Allowed VLANs on the trunk were restricted to **1, 10, and 20**.

---

2. Core Switch Configuration (Switch3/IOU3)

The core switch serves as a Layer 3 device (Router-on-a-Stick) for Inter-VLAN routing and the uplink to the FortiGate firewall.

- **VLANs and Trunk Ports:**
  - VLAN 10 and VLAN 20 were created .
  - Uplink interfaces E0/0 and E0/1 were configured as **802.1Q trunk ports** allowing VLANs **1, 10, and 20**
- **Layer 3 and SVI Configuration:**
  - Interface Ethernet0/2 was converted to a **Layer 3 routed port** (no switchport).
  - E0/2 was assigned the IP address **10.10.10.2/30**.
  - SVI (Switched Virtual Interface) **VLAN 10** was created and configured with the gateway IP address **192.168.10.1/24**.
  - SVI **VLAN 20** was created and configured with the gateway IP address **192.168.20.1/24**
- **Routing:**
  - A **default static route** was configured to point all unknown traffic to the FortiGate firewall at **10.10.10.1**.

---

3. FortiGate Firewall Configuration

The FortiGate was configured with WAN and LAN interfaces, static routes, and firewall policies.

- **Interface Configuration (CLI and GUI):**
  - **WAN Interface (port1):** Configured with static IP **192.168.126.139** and set to **Role: WAN** Administrative access allowed: HTTPS and PING
  - **LAN Interface (port2):** Configured with static IP **10.10.10.1** and set to **Role: LAN**. Administrative access allowed: HTTP, HTTPS, PING, and SSH.

- **Static Routes:**
  - A **default route (0.0.0.0/0)** was set to use Gateway **192.168.126.2** via the WAN (port1) interface
  - A route for the **192.168.10.0/24** network was set to use Gateway **10.10.10.2** via the LAN (port2) interface
  - A route for the **192.168.20.0/24** network was set to use Gateway **10.10.10.2** via the LAN (port2) interface.

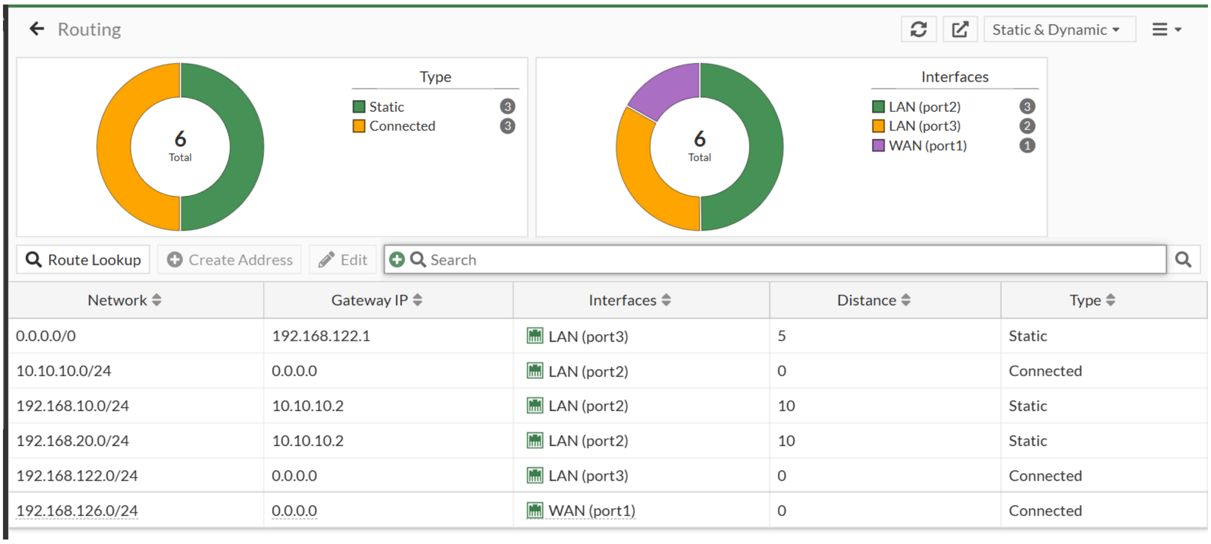
- **Firewall Policies:**
  - **VLAN10 Policy (LAN to WAN):** Allows traffic from the VLAN10 subnet to the WAN interface (port1). **Action: ACCEPT**, with **NAT** enabled Allowed services include PING, HTTP, SSH, and DNS
  - **VLAN20 Policy (LAN to WAN):** Allows traffic from the VLAN20 subnet to the WAN interface (port1) **Action: ACCEPT**, with **NAT** enabled . Allowed services include PING, HTTP, and SSH
  - A general **LAN-to-WAN** policy was also configured to accept **ALL** services from the LAN interface to the WAN interface with NAT enabled.

---

4. Verification and Testing

Connectivity testing was performed from the PCs and the FortiGate firewall.

- **PC Connectivity:**
  - **Internal Gateway Ping:** PC1, PC2, PC3, and PC4 successfully pinged their respective VLAN gateways (e.g., PC1192.168.10.1).
  - **WAN Ping:** PC1, PC2, PC3, and PC4 successfully pinged the FortiGate WAN IP (192.168.126.139), confirming inter-VLAN routing and outbound NAT.
- **Firewall Connectivity:**
  - The FortiGate successfully pinged an external IP (8.8.8.8) with **0% packet loss**, confirming internet access through port1.
  - The FortiGate successfully pinged an internal device (192.168.10.10) with **0% packet loss**, confirming connectivity to the internal network through port2.
- **Security Testing (Out of Scope):**
  - A PC (PC5) attempting to ping the FortiGate LAN interface (10.10.10.1) and an external IP (8.8.8.8) resulted in a **100% packet loss/timeout**, confirming the device was correctly isolated or unconfigured.

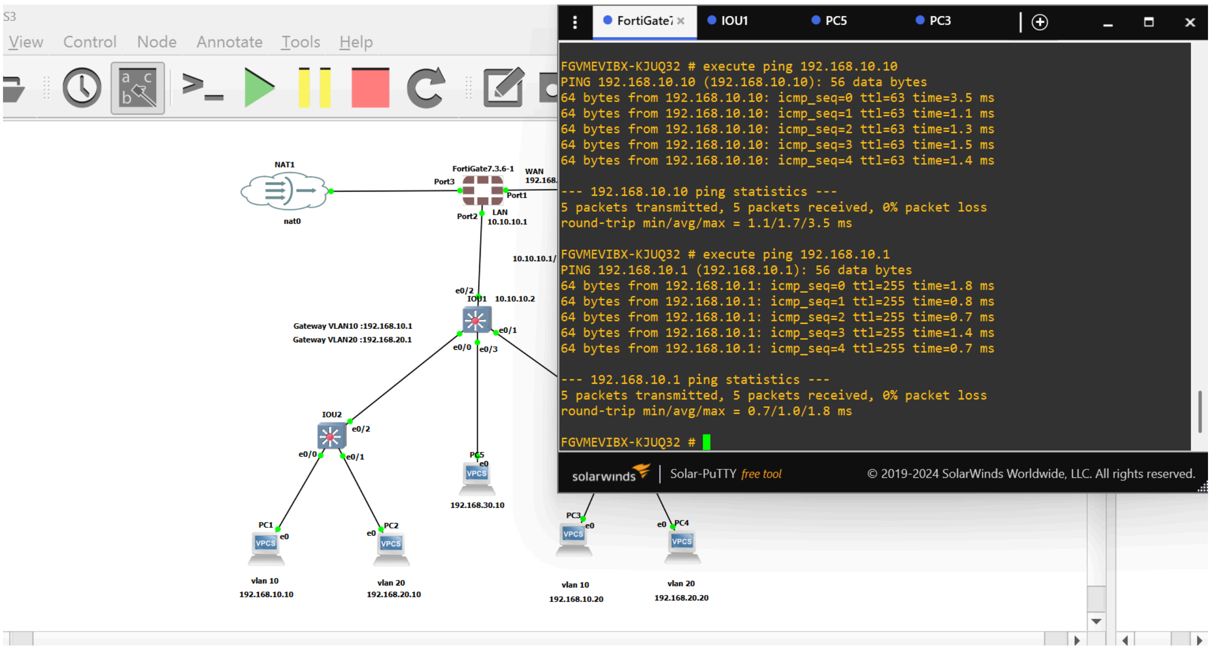


Network	Gateway IP	Interfaces	Distance	Type
0.0.0.0/0	192.168.122.1	LAN (port3)	5	Static
10.10.10.0/24	0.0.0.0	LAN (port2)	0	Connected
192.168.10.0/24	10.10.10.2	LAN (port2)	10	Static
192.168.20.0/24	10.10.10.2	LAN (port2)	10	Static
192.168.122.0/24	0.0.0.0	LAN (port3)	0	Connected
192.168.126.0/24	0.0.0.0	WAN (port1)	0	Connected

(Static Internal Routes): تم إعداد طريقين (Static Routes) لإعادة توجيه البيانات الموجهة لشبكات **VLAN** **الداخلية (192.168.10.0/24** و **192.168.20.0/24)** إلى جهاز التوجيه الداخلي (Core Switch) على العنوان **10.10.10.2**، وذلك خلال LAN port2. يضمن هذا الإعداد أن firewall يمتلك المسار الصحيح للوصول إلى الأجهزة النهائية داخل الشبكة المحلية.

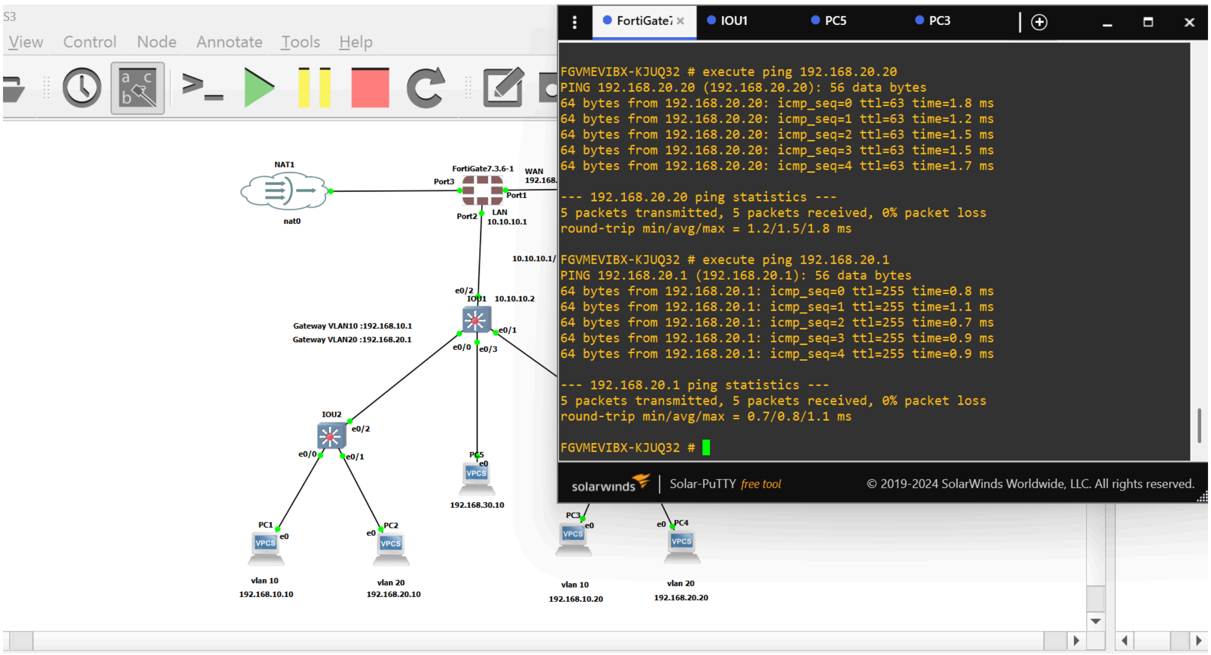
(Default Gateway): تم تحديد default gateway واحد **(0.0.0.0/0)** لتوجيه كل packets التي لا تنتمي إلى الشبكات المذكورة في الجدول (حركة الإنترنت) إلى **192.168.122.1NAT** عبر LAN port3

Ping to VLAN 10



```
FGVMEVIBX-KJUQ32 # execute ping 192.168.10.10
PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: icmp_seq=0 ttl=63 time=3.5 ms
64 bytes from 192.168.10.10: icmp_seq=1 ttl=63 time=1.1 ms
64 bytes from 192.168.10.10: icmp_seq=2 ttl=63 time=1.3 ms
64 bytes from 192.168.10.10: icmp_seq=3 ttl=63 time=1.5 ms
64 bytes from 192.168.10.10: icmp_seq=4 ttl=63 time=1.4 ms

--- 192.168.10.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.1/1.7/3.5 ms

FGVMEVIBX-KJUQ32 # execute ping 192.168.10.1
PING 192.168.10.1 (192.168.10.1): 56 data bytes
64 bytes from 192.168.10.1: icmp_seq=0 ttl=255 time=1.8 ms
64 bytes from 192.168.10.1: icmp_seq=1 ttl=255 time=0.8 ms
64 bytes from 192.168.10.1: icmp_seq=2 ttl=255 time=0.7 ms
64 bytes from 192.168.10.1: icmp_seq=3 ttl=255 time=1.4 ms
64 bytes from 192.168.10.1: icmp_seq=4 ttl=255 time=0.7 ms

--- 192.168.10.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.0/1.8 ms

FGVMEVIBX-KJUQ32 #
```

ping to VLAN 20



```
FGVMEVIBX-KJUQ32 # execute ping 192.168.20.20
PING 192.168.20.20 (192.168.20.20): 56 data bytes
64 bytes from 192.168.20.20: icmp_seq=0 ttl=63 time=1.8 ms
64 bytes from 192.168.20.20: icmp_seq=1 ttl=63 time=1.2 ms
64 bytes from 192.168.20.20: icmp_seq=2 ttl=63 time=1.5 ms
64 bytes from 192.168.20.20: icmp_seq=3 ttl=63 time=1.5 ms
64 bytes from 192.168.20.20: icmp_seq=4 ttl=63 time=1.7 ms

--- 192.168.20.20 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 1.2/1.5/1.8 ms

FGVMEVIBX-KJUQ32 # execute ping 192.168.20.1
PING 192.168.20.1 (192.168.20.1): 56 data bytes
64 bytes from 192.168.20.1: icmp_seq=0 ttl=255 time=0.8 ms
64 bytes from 192.168.20.1: icmp_seq=1 ttl=255 time=1.1 ms
64 bytes from 192.168.20.1: icmp_seq=2 ttl=255 time=0.7 ms
64 bytes from 192.168.20.1: icmp_seq=3 ttl=255 time=0.9 ms
64 bytes from 192.168.20.1: icmp_seq=4 ttl=255 time=0.9 ms

--- 192.168.20.1 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.7/0.8/1.1 ms

FGVMEVIBX-KJUQ32 #
```