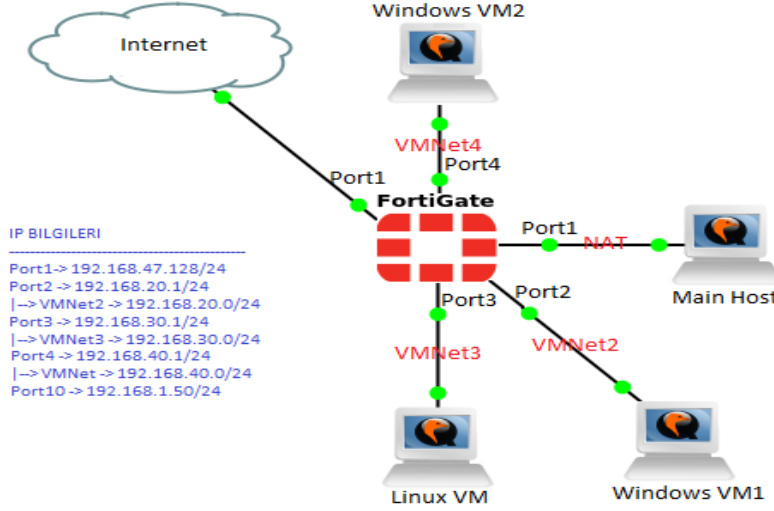


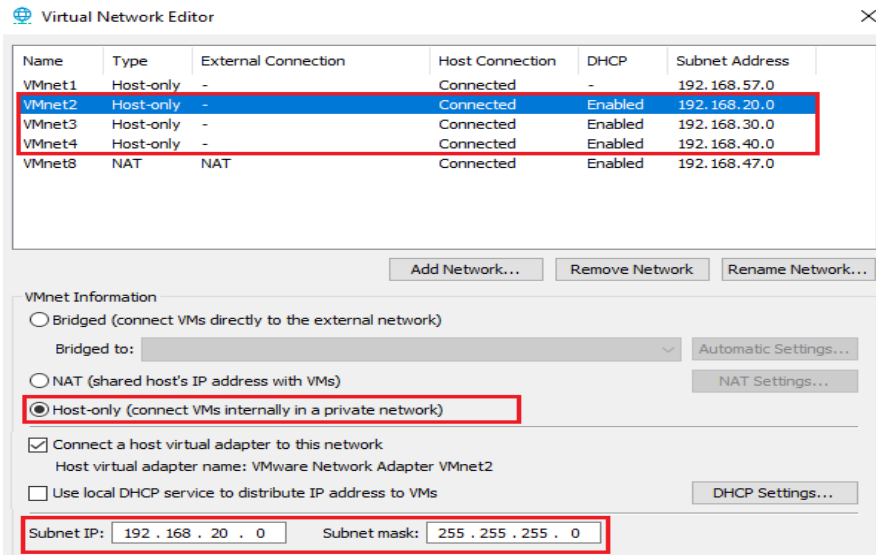
## LABARATUVAR ORTAMININ KURULUMU

Bu yazıda Fortigate güvenlik duvarı üzerinde uygulamalar yapabileceğimiz labaratuvar ortamının kurulumu yapılacaktır. Labaratuvar ortamı aşağıdaki görselden de anlaşılacağı üzere Firewall gateway arkasında 1 adet Linux istemci 2 adet de Windows istemci kurulacaktır. İstemciler Fortigate Firewall üzerinden internete çıkmaları sağlanacaktır.

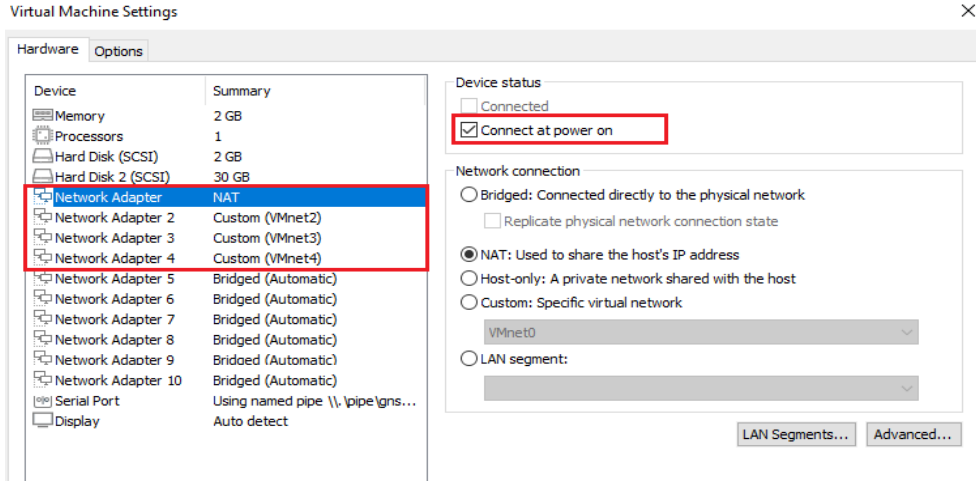


Labaratuvar ortamı kurulumu için Linux ve Windows VM kurulumları tamamlandıktan sonra VM'lerin network ayarlamalarını yapmak için VMWare-> Edit-> Virtual Network Edit kısmında sanal networkleri oluşturmakla başlayabiliriz.

"Change Settings" seçeneğini seçtikten sonra açılan pencerede "Add Network" butonu ile "VMNet2", "VMNet3" ve "VMNet4" adında üç adet sanal network oluşturularak network bilgilerinin tanımlanması gerekiyor. Tanımlama sırasında dikkat edilmesi gereken noktalardan birisi de "Use local DHCP service to distribute IP address to VMs" seçeneğinin seçili olmaması gerekiyor. Bu seçenek seçilmediğinde istemcilere ip adres bilgilerini manuel olarak tanımlarken default Gateway adresi olarak Fortigare FW'un o networkteki ip adresini tanımlayarak istemcilerin farklı networklere çıkışlarını kontrol edebilir duruma geleceğiz.

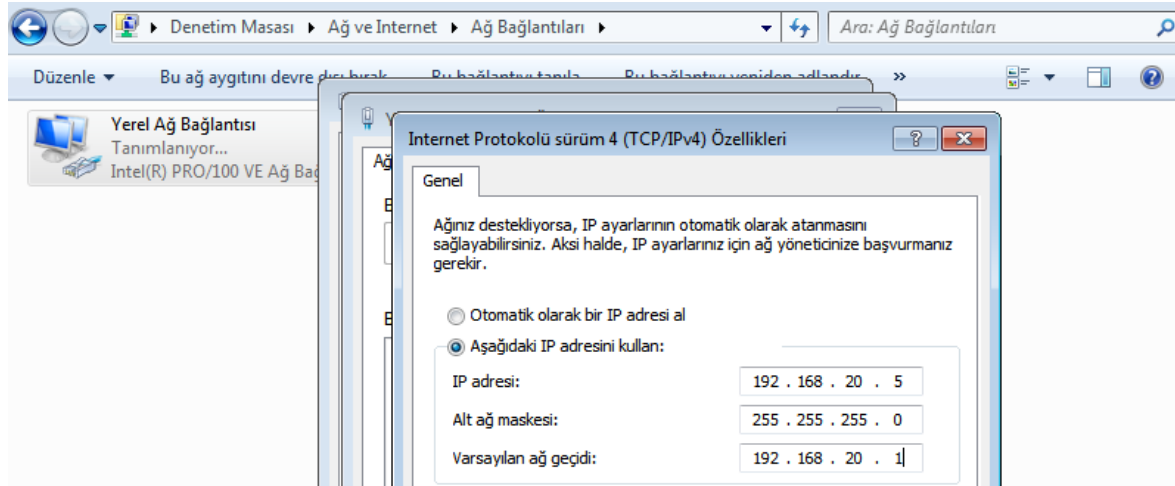


Sanal networkler oluşturulduktan sonra Fortigate FW'un ilgili portlarını bu networklere dahil etmek gerekiyor. Bu işlem için Fortigate VM'in ayarlar sayfasına girilerek portlarını topolojide belirtilen networklere dahil ediliyor. Dahil edilirken "Connect at power on" seçeneğinin seçili olmasına dikkat ediniz.



Fortigate FW'un bağlantıları yapıldıktan sonra topolojide bulunan diğer VM'lerde sırasıyla bağlanmaları gereken sanal networklere dahil edilerek ip adresleri tanımlanıyor. Özetle;

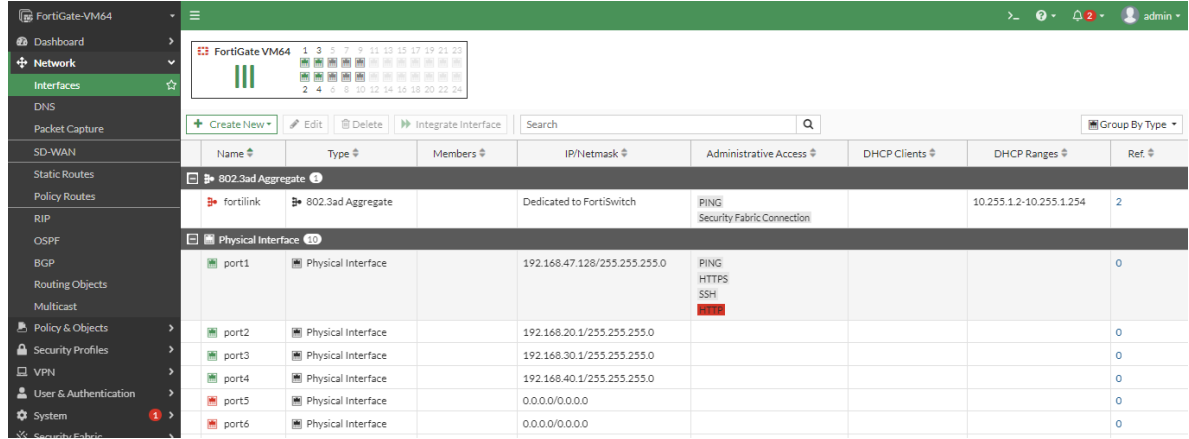
- Windows VM1 -> 192.168.20.0/24 networküne dahil edilerek 192.168.20.5 ip, 192.168.20.1 Default Gateway adresi olarak veriliyor.
- Linux VM -> 192.168.30.0/24 networküne dahil edilerek 192.168.30.5 ip, 192.168.30.1 Default Gateway adresi olarak veriliyor.
- Windows VM2 -> 192.168.40.0/24 networküne dahil edilerek 192.168.40.5 ip, 192.168.40.1 Default Gateway adresi olarak veriliyor.



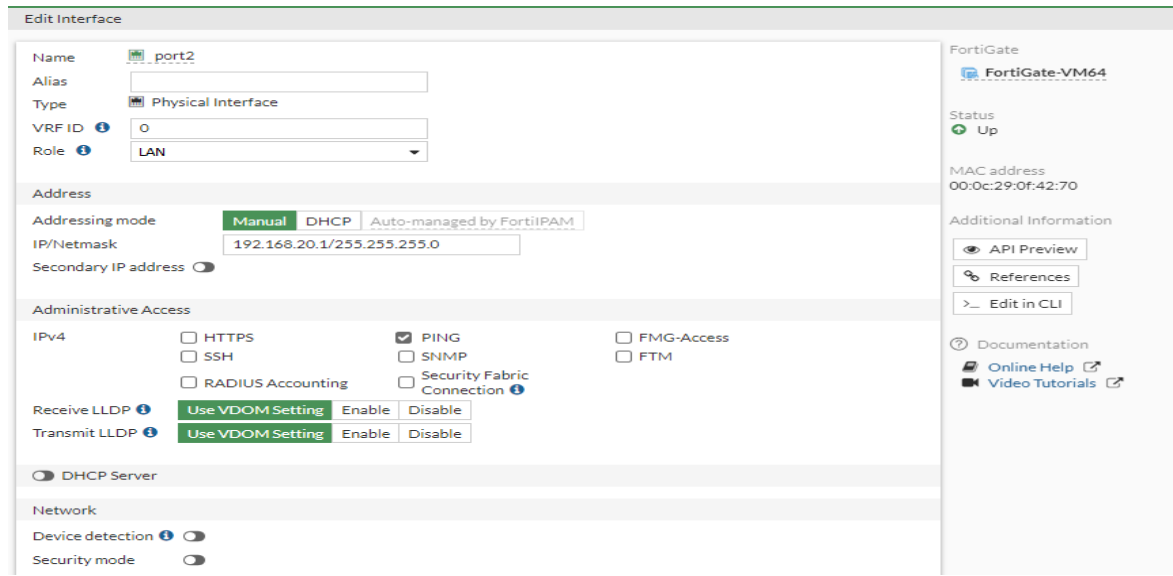
Bağlantıları tammaladıktan sonra Fortigate FW'un arayüzlerinde de ip adreslerinin tanımlanması gibi port özellikleri tanımlanmalıdır. Bu işlem iki farklı şekilde gerçekleştirilebilir. İlk seçenek komut satırı üzerinde aşağıdaki komutlar her bir port için ayrı ayrı uygulanabilir (ip tanımı yapılabileceği portun gibi diğer özellikleri de devreye alınabilir).

```
config system interface
edit port2
set ip 192.168.20.1/24
set allowaccess ping
end
```

İkinci seçenek ise web arayüzü üzerinden yapılabilir. Bunun için “Network-> Interfaces” kısmındaki portlardan ilgili portun arayüzüne giriş yapılır.



Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref
802.3ad Aggregate	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
port1	Physical Interface		192.168.47.128/255.255.255.0	PING HTTPS SSH			0
port2	Physical Interface		192.168.20.1/255.255.255.0				0
port3	Physical Interface		192.168.30.1/255.255.255.0				0
port4	Physical Interface		192.168.40.1/255.255.255.0				0
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0



**Edit Interface**

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

**Addressing mode**  
Manual DHCP Auto-managed by FortiIPAM  
IP/Netmask: 192.168.20.1/255.255.255.0  
Secondary IP address: ☐

**Administrative Access**  
IPv4: ☐ HTTPS ☒ PING ☐ FMG-Access  
☐ SSH ☐ SNMP ☐ FTM  
☐ RADIUS Accounting ☐ Security Fabric Connection  
Receive LLDP: Use VDOM Setting Enable Disable  
Transmit LLDP: Use VDOM Setting Enable Disable

☐ DHCP Server

**Network**  
Device detection: ☐  
Security mode: ☐

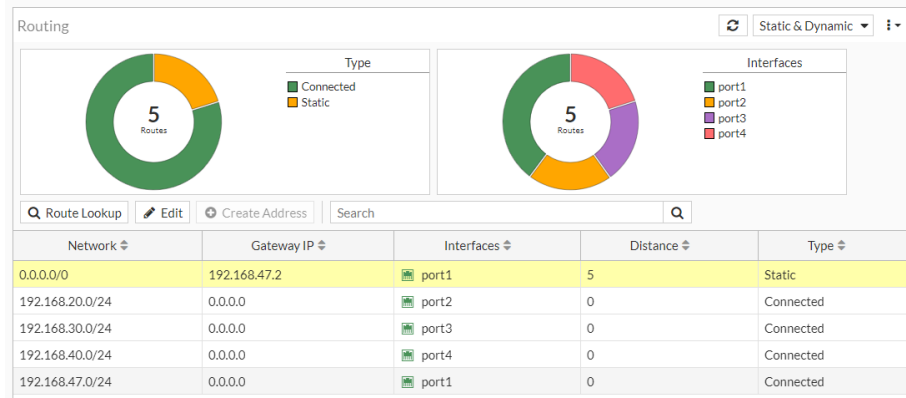
FortiGate VM64  
Status: Up  
MAC address: 00:0c:29:0f:42:70  
Additional Information: API Preview, References, Edit in CLI, Documentation, Online Help, Video Tutorials

Bu kısımda portun ip adresini nasıl alacağı, erişim izni verilecek protokoller, DHCP hizmeti verip vermeyeceği gibi daha birçok özellik devreye alınabilir. Burada ayrıca “Role” seçeneği Port1 için WAN seçilirken Port2, Port3 ve Port4 için LAN seçimi yapılmalıdır (Role belirtilmediği takdirde varsayılanda LAN geliyor - <https://docs.fortinet.com/document/fortigate/6.2.15/cookbook/574723/interface-settings>). Ip bilgileri tanımlandıktan sonra erişim kontrolü yapabilmemiz için PING paketlerine izin verilmesi gerekiyor (Web arayüzünün sağ kenarında “Edit in CLI” seçeneği ile CLI ekranı da kullanılabilir).

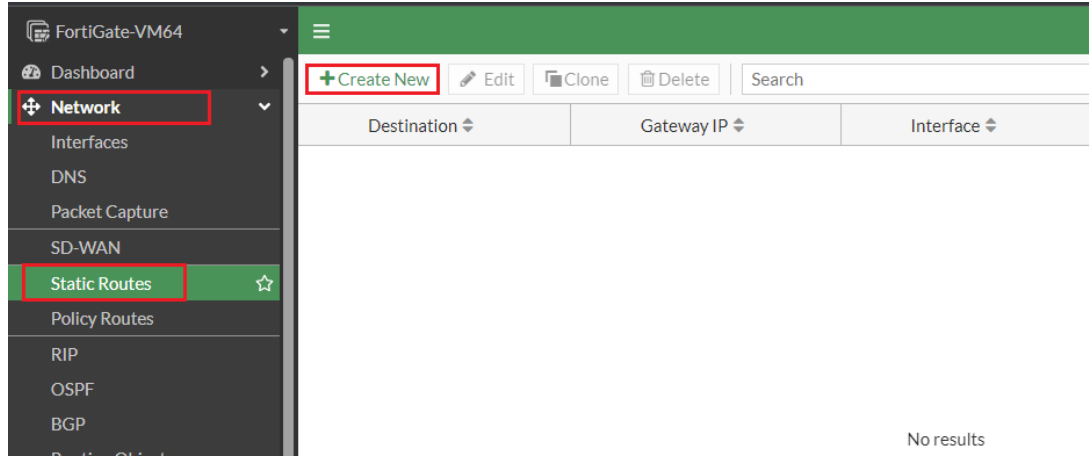
Fortigate arayüzlerine de ip adresleri tanımlandığına göre istemcilerden ilgili Fortigate arayüzlerine ping atabilir duruma gelinmelidir.

```
C:\Windows\system32\cmd.exe
Microsoft Windows [Sürüm 6.1.7601]
Telif Hakkı (c) 2009 Microsoft Corporation. Tüm hakları saklıdır.
C:\Users\Windows? Pro>ping 192.168.20.1
192.168.20.1 yoklanıyor 32 bayt veri ile:
192.168.20.1 cevabı: bayt=32 süre<1ms TTL=255
192.168.20.1 cevabı: bayt=32 süre<1ms TTL=255
192.168.20.1 cevabı: bayt=32 süre<1ms TTL=255
192.168.20.1 cevabı: bayt=32 süre<1ms TTL=255
192.168.20.1 için Ping istatistiği:
Paket: Giden = 4, Gelen = 4, Kaybolan = 0 (%0 kayıp),
Mili saniye türünden yaklaşık tür süreleri:
En Az = 0ms, En Çok = 0ms, Ortalama = 0ms
C:\Users\Windows? Pro>
```

Buraya kadarki kısımda sanal makinelerin Fortigate FW'e erişimleri sağlandı. Fortigate FW'un internete erişebilmesi için Static Route tanımlanması gerekiyor. Static Route tanımlanması otomatik olarak eklenmiş olabilir. Kontrol edebilmek için "Dashboard-> Routing Monitor" yolunu takip edebilirsiniz. Burada NAT Port1/NAT tanımlı port için Static Route tanımlanması varsayılarda gelmiş demektir. Yani ayrıca Static Route tanımlanmasına gerek yoktur.



Static Route tanımlanmadığı durumlarda "Network-> Static Route-> Create" yolunu takip ediliyor.



Bu kısımda "Destination" alanı ile herhangi bir hedef network adresine gönderilecek paketler temsil ediliyor. "Gateway" kısmında Port1'in gateway adresi/internete çıkış yapacağı ip adresi tanımlanıyor (Port1'in Gateway adresini Network-> Interfaces-> Port1 yolunu takip ederek görebilirsiniz). "Interface" kısmında Fortigate FW'un hangi portundan çıkış yapacağı tanımlanıyor.

Automatic gateway retrieval: ☒

Destination: Subnet Internet Service  
0.0.0.0/0.0.0.0

Gateway Address: Dynamic Specify  
192.168.47.2

Interface: port1

Administrative Distance: 10

Comments: Write a comment... 0/255

Status: ☒ Enabled ☐ Disabled

Advanced Options

OK Cancel

Static Route tanımlandıktan sonra test için internet üzerindeki herhangi bir adrese ping atılabilir.

```
CLI Console (1)
FortiGate-VM64 # execute ping 8.8.8.8
PING 8.8.8.8 (8.8.8.8): 56 data bytes
64 bytes from 8.8.8.8: icmp_seq=0 ttl=128 time=28.1 ms
64 bytes from 8.8.8.8: icmp_seq=1 ttl=128 time=16.7 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=128 time=17.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=128 time=18.3 ms
64 bytes from 8.8.8.8: icmp_seq=4 ttl=128 time=17.2 ms

--- 8.8.8.8 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 16.7/19.6/28.1 ms

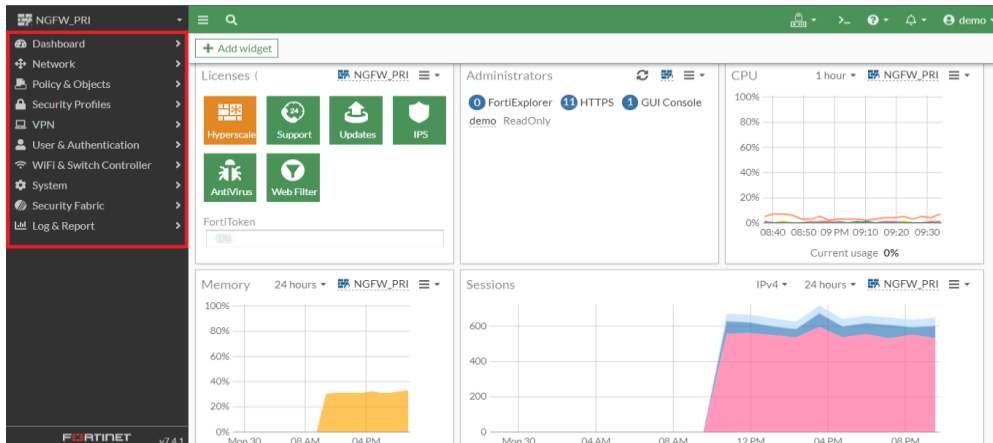
FortiGate-VM64 #
```

Bu işlemle beraber ortamının kurulum aşamaları tamamlandı. Bundan sonra Fortigarte FW üzerinde uygulamalar yapmaya başlanabilir.

## Fortigate Menülere Genel Bakış

Fortigate FW'un menülerine genel bir bakış atıldığında;

- **Dashboard**, cihazın genel durumu hakkında bilgilerin görüntülediği alandır. Alt tablalarında ekleme, çıkarma veya yer değiştirme işlemleri yapılarak widget'lar isteğe göre şekillendirilebilir.
- **Fortiview**, trafik akışı hakkındaki detayları görüntülemek için kullanılan alandır.
- **Network**, cihaz üzerindeki network bazlı ayarlamaları yapmak için kullanılan alandır.
- **Policy & Objects**, bir cihazın internet üzerinde bir hedefe ulaşması veya internet üzerindeki bir cihazın LAN içerisindeki bir cihaza erişmesi sürecinde kullanılacak politikaları tanımlamak için kullanılan alandır.
- **Security Profiles**, akan trafik üzerinde uygulanması istenen çeşitli güvenlik özelliklerini konfigüre etmek için kullanılan alandır.
- **VPN**, Ipsec ve SSLVPN gibi tünelleme konfigürasyonları yapabilmek için kullanılan alandır.
- **User & Authentication**, kullanıcı ve kimlik doğrulama işlemleri için konfigürasyonların yapıldığı alandır.
- **Wifi & Switch Controler**, kullanılan FortiAP'lerin konfigürasyonları için kullanılan alandır.
- **System**, cihaz üzerindeki sistemsel ayarlamaları yapmak için kullanılan alandır.
- **Security Fabric**, ağ üzerindeki etkilenen cihazları otomatik olarak görüntülenebilmesine ve dinamik olarak izole etmesine, ağ bölümlerini bölümlemesine, kuralları güncellemesine, yeni politikalar sunmasına ve kötü amaçlı yazılımları kaldırmasına olanak tanıyan alandır.
- **Log & Report**, wifi, VPN gibi logları görüntülemek için kullanılan alandır.



## NOTLAR

- Fortigate FW'un varsayılanda WAN bacağı DHCP modunda gelirken LAN bağacı 192.168.1.99 ip adresine ayarlanmış şekilde geliyor. Bu nedenle ilk konfigürasyonu için Console portundan bağlanılarak gerçekleştirilebildiği gibi 192.168.1.99 ip adresiyle web arayüzüne bağlanılarak da gerçekleştirilebiliyor.
  - Web arayüzünde kullanıcı adı kısmına "admin", parola kısmını boş bırakarak giriş yapılıyor. İlk girişte parola değiştirilmesi için uyarı verecektir. Parola bilgisi verildikten sonra "System-> Settings" yolu izlenerek tarih ve zaman bilgileri, kullanılacak servislerin çalışacağı port bilgileri gibi bilgiler tanımlanır.