

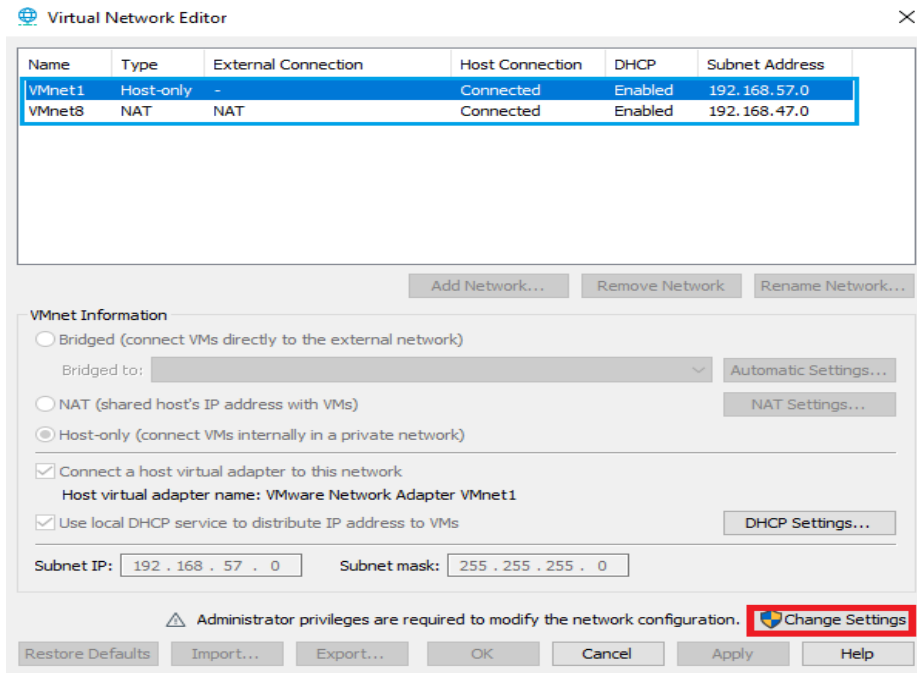
# FORTIGATE FIREWALL

Günümüzde çeşitli güvenlik özelliklerinin yanında router özelliklerini de desteklediği için kurumların internet çıkışlarında yaygın olarak güvenlik duvarı kullanımına yöneliyor. Bu nedenle yaygın olarak kullanılan güvenlik duvarlarını incelemeye ve konfigürasyonlarına yönelik notlar çıkarmaya da karar verdim. İncelemeye Fortigate Firewall ile başlayacağım.

Fortagate Firewall ile ilgili ilk olarak sanallaştırma üzerine çalışma ortamının kurulmasıyla başlayacağım. Kurulum için indirilmesi gereken uygulamalara bakıldığında;

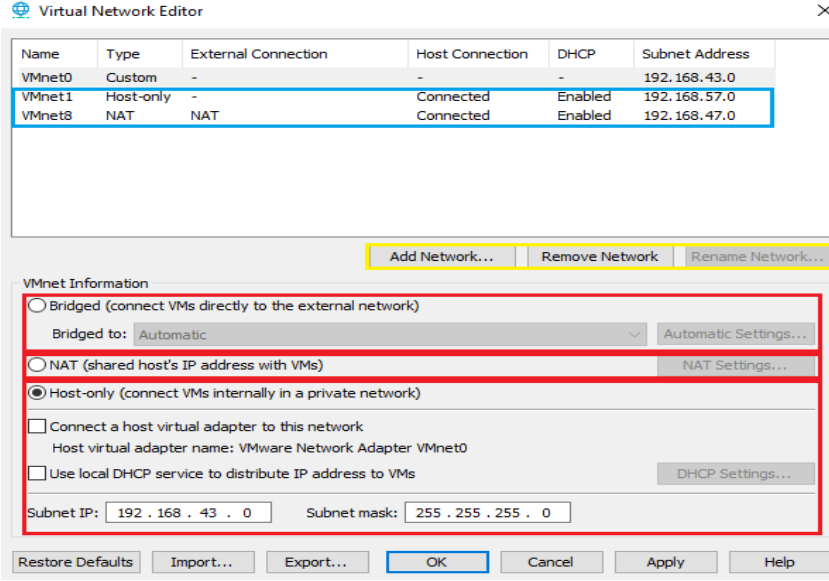
- VMWare Workstation Pro
- Fortigate FW (<https://support.fortinet.com/welcome/#/>)

İndirme ve temel kurulumlar (GNS3 ve VMWare kurulumları) yapıldıktan sonra ilk olarak VMWare üzerinde network ayarlarının yapılması gerekiyor. Bunun için VMWare ekranının sol üst köşesindeki **“Edit -> Virtual Network Editor”** seçeneği takip edilerek ayarlar sayfasına girilir. Bu kısım adından da anlaşılacağı gibi sanal network tanımları oluşturmak ve ayarlamalarını yapmak için kullanılıyor. Burada oluşturulan VMNet tanımlarına VMWare üzerindeki sanal makinelerin portları dahil edilerek sanal makinelerin bağlantı kurabilecekleri kapsam belirleniyor. Varsayılanda iki tane VMNet tanımı geliyor. Virtual Network Editor üzerinde değişiklik yapabilmek için sağ alt köşedeki **“Change Setting”** seçeneğinin seçilmesi gerekiyor.

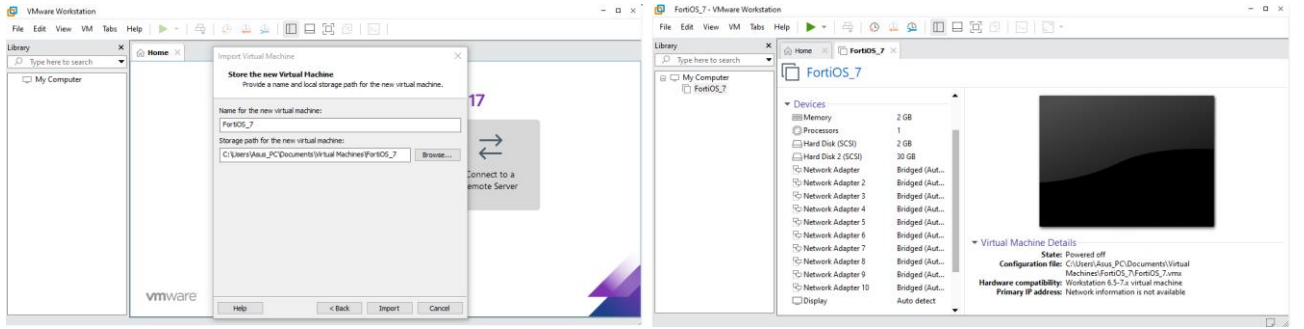


“Change Setting” seçeneği seçildikten sonra “Add Network” seçeneği ile yeni VMNet oluşturulabilir. Varolan veya sonradan oluşturulan herhangi bir VMnet seçildikten sonra;

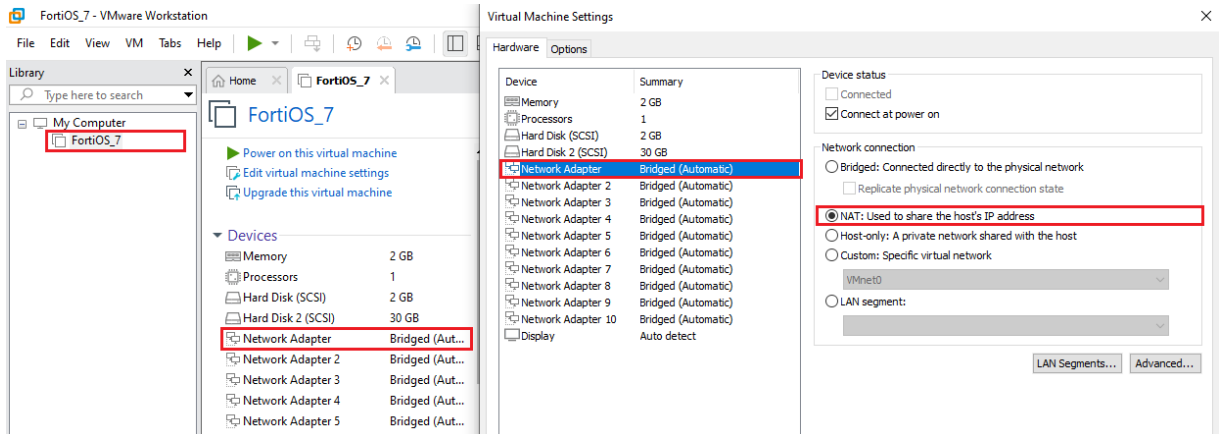
- “Bridge” seçeneği ile VM doğrudan internete çıkarılması sağlanabiliyor.
- “NAT” seçeneği ile VM’in ip adresi ana makinenin network adresine NAT’lanarak ana makin-VM arası bağlantı kurulması sağlanabiliyor
- “Host-Only” seçeneği seçilerek sanal makineler arasında kullanılacak sanal bir network tanımı yapılabilir (Bu seçimler topolojilere göre değişiklik göstereceği için şimdilik herhangi bir değişiklik yapılmıyor).



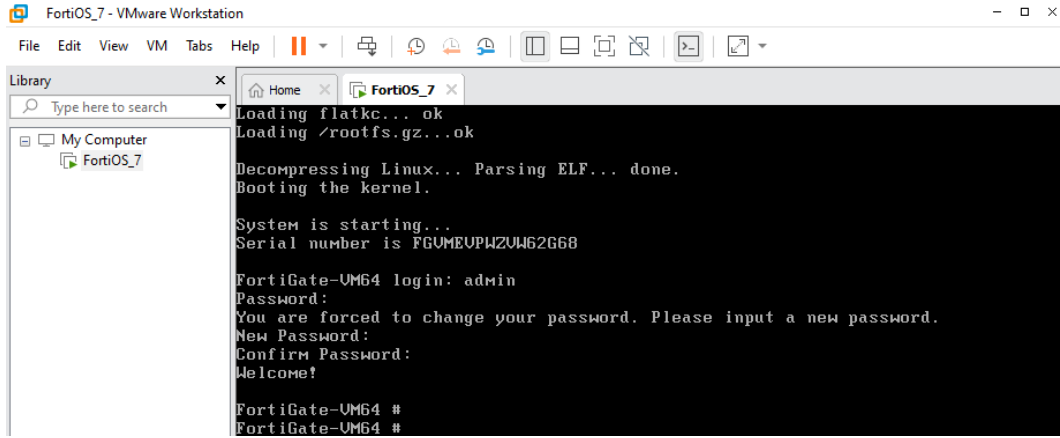
VMWare üzerindeki sanal network ayarlamaları yapıldıktan sonra “Open a Virtual Machine” seçeneğiyle indirilen Fortagate görüntüsü seçilip ve yüklenecek görüntüye isim tanımlı yapıldıktan sonra görüntü import edilecektir.



Fortigate görüntüsü VMWare uygulamasına aktarıldıktan sonra varsayılanda 2 GB ram 1 CPU, 32 GB hafıza alanı ve 10 sanal port ile gelmektedir. Bu portlar varsayılanda cihazınızda kullanılan network bağlantınıza doğrudan bağlı şekilde geliyor. Kurulum aşamasında ben ana bilgisayarımdan Fortigate arayüzüne bağlanacağım için 1. Portu NAT ayarlarına çekiyorum. Eğer ki burada farklı bir VM üzerinden Fortigate arayüzüne bağlanılacak ise “Custom: Specific Virtual Network” seçeneği ile “Virtual Network Editor” kısmında tanımlı VMNet’lerden biri seçilebilir (Aynı zamanda arayüze bağlanılamıyorsa istenen sanal makinenin de network ayarlarında aynı VMNet’in seçilmesi gerekiyor unutma).



Seimler uygulandıktan sonra sanal makina başlatılabilir (Deneme sürümü olduėu için Web filtreleme gibi bazı özellikler kullanılamıyor). Yükleme işlemleri sonunda oturum açmak için kullanıcı adı ve parola soracaktır. Kullanıcı adı olarak “admin” girilir ve parola kısm boş girildikten sonra peerola belirleme işlemi için yeni bir parola girilmesini isteyecektir.



```
FortiOS_7 - VMware Workstation
File Edit View VM Tabs Help
Library
Type here to search
My Computer
FortiOS_7
Loading flatk... ok
Loading /rootfs.gz...ok
Decompressing Linux... Parsing ELF... done.
Booting the kernel.
System is starting...
Serial number is FGUMEUPWZUM62G68
FortiGate-UM64 login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!
FortiGate-UM64 #
FortiGate-UM64 #
```

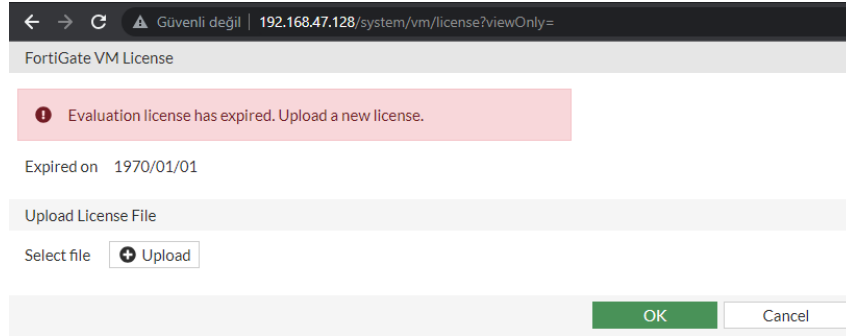
Admin hesabı için yeni parola bilgisi tanımlandıktan sonra arayüzlerin durumunu görüntülemek için “**show system interface ?**” komutu kullanılıyor (Daha fazla komut için [https://help.fortinet.com/faith/5-3/Content/Admin%20Guides/5\\_3%20Admin%20Guide/200/204\\_CLI\\_commands.htm](https://help.fortinet.com/faith/5-3/Content/Admin%20Guides/5_3%20Admin%20Guide/200/204_CLI_commands.htm) sayfasını ziyaret edebilirsiniz).

```
FortiGate-UM64 # show system interface
name      Name.
fortilink static 0.0.0.0 0.0.0.0 10.255.1.1 255.255.255.0 up disable a
ggregate enable
port1     dhcp 0.0.0.0 0.0.0.0 192.168.47.128 255.255.255.0 up disable phy
sical enable
port2     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port3     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port4     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port5     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port6     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port7     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port8     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port9     static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical enab
le
port10    static 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up disable physical ena
ble
--More-- _
```

İlk portun ip bilgilerini aldıėı gördükten sonra aşğıdaki komutları çalıştırarak bu port üzerinde izin verilecek protokollerin tanımlanması gerekiyor ki bu porta atanan ip adresi üzerinden fortigate arayüzüne erişebilelim (Tanımlamamalar sonrasında ICMP protokolüne de izin verildiėi için Fortigate arayüzüne bağlanılacak cihazdan Fortigate arayüzüne tanımlı ip adresine ping atarak bağlantıyı kontrol edebilirsiniz).

```
FortiGate-UM64 # config system interface
FortiGate-UM64 (interface) # edit port1
FortiGate-UM64 (port1) # set allowaccess http https ssh ping
FortiGate-UM64 (port1) # end
FortiGate-UM64 #
```

Bu adımlardan sonra Fortigate arayüzünde tanımlı ip adresini kullanarak tarayıcıdan arayüzüne erişilebilir (Kurulum yaparken tanımladığın kullanıcı adı ve parola bilgisini kullanarak oturum açabilirsin). Giriş yaptıktan sonra lisans süresinin dolmasıyla ilgili bir hata verecektir.



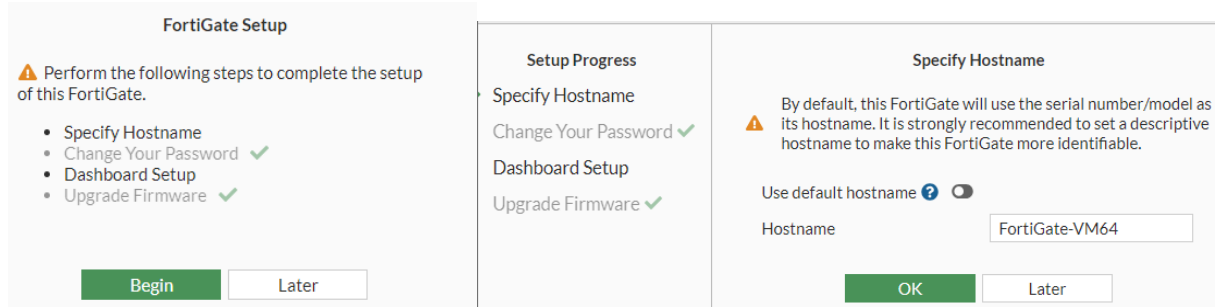
The screenshot shows the FortiGate VM License page. At the top, there's a warning message: "Evaluation license has expired. Upload a new license." Below this, it says "Expired on 1970/01/01". There's a section for "Upload License File" with a "Select file" button and an "Upload" button. At the bottom, there are "OK" and "Cancel" buttons.

Lisans hatasını gidermek için komut satırında aşağıdaki komutların çalıştırılarak güvenlik duvarının tarih ve zaman bilgilerini NTP sunucusundan otomatik olarak senkronize etmesi engellenebiliyor (alternatif olarak **“execute factoryreset”** komutu çalıştırılarak fabrika ayarlarına döndürülmesi sağlanabiliyor. Unutma fabrika ayarlarına geri döndürürsen konfigürasyonların tekrar yapılması gerekiyor)

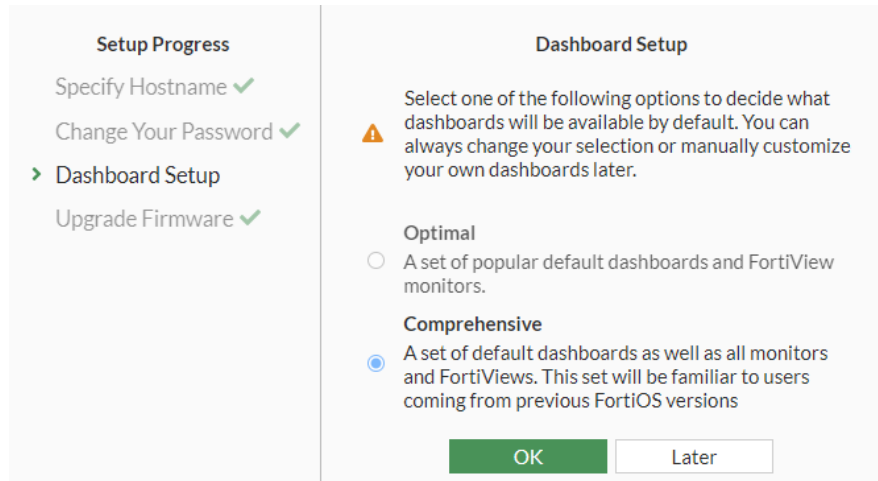
```
FortiGate-VM64-KVM # config system ntp
FortiGate-VM64-KVM (ntp) # set ntpsync disable
FortiGate-VM64-KVM (ntp) # set type custom
FortiGate-VM64-KVM (ntp) # end
FortiGate-VM64-KVM # execute reboot
```

```
FortiGate-VM64 # execute factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)_
```

Lisans hatasını giderilip Fortigate arayüzüne tekrar giriş yapıldıktan sonra ilk olarak bir Hostname belirlememiz ve kontrol paneli seçmemiz isteniyor.



The screenshot shows the FortiGate Setup screen. On the left, there's a list of steps: "Specify Hostname", "Change Your Password", "Dashboard Setup", and "Upgrade Firmware". The "Specify Hostname" step is currently active. On the right, there's a section titled "Specify Hostname" with a warning message: "By default, this FortiGate will use the serial number/model as its hostname. It is strongly recommended to set a descriptive hostname to make this FortiGate more identifiable." Below this, there's a toggle for "Use default hostname" and a text input field for "Hostname" with the value "FortiGate-VM64". At the bottom, there are "OK" and "Later" buttons.



The screenshot shows the FortiGate Setup screen, specifically the "Dashboard Setup" step. On the left, there's a list of steps: "Specify Hostname", "Change Your Password", "Dashboard Setup", and "Upgrade Firmware". The "Dashboard Setup" step is currently active. On the right, there's a section titled "Dashboard Setup" with a warning message: "Select one of the following options to decide what dashboards will be available by default. You can always change your selection or manually customize your own dashboards later." Below this, there are two options: "Optimal" (radio button) and "Comprehensive" (radio button, which is selected). The "Comprehensive" option is described as: "A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions". At the bottom, there are "OK" and "Later" buttons.

Yukarıdaki adımlardan sonra Fortigate kurulum adımları tamamlanmıştır. Artık kendi topolojilerimizi oluşturup uygulamalar yapmaya başlayabiliriz.

The screenshot displays the FortiGate VM64 dashboard interface. The top navigation bar includes a search icon, a star icon, a settings icon, a user profile icon labeled 'Gizli mod', and a dropdown menu for 'admin'. The left sidebar contains a 'Dashboard' menu with a 'Status' sub-menu, and a list of monitoring tools including FortiView Sources, FortiView Destinations, FortiView Applications, FortiView Web Sites, FortiView Threats, FortiView Compromised Hosts, FortiView Policies, FortiView Sessions, Device Inventory Monitor, Routing Monitor, DHCP Monitor, SD-WAN Monitor, FortiGuard Quota Monitor, and ID Protection Monitor. The main content area is divided into several widgets: 'System Information' showing Hostname (FortiGate-VM64), Serial Number (FGVMEVPWZVW62G68), Firmware (v7.0.0 build0066 (GA)), Mode (NAT), System Time (2023/10/28 04:39:14), Uptime (00:00:11:09), and WAN IP (Unknown); 'Licenses' showing FortiCare Support, Firmware & General Updates, IPS, AntiVirus, and Web Filtering, with a FortiToken of 0/0 and a red warning 'Unable to connect to FortiGuard servers.'; 'Virtual Machine' showing FGVMEV License, Allocated vCPUs (1/1, 100%), and Allocated RAM (2 GiB / 2 GiB, 98%); 'FortiGate Cloud' showing Status as 'Not Supported'; 'Security Fabric' showing various security icons and FortiGate-VM64; and 'Administrators' showing HTTP and FortiExplorer protocols, with users 'admin' and 'super\_admin'.

System Information	Licenses	Virtual Machine	FortiGate Cloud	Security Fabric	Administrators
Hostname: FortiGate-VM64 Serial Number: FGVMEVPWZVW62G68 Firmware: v7.0.0 build0066 (GA) Mode: NAT System Time: 2023/10/28 04:39:14 Uptime: 00:00:11:09 WAN IP: Unknown	FortiCare Support Firmware & General Updates IPS AntiVirus Web Filtering FortiToken: 0/0 Unable to connect to FortiGuard servers.	FGVMEV License Allocated vCPUs: 1 / 1 (100%) Allocated RAM: 2 GiB / 2 GiB (98%)	Status: Not Supported	FortiGate-VM64	HTTP, FortiExplorer admin, super_admin

