

FORTİGATE FİREWALL KURULUMU

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.

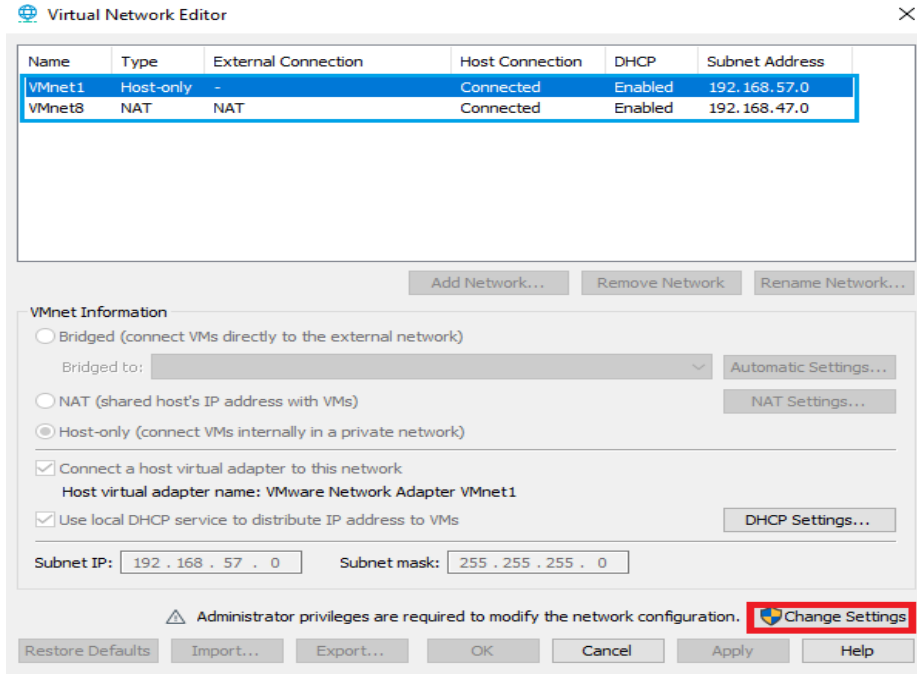
Fortagate Firewall ile ilgili ilk olarak sanallaştırma üzerine çalışma ortamının kurulmasıyla başlayacağım. Kurulum için indirilmesi gereken uygulamalara bakıldığında;

- VMWare Workstation Pro
- Fortigate FW (<https://support.fortinet.com/welcome/#/>)
 - o Kayıt olduktan sonra aşağıdaki görselde ifade edilen sıralama takip edilerek istenilen Fortigate FW görüntüsü indirilir.

The screenshot shows the FortiCloud support page. The 'Support' menu is highlighted with a red box and labeled '1'. The 'Downloads' section is visible, with 'VM Images' highlighted by a red box and labeled '2'. Below this, the 'FortiGate for VMware ESXi platform Version 7.0.13' page is shown. The 'Select Product' dropdown is set to 'FortiGate' (labeled '1') and the 'Select Platform' dropdown is set to 'VMWare ESXi' (labeled '2'). The 'Latest Version' section shows '7.0.13' highlighted with a green box and labeled '3'. The 'Download' button is highlighted with a green box and labeled '4'.

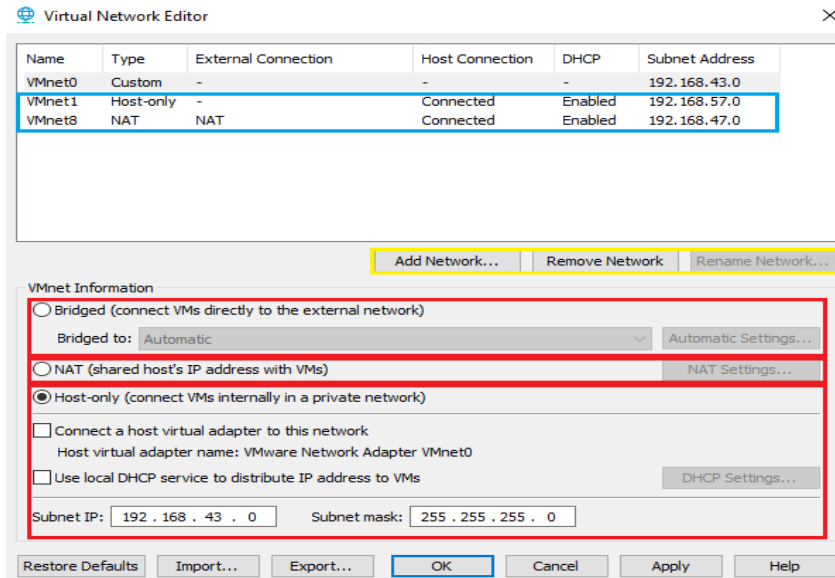
File Information	Checksum	Release Date
Upgrade from previous version of FortiGate for VMware FFW_VM64-v7.0.13.M-build0566-FORTINET.out (81.22 MB)	6754d583b77f32d9d8151a336c9af5f7 (Regular) a4bf76b417932981fc506915bdc7a346f31d1932de6fbc86a94cbfec8064a31111c8e06059d008621ae5295696f037f172be3e5487f3c98ef4e0ef547a8a21 (SHA-512)	2023-10-26
New deployment of FortiGate for VMware FFW_VM64-v7.0.13.M-build0566-FORTINET.out.ovf.zip (80.94 MB)	4cec6c90e4af70cb96b55ad5ea5b6d5ea (Regular) 4f1cdd31f1ba59891e1cf6679f3225f5a62e3d79d78cd4ba3d00e2384ed82cfea239525e72a67eaa2fc4333c0000f77edf4763b2b6bfb6d91ab764db64fa9ef (SHA-512)	2023-10-26

İndirme işlemleri ve VMWare kurulumu 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.

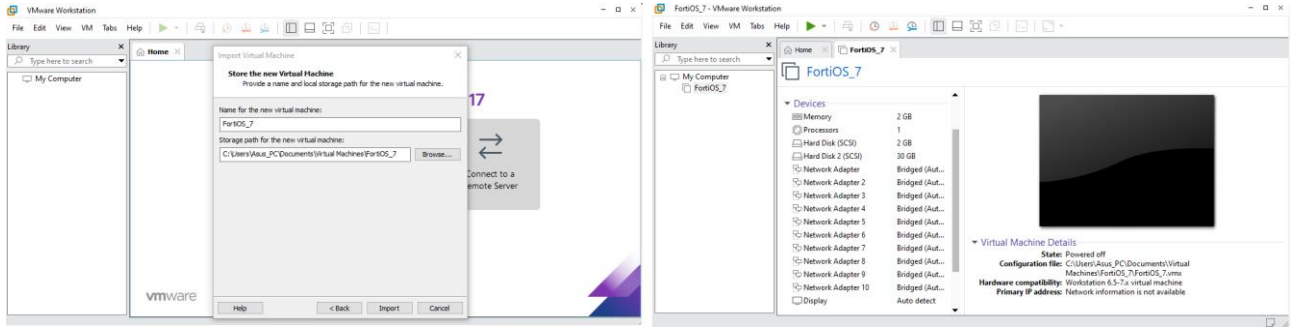


“Change Setting” seçeneği seçildikten sonra “Add Network” seçeneği ile yeni VMNet oluşturulabilir. Varsayılanda gelen veya sonradan oluşturulan herhangi bir VMnet seçildikten sonra (Şimdilik sadece kurulum yapılacağı için VMNet üzerinde herhangi bir ayarlama yapmaya gerek yoktur);

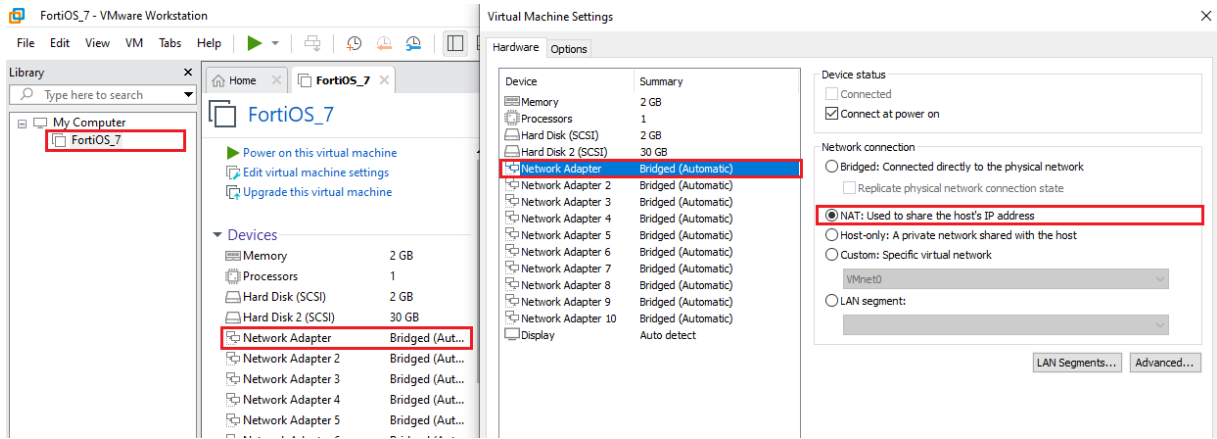
- “Bridge” seçeneği ile VM doğrudan internete çıkarılması sağlanabiliyor.
- “NAT” seçeneği ile VM’in ip adresi ana makinenin network adresine NAT’lanarak ana makin-VM arası bağlantı kurulması sağlanabiliyor
- “Host-Only” seçeneği seçilerek sanal makineler arasında kullanılacak sanal bir network tanımı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



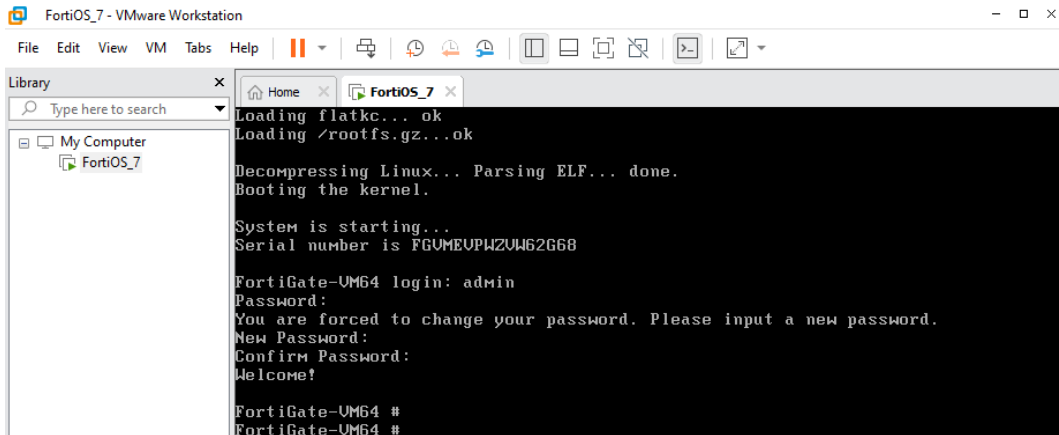
İsteğe yönelik Fortigate VM üzerindeki sanal network ayarlamaları yapıldıktan sonra “Open a Virtual Machine” seçeneğiyle indirilen Fortigate görüntüsü seçilip ve yüklenecek görüntüye isim tanımı yapıldıktan sonra görüntü import edilecektir.



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). Kullanılmayacak arayüzleri kapatmak için “Connect at power on” kısmındaki seçimi kaldırabilirsin.



Seçimler uygulandıktan sonra sanal makina başlatılabilir (Deneme sürümü olduğu 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 kısmı boş girildikten sonra parola belirleme işlemi için yeni bir parola girilmesini isteyecektir.



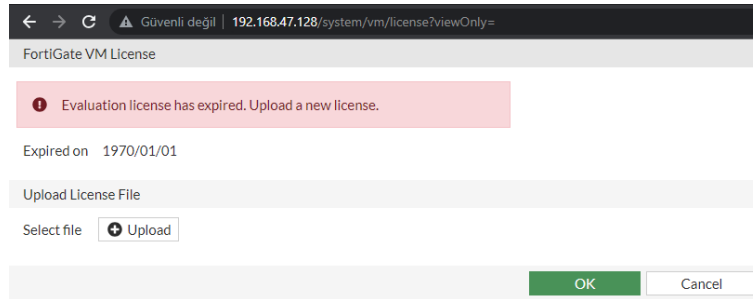
Admin hesabı için yeni parola bilgisi tanımlandıktan sonra arayüzlerin durumunu görüntülemek için “**show system interface ?**” komutu kullanılıyor (Daha fazla komut için https://help.fortinet.com/fauth/5-3/Content/Admin%20Guides/5_3%20Admin%20Guide/200/204_CLI_commands.htm sayfasını ziyaret edebilirsiniz).

```
FortiGate-VM64 # 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 aldığı gördükten sonra aşağıdaki komutları çalıştırarak bu port üzerinde izin verilecek protokollerin tanımlanması gerekiyor ki bu porta atanan ip adresi üzerinden fortigate arayüzüne erişilelim (Tanımlamalar sonrasında Ping paketlerine de izin verildiği için Fortigate arayüzüne bağlanılacak cihazdan Fortigate arayüzüne tanımlı ip adresine ping atarak bağlantıyı kontrol edebilirsiniz).

```
FortiGate-VM64 # config system interface
FortiGate-VM64 (interface) # edit port1
FortiGate-VM64 (port1) # set allowaccess http https ssh ping
FortiGate-VM64 (port1) # end
FortiGate-VM64 #
```

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



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

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

```
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
```

- Bu seçenekler Fortigate V7.0.13 için geçerlidir. Farklı sürümlerde lisanslama süreci değişiklik gösterebilir (Örnek olarak Fortinet hesabıyla kimlik doğrulama işlemi gerekebilir).

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

FortiGate Setup
Perform the following steps to complete the setup of this FortiGate.

- Specify Hostname
- Change Your Password ✓
- Dashboard Setup
- Upgrade Firmware ✓

Begin Later

Setup Progress
Specify Hostname ✓
Change Your Password ✓
Dashboard Setup
Upgrade Firmware ✓

Specify Hostname
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.
Use default hostname ? ☐
Hostname

OK Later

Setup Progress
Specify Hostname ✓
Change Your Password ✓
Dashboard Setup
Upgrade Firmware ✓

Dashboard Setup
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.
Optimal
☐ A set of popular default dashboards and FortiView monitors.
Comprehensive
☒ A set of default dashboards as well as all monitors and FortiViews. This set will be familiar to users coming from previous FortiOS versions

OK Later

Yukarıdaki adımlardan sonra Fortigate kurulum adımları tamamlanmıştır (İsteğe bağlı olarak GNS3 üzerine entegre edilerek de kullanılabilir. Bunun için GNS3 üzerinde “preferences->VMWare VMs-><Oluşturulan Fortigate VM>” seçilerek GNS3 üzerinde kurulan topolojilerde kullanılabilir). Artık kendi topolojilerimizi oluşturup uygulamalar yapmaya başlayabiliriz.

FortiGate-VM64

Dashboard
Status
+ Add Widget

System Information
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

Licenses
FortiCare Support
Firmware & General Updates
IPS
AntiVirus
Web Filtering
FortiToken: 0/0
Unable to connect to FortiGuard servers.

Virtual Machine
FGVMEV License
Allocated vCPUs: 1 / 1 (100%)
Allocated RAM: 2 GiB / 2 GiB (98%)

FortiGate Cloud
Status: Not Supported

Security Fabric
FortiGate-VM64

Administrators
HTTP FortiExplorer
admin super_admin

Notlar:

- Fortigate FW cihazı fiziksel olarak ilk kurulumu Console portundan bağlanılarak yapılabildiği gibi cihazların LAN bacağına varsayılanda 192.168.1.99 ip adresi atanmış olarak gelmektedir. Bu ip adresi üzerinden de arayüzüne bağlanılarak ilk kurulum gerçekleştirilebiliyor.
 - 192.168.1.99 ip adresiyle arayüze bağlanıldığında kullanıcı adı kısmına “admin” girilerek parola kısmı boş bırakılıyor. Giriş yapıldıktan sonra da kullanıcıyı parola belirleme ekranı karşılamaktadır.