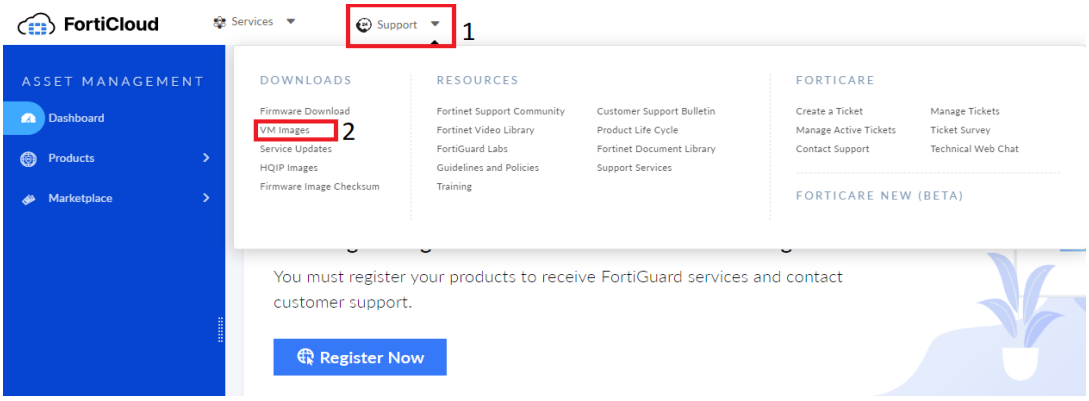
FORTİGATE FİREWALL KURULUMU

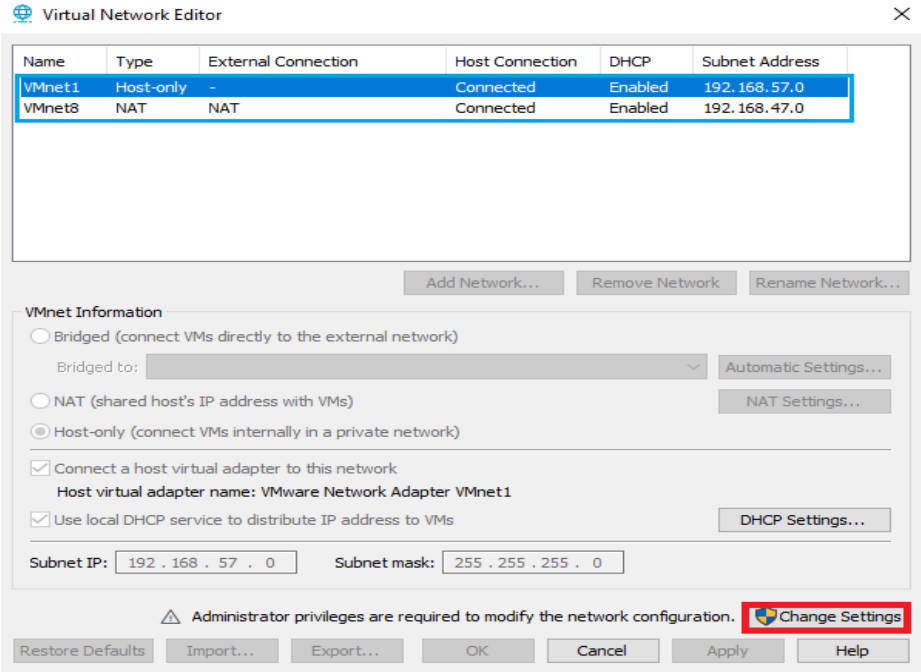
Günümüzde çeşitli güvenlik özelliklerinin yanında router özelliklerini de desteklediği için kurumların internet çıkışlarında yaygın olarak güvenlik duvarı kulanımına yöneltiyor. Bu nedenle yaygın olarak kullanılan güvenlik duvarlarını incelemeye ve konfigürasyonlarına yönelik notlar çıkarmaya da karar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

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/#/)
    - Kayıt olduktan sonra aşağıdaki görselde ifade edilen sıralama takip edilerek istenilen Fortigate FW görüntüsü indirilir.

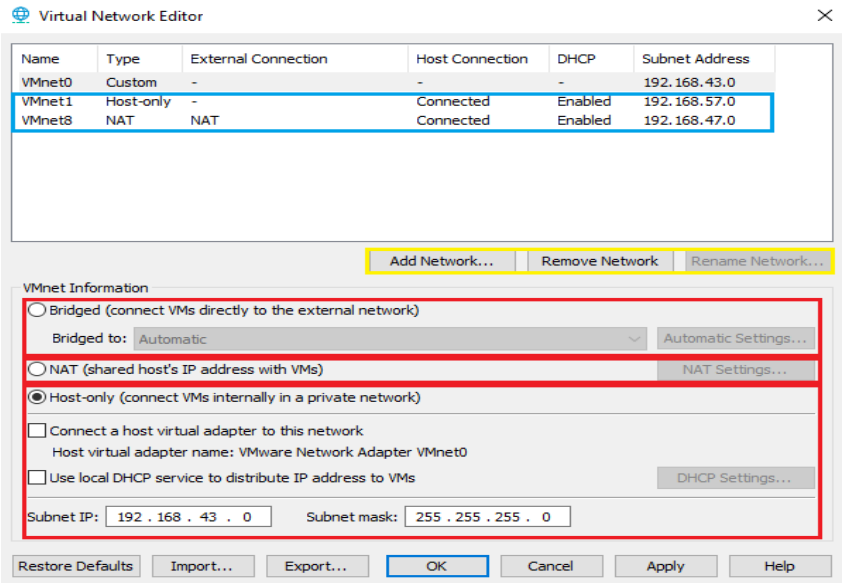


İndirme işlemleri ve VMWare kurulumu yapıldıktan sonra ilk olarak VMWare üzerinde network ayarlarının yapılması gerekiyor. Bunun için VMWare ekranının sol üst köşesindeki "**Edit -> Virtual Network Editor**" seçeneği takip edilerek ayarlar sayfasına girilir. Bu kısım adından da anlaşılacağı gibi sanal 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.

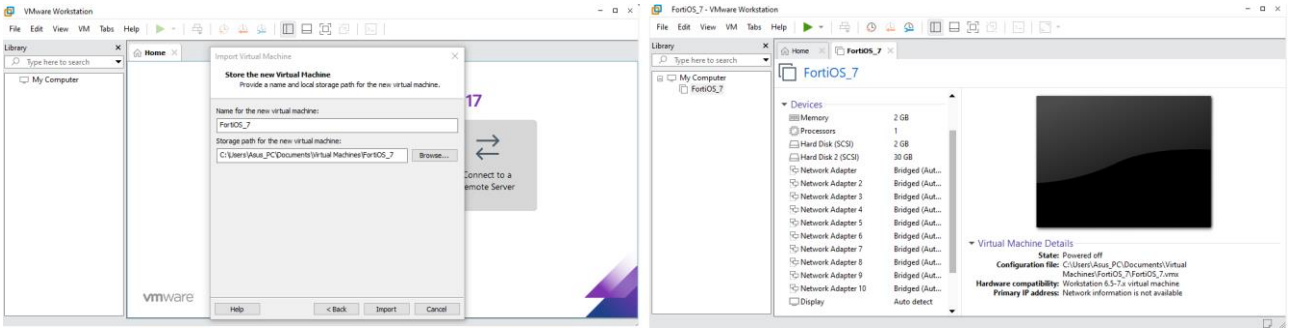


"Change Setting" seçeneği seçildikten sonra "Add Network" seçeneği ile yeni VMNet oluşturulabilir. Varsayılanda gelen veya sonradan oluşturulan herhangi bir VMnet seçildikten sonra (Şimdilik sadece kurulum yapılacağı için VMNet üzerinde herhangi bir ayarlama yapmaya gerek yoktur);

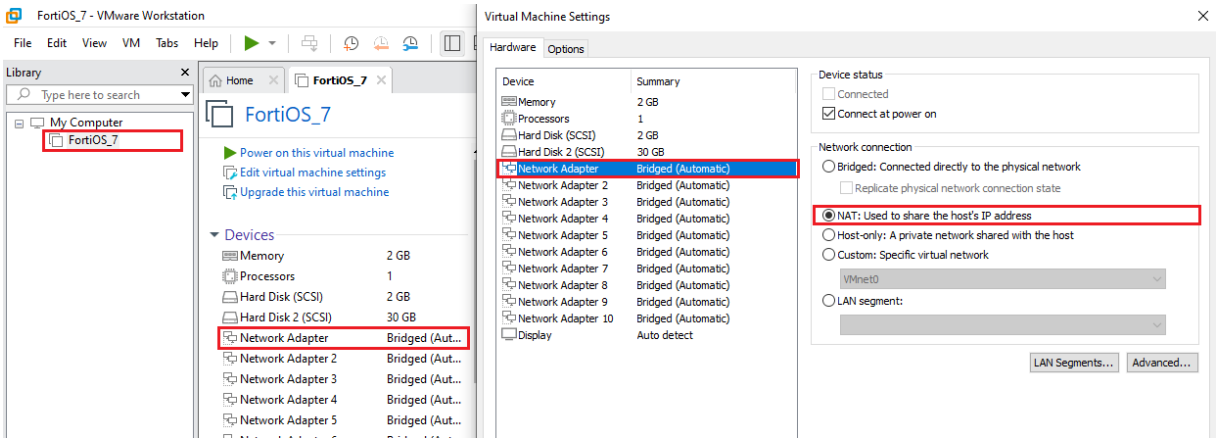
- "Bridge" seçeneği ile VM doğrudan internete çıkarılaması sağlanabiliyor.
- "NAT" seçeneği ile VM'in ip adresi ana makinenin network adresine NAT'lanarak ana makin-VM arası bağlantı kurulması sağlanabiliyor
- "Host-Only" seçeneği seçilerek sanal makineler arasında kullanılacak sanal bir network tanımı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



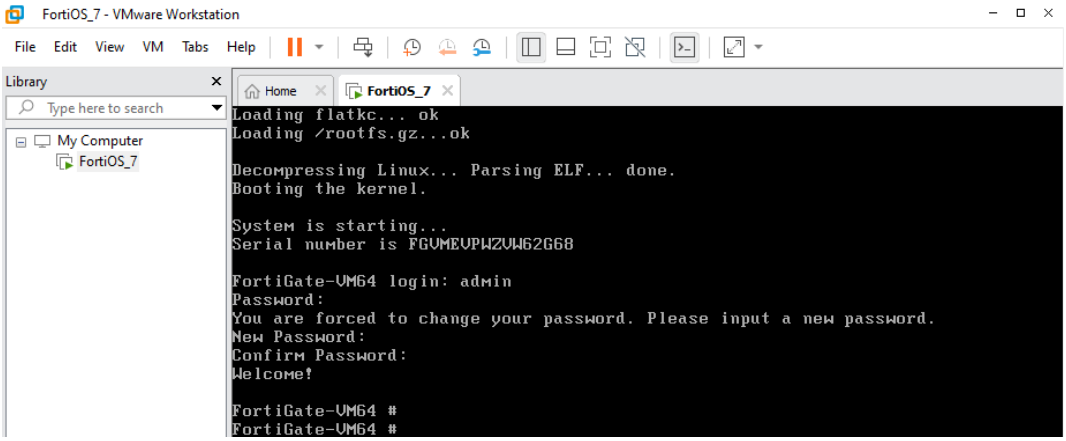
İsteğe yönelik Fortigate VM üzerindeki sanal network ayarlamaları yapıldıktan sonra "Open a Virtual Machine" seçeneğiyle indirilen Fortagate görüntüsü seçilip ve yüklenecek görüntüye isim tanımı yapıldıktan sonra görüntü import edilecektir.



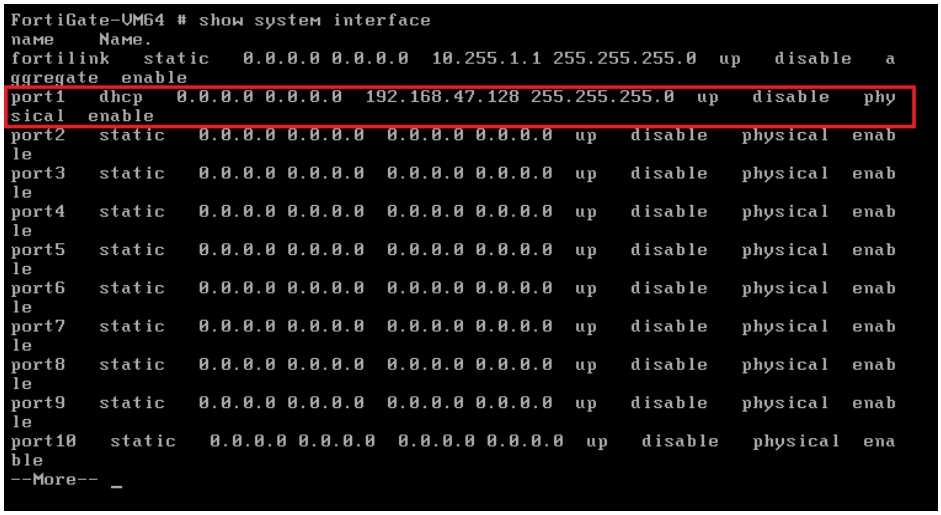
Fortigate görüntüsü VMWare uygulamasına aktarıldıktan sonra varsayılanda 2 GB ram 1 CPU, 32 GB hafıza alanı ve 10 sanal port ile gelmektedir. Bu portlar varsayılanda cihazınızda kullanılan network bağlantınıza doğrudan bağlı şekilde geliyor. Kurulum aşamasında ben ana bilgisayarımdan Fortigate arayüzüne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



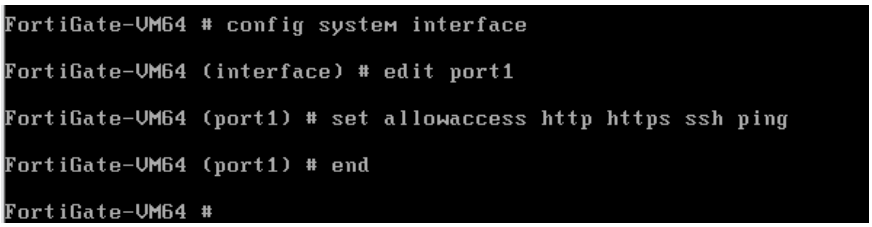
Seçimler uygulandıktan sonra sanal makina başlatılabilir (Deneme sürümü olduğu için Web filtreleme gibi bazı özellikler kullanılamıyor). Yükleme işlemleri sonunda oturum açmak için kullanıcı adı ve parola soracaktır. Kullanıcı adı olarak "admin" girilir ve parola kısm boş girildikten sonra parola belirleme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



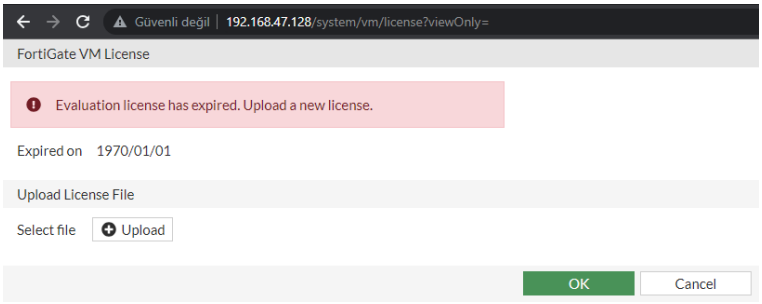
Admin hesabı için yeni parola bilgisi tanımlandıktan sonra arayüzlerin durumunu görüntülemek için "**show system interface ?**" komutu kullanılıyor (Daha fazla komut için https[:]//help.fortinet.com/fauth/5-3/Content/Admin%20Guides/5_3%20Admin%20Guide/200/204_CLI_commands.htm sayfasını ziyeret edebilirsin).



İlk portun ip bilgilerini aldığı görldükten sonra aşağıdaki komutları çalıştırarak bu port üzerinde izin verilecek protokollerin tanımlanması gerekiyor ki bu porta atanan ip adresi üzerinden fortigate arayüzüne erişebilelim (Tanımlamamlar sonrasında Ping paketlerine de izin verildiği için Fortigate arayüzüne bağlanılacak cihazdan Fortigate arayüzüne tanımlı ip adresine ping atarak bağlantıyı kontrol edebilirsin).



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 dolmasıyal ilgili bir hata verecektir.



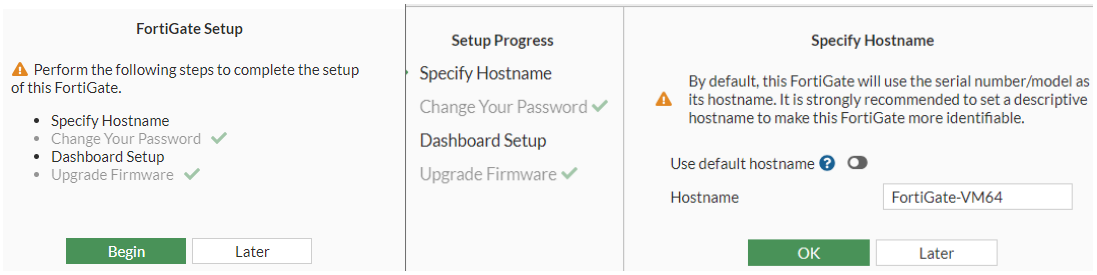
Lisans hatasını gidermek için komut satırında aşağıdaki komutların çalıştırılarak "**execute factoryreset**" komutu çalıştırılarak fabrika ayarlarına döndürülmesi sağlanabiliyor. Unutma fabrika ayarlarına geri döndürürsen konfigürasyonların tekrar yapılması gerekiyor (alternatif olarak güvenlik duvarının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

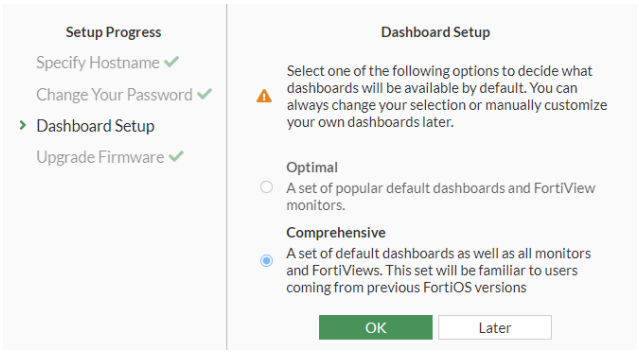
```
FortiGate-VM64 # execute factoryreset
This operation will reset the system to factory default!
Do you want to continue? (y/n)_
```

```
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
```

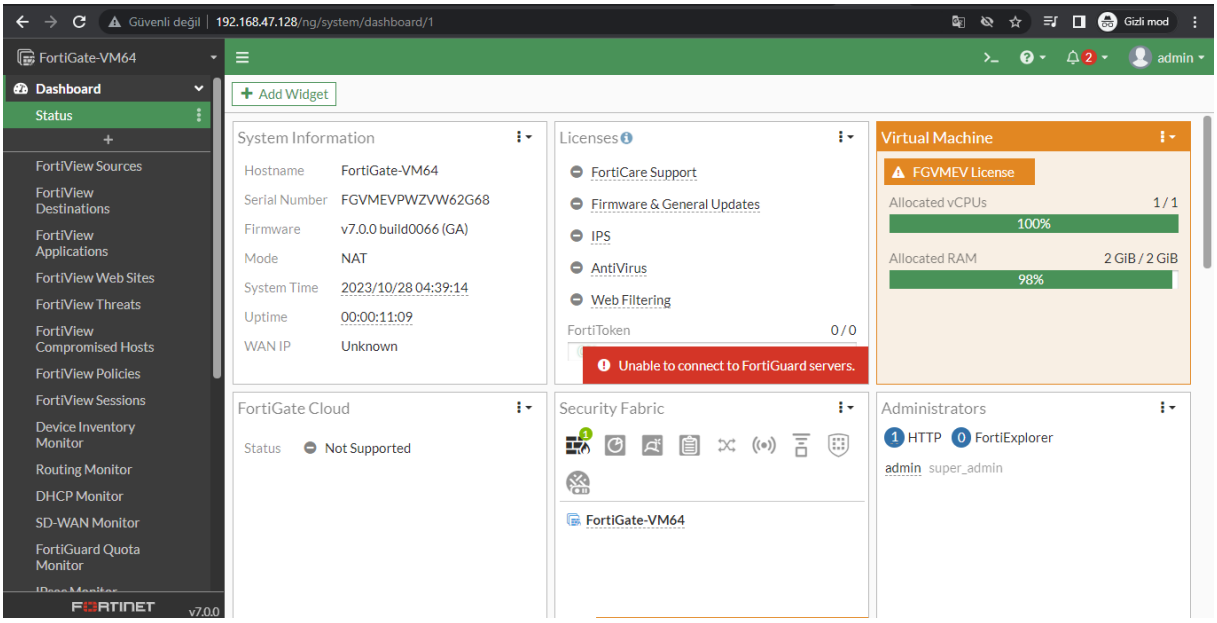
- Bu seçenekler Fortigate V7.0.13 için geçerlidir. Farklı sürümlerde lisanslama süreci değişiklik gösterebilir (Örnek olarak Fortinet hesabıyla kimlik doğrulama işlemi gerekebilir).

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





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.



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.