

# FORTIGATE FIREWALL KURULUMU

Günümüzde çeşitli güvenlik özelliklerinin yanında router özelliklerini de desteklediği için kurumlar internet çıkışlarında güvenlik duvarı kullanmayı tercih ediyor. Bu nedenle yaygın olarak kullanılan güvenlik duvarlarını incelemeye ve konfigürasyonlarına yönelik notlar çıkarmaya da karar verdim. İncelemeye bu seriden de anlaşılağı üzere Fortigate Firewall ile başlaayım.

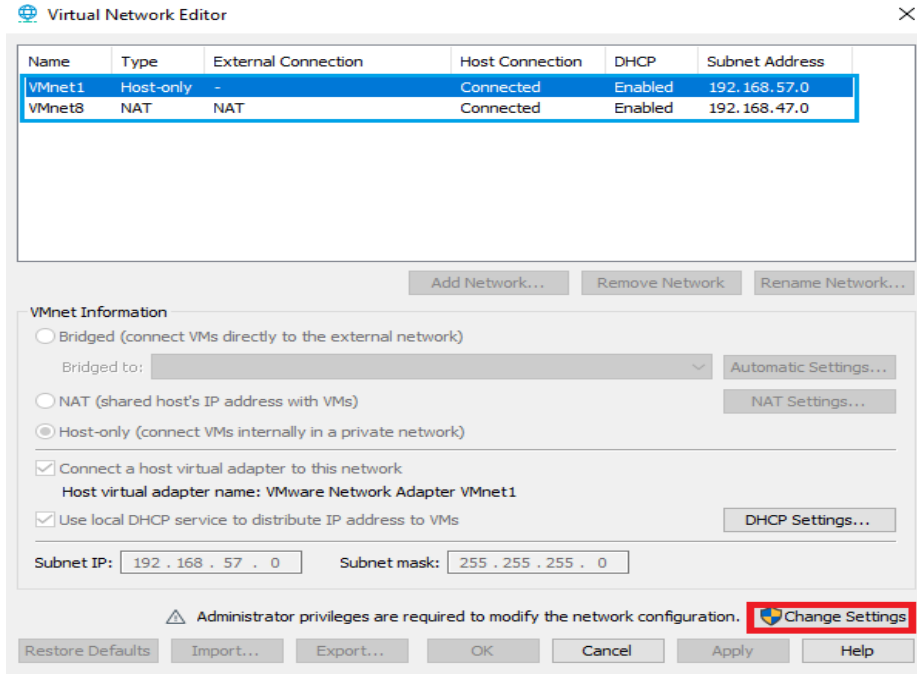
Fortagate Firewall ile ilgili ilk olarak sanallaştırma üzerine çalışma ortamının kurulmasıyla başlayacağım. Bu seriyi takip edenlerin uygulama yapmak için yeterli kaynağı sahip olamayabileceğini düşünerek kısıtlı imkana sahip kişiler için kurulumu VMWare üzerinde gerçekleştirirken aynı zamanda benimde bu süreçte severek kullandığım Eve-ng üzerinde kurulumun nasıl gerçekleştirilebileceğini acıkamaya çalışacağım. VMWare üzerinde kurulum yapabilmek 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 selected, leading to the 'Downloads' section. Under 'Downloads', 'VM Images' is selected, leading to the 'FortiGate for VMWare ESXi platform Version 7.0.13' page. On this page, the 'Download' button is highlighted.

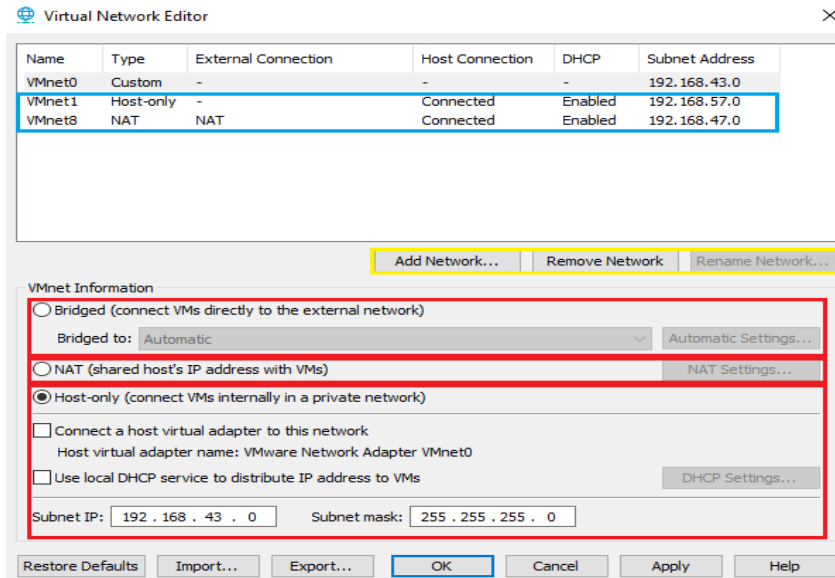
File Information	Checksum	Release Date
Upgrade from previous version of FortiGate for VMWare FW_VM64-v7.0.13.M-build0566-FORTINET.out (81.22 MB)	6754d583b77f32d9d8151a3369ef5f7 (Regular) a4b7f6b417932981fc506915bcb7a346f31d1932de6fbc86a94cbfec8064a3111c8e06059d008621aef5295696f037f172be3e5487f3c98ef4e0ef547a8a21 (SHA-512)	2023-10-26
New deployment of FortiGate for VMWare FW_VM64-v7.0.13.M-build0566-FORTINET.out.ovf.zip (80.94 MB)	4cec6c90e4ef70cb96b5ad5ea5b6d5ea (Regular) 4f1cdd31f1ba59891e1cf6679f3225f5a62e3d79d78cd4fba3d00e2384ed82cea239525e72a67eaa2fc4333c0000f77edf4763b2b6bf6d91ab764db64fa9ef (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 anlaşılağı 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 sanal networkler tanımlanıyor. Varsayılanda iki tane VMNet tanımı geliyor. Virtual Network Editor üzerinde değişiklik yapabilmek için sağ alt köşedeki **Change Setting** seçeneğinin seçilmesi gerekiyor.

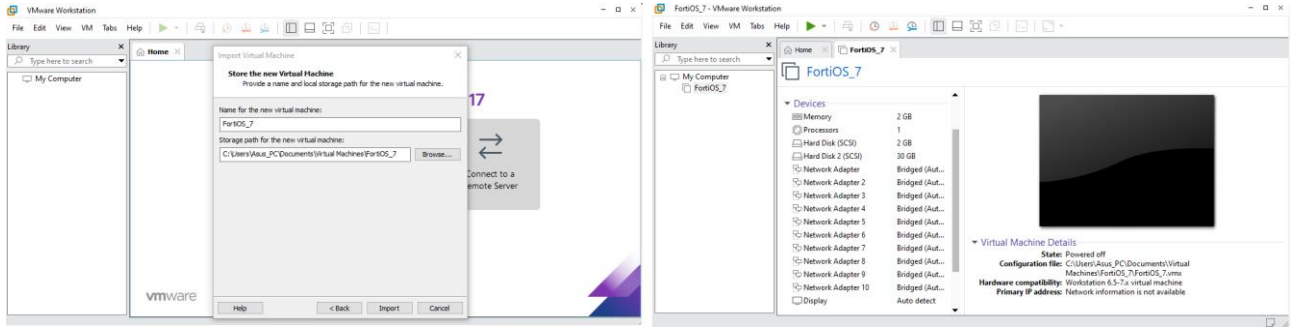


“Change Setting” seçeneği seçildikten sonra “Add Network” seçeneği ile yeni VMNet oluşturulabilir. Varsayılanda gelen veya sonradan oluşturulan herhangi bir VMnet seçildikten sonra (Şimdilik sadece kurulum yapılacağı için VMNet üzerinde herhangi bir ayarlama yapmaya gerek yoktur);

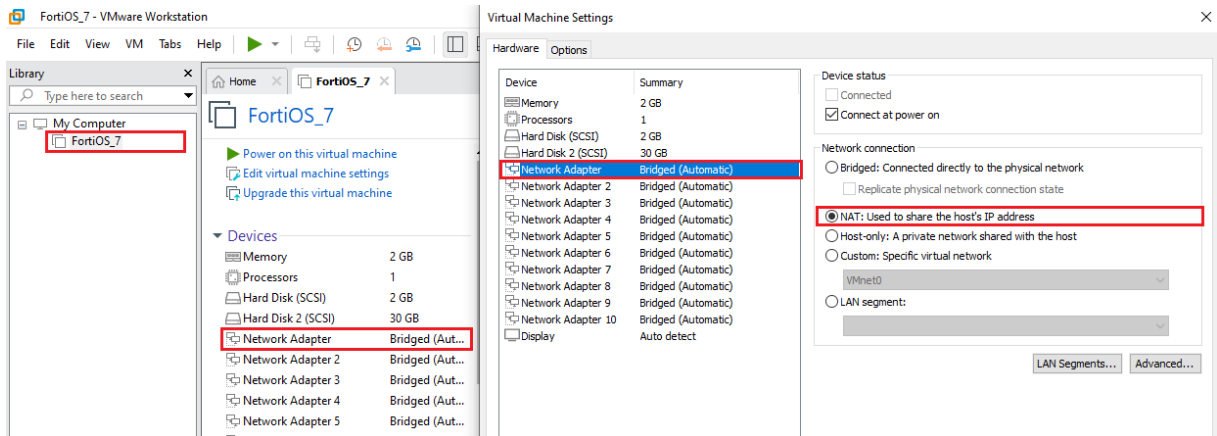
- **Bridge seçeneği**, VM’in doğrudan internete çıkarılması sağlıyor.
- **NAT seçeneği**, VM’in ip adresi NAT’lanarak ana makinenin networküne dahil edilmesini sağlıyor. Ana makina-VM arası bağlantı kurulması sağlanabiliyor.
- **Host-Only seçeneği**, seçilerek sanal makineler arasında kullanılacak sanal/özel bir network tanımı oluşturmak için kullanılıyor (Bu seçimler topolojilere göre değişiklik göstereceği için şimdilik herhangi bir değişiklik yapılmıyor).



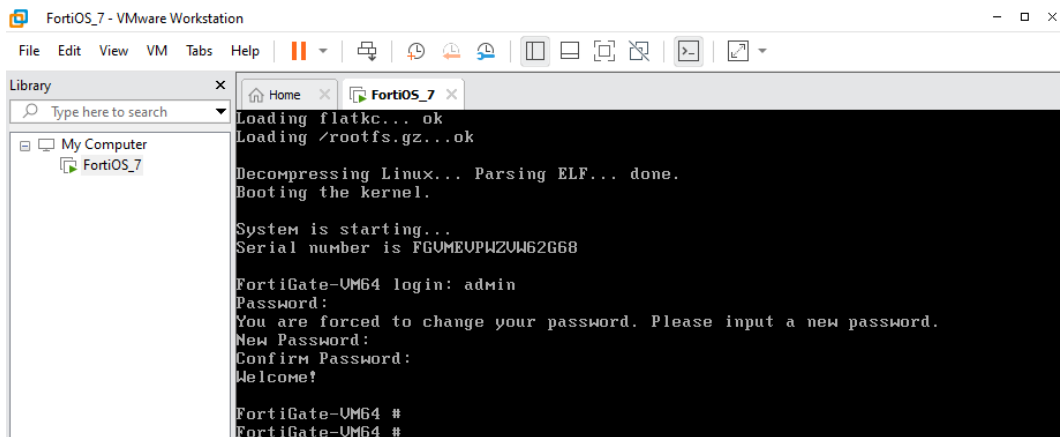
İsteğe yönelik Fortigate VM üzerindeki sanal network ayarlamaları yapıldıktan sonra “Open a Virtual Machine” seçeneğiyle indirilen Fortigate görüntüsü seçilip ve yüklenecek görüntüye isim tanımı yapıldıktan sonra görüntü Import edilmesi gerekiyor.



Fortigate görüntüsü VMWare uygulamasına aktarıldıktan sonra varsayılanda 2 GB RAM 1 CPU, 32 GB hafıza alanı ve 10 sanal port ile gelmektedir (İsteğe/kaynak miktarına bağlı olarak bu değerler yükseltilebilir). 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 (Bu sayede Fortigate FW başlatıldığında 1. port DHCP üzerinden ip alacaktır). 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 bağlanacak sanal makinenin de network ayarlarında aynı VMNet’e dahil edilmesi gerekiyor). Kullanılmayacak arayüzleri kapatmak için **“Coonect at power on”** kısmındaki seçimi kaldırabilirsiniz.



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”**, parola kısmı boş girildikten sonra parola belirleme işlemi için yeni bir parola girilmesini isteyecektir.



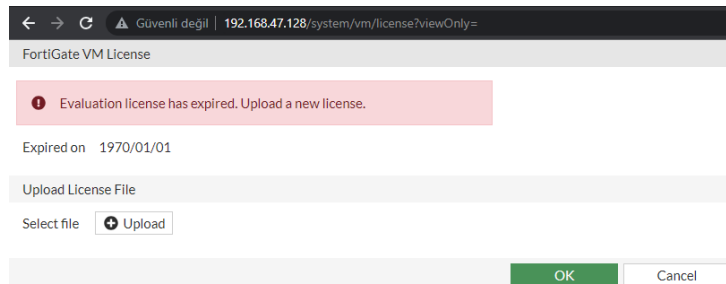
Admin hesabı için yeni parola bilgisi tanımlandıktan sonra arayüzlerin durumunu görüntülemek için “**show system interface**” komutunun sonunda “?” sembolünün girilmesi gerekiyor (Daha fazla komut için [https://help.fortinet.com/fauth/5-3/Content/Admin%20Guides/5\\_3%20Admin%20Guide/200/204\\_CLI\\_commands.htm](https://help.fortinet.com/fauth/5-3/Content/Admin%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 bilgisi aldığı gördükten sonra aşağıdaki komutları çalıştırarak bu port üzerinde izin verilecek protokollerin tanımlanması gerekiyor ki bu porta atanan ip adresi üzerinden fortigate arayüzüne erişebilelim (Tanımlamamalar 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 herhangi bir tarayıcı üzerinden arayüze erişilebilir (Kurulum yaparken tanımladığın kullanıcı adı ve parola bilgisini kullanarak oturum açabilirsin). Giriş yaptıktan sonra lisans süresinin sona ermesiyle ilgili bir hatayla karşılaşabilirsin (kendi sitesi dışında bir kaynaktan indirdiyse muhtemeldir).



The screenshot shows a web browser window with the address bar displaying "192.168.47.128/system/vm/license?viewOnly=". The page title is "FortiGate VM License". A red error message box states: "Evaluation license has expired. Upload a new license." Below this, it shows "Expired on 1970/01/01". There is 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 “**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
```

- Farklı sürümlerde lisanslama süreci değişiklik gösterebilir (Örnek olarak aşağıdaki görselde de görülebileceği gibi Fortinet hesabıyla kimlik doğrulama işlemi gerekebilir).

FortiGate VM License

VM is not licensed or license is invalid for current VM configuration. Upload a new license or reconfigure the VM.

How will you license this VM? ☐ Full License ☒ Evaluation License

This license can only be used once per FortiCare account and has several restrictions:

- Support for low encryption operation only
- Maximum of 1 CPU and 2GiB of memory
- Maximum of three interfaces, firewall policies, and routes each
- No FortiCare Support

[Learn more about the Evaluation VM License](#)

Login to FortiCare to activate VM Trial

Email

Password

Are you a government user? ☐

OK Cancel

Lisans hatasını giderilip Fortigate arayüzüne tekrar giriş yapıldıktan sonra cihaza yeni bir Hostname belirlenmesi ve kullanılmak istenen kontrol panelinin seçilmesi 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.

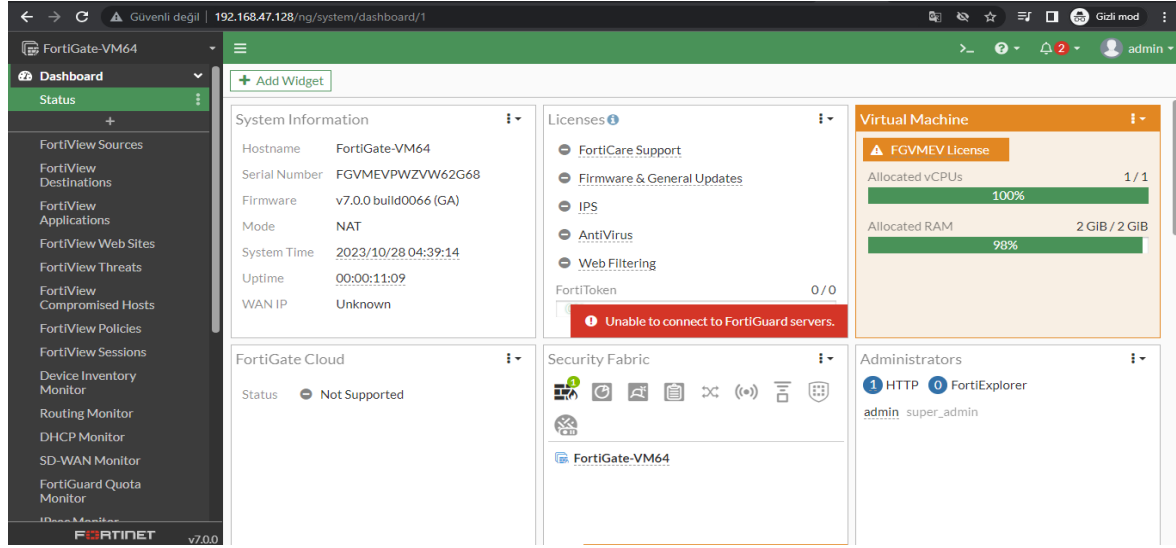
**Comprehensive**

☒ 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 veya doğrudan internet üzerinde “.qcow2” formatlı dosyası indirilerek GNS3 üzerinde kurulumu yapılarak

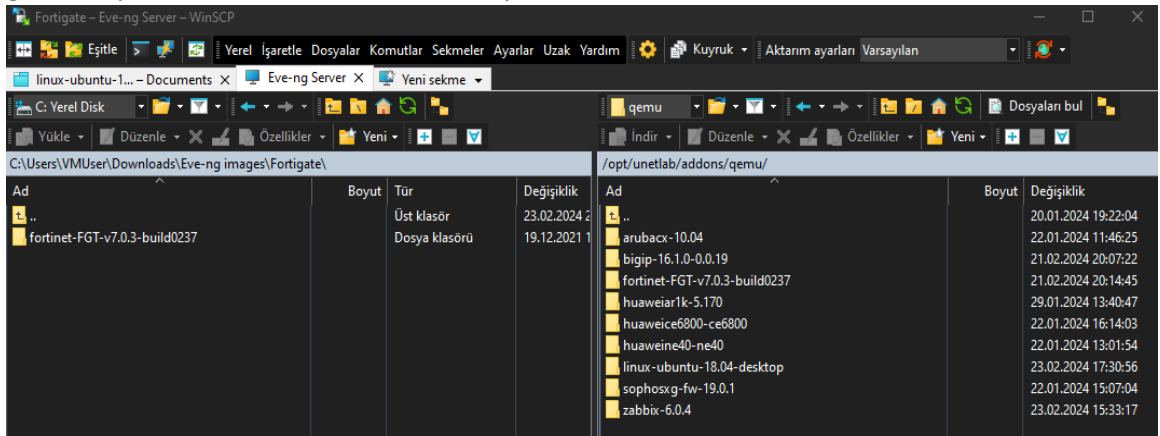
da kullanılmaya başlanabilir). Artık VMWare üzerinde veya GNS3 üzerinde kendi topolojilerimizi oluşturup uygulamalar yapmaya başlayabiliriz.



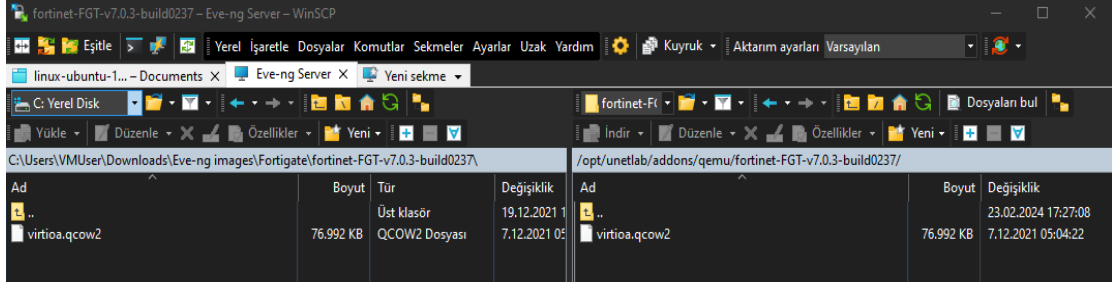
## Eve-ng Üzerinde Fortigate FW Kurulumu

Eve-ng üzerinde Fortigate FW kurulumu için öncelikle kurulum yapacağın ortamı seçilmeli. Seçim sürecinde Eve-ng'nin kendi sitesinde belirttiği uygun olmayan platformları göz önünde bulundurulmalıdır. Ben evde boş duran eski bir leptopta Ubuntu Server Focal Fossa kurup üzerinde Eve-ng yazılımını yükledim (Bare Metal kurulum olarak biliniyor). Kurulum sürecine ve bu süreçte karşılaştığım problemlere Github hesabı üzerinde "**Networking-Works/1- Lab Hazırlığı /Eve-ng Lab Ortam Hazırlığı/**" dizininden ulaşabilirsin. Kurulum adımlarını takip edip tamamladıktan sonra;

- Fortigate FW'un ".qcow2" uzantılı dosyasını bulmalısın (İnternet üzerinde birkaç arama yaparak bulabilirsin). Bulduğun dosya yüksek ihtimalle sıkıştırılmış/arşivlenmiş durumda olacaktır. Sunucuya yüklemeyen önce arşivden çıkarmayı öneririm. Sunucuya yükledikten sonra çıkarmak istersen **Eve-ng Lab Ortam Hazırlığı** notlarından yardım alabilirsin.
- Eve-ng yazılımının çalıştığı cihaza WinSCP, Filezilla gibi herhangi bir FTP yazılımı kullanarak bağlanmalısın.
- Bağlandıktan sonra sunucu cihaz üzerinde **/opt/unetlab/addons/qemu** dizini altına içerisinde Fortigate bulunan bir dizin oluşturmalısın (Fortigate kelimesinden sonra "\_" gibi karakterler kullanmamaya dikkat etmelisin. Aksi takdirde tarayıcı üzerinde görünmeyecektir. "-" sembolü kullanılabilir).



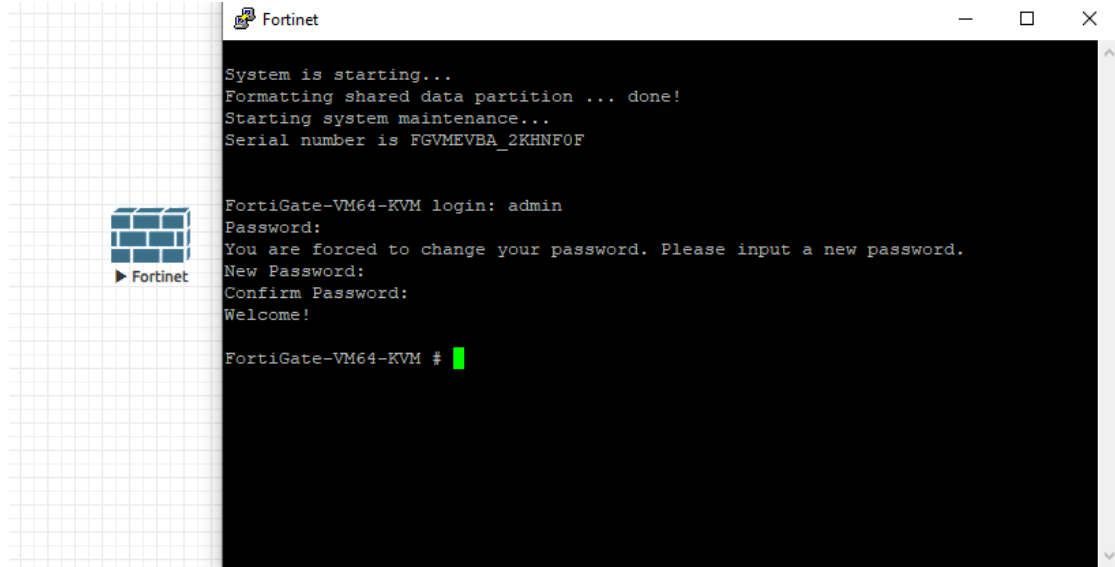
- Oluşturduğun dizin altına indirdiğin “.qcow2” uzantılı Fortigate dosyasını yükleyebilirsin (Dosya adının “hda” veya “virtioa” olmasına dikkat et. Yani dosya adı “hda.qcow2” veya “virtioa.qcow2” olmalı. Bu isimde olmazsa işletim sistemini görmüyor. Bu nedenle farklı bir isme sahipse bunu değiştirmelisin).



- Son olarak Eve-ng yazılımının çalıştığı cihaza SSH üzerinden bağlantı kurularak “/opt/unetlab/wrappers/unl\_wrapper -a fixpermissions” komutunun çalıştırılması gerekiyor.

```
root@eve-ng:~# /opt/unetlab/wrappers/unl_wrapper -a fixpermissions
root@eve-ng:~#
```

Bu adımlar sonrasında artık yeni bir proje oluşturulup Fortigate FW’u keşfetmeye başlayabilirsin.



## 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.