

İlk Konfigürasyon

İlk konfigürasyona arayüzüne bağlanarak başlayacağız. Bu ve bundan sonraki süreçte Eve-ng kullanacağımızdan bahsetmiştim (VMWare kullanıyorsan burada yapacaklarımızı VMWare üzerinde nasıl uygulanacağını araştırmak sana kalıyor).

- Bağlantı için Eve-ng üzerinde yeni bir proje oluşturup proje içerisinde fareye sağ tık yapıp **“Node -> Fortigate”** yolunu izleyerek projeye Fortigate FW’un eklenmesi gerekiyor. Ardından ana bilgisayar üzerinden bağlantı kurabilmek için yine fareye sağ tıklayarak **“Network -> Managment <Cloud0>”** yolu takip edilerek bir network bağlantısı eklenir. Fortigate FW ve Net tanımlı birbirine bağlandıktan sonra Fortigate FW çalıştırılabilir. Çalıştıktan sonra üzerine tıklayarak komut satırına Telnet ile bağlanabilirsin.

EDIT NODE

Template: Fortinet FortiGate

ID: 1

Image: fortinet-FGT-7.0.3-build0237

Name/prefix: Fortinet

Icon: Firewall.png

UUID: 82b2fd00-ac7c-4ea0-b5c7-7ed9822ab944

CPU Limit: ☐

CPU: 1 RAM (MB): 1024 Ethernets: 4

QEMU Version: 4.1.0 QEMU Arch: x86_64 QEMU Nic: virtio-net-pci

QEMU custom options: -machine type=pc,accel=kvm-serial mon:stdio-nographic-no-user-config-nofda

Startup configuration: None

Delay (s): 0

Console: telnet

Left: 669 Top: 295

Save Cancel

EDIT NETWORK

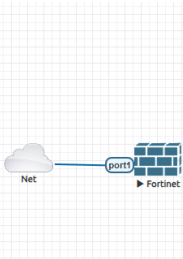
ID: 1

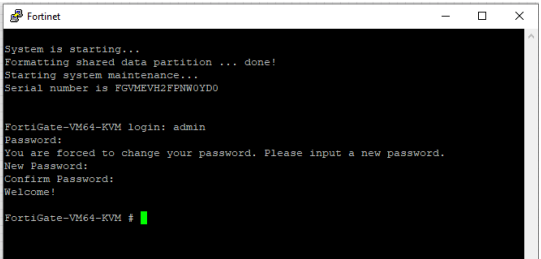
Name/Prefix: Net

Type: Management(Cloud0)

Left: 510 Top: 297

Save Cancel





```
FortiGate-VM64-KVM login: admin
Password:
You are forced to change your password. Please input a new password.
New Password:
Confirm Password:
Welcome!
FortiGate-VM64-KVM #
```

- Komut satırına bağlandıktan sonra kullanıcı adı “admin”, parola kısmını boş bırakarak giriş yapabilirsin. İlk girişte yeni parola tanımlamanı isteyecektir. Parola tanımlandıktan sonra ip alan portun izinlerinin de tanımlanması gerekiyor. Bunun için **“config system interface”**, **“edit port<Port Number>”**, **“set allow-access <Protocols Names>”** komutlarıyla tanımlar yapıldıktan sonra **“end”** komutuyla konfigürasyonu tamamlıyoruz.

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

- Artık web arayüzüne bağlanabiliriz. Bağlanılacak ip adresini öğrenmek için **“show system interface”** komutundan sonra **“?”** simgesi ekleyerek Net bağlantısına bağladığın portun hangi ip adresini aldığını görebilirsin. Tarayıcıdan bu adresi girerek arayüze bağlanabilirsin.

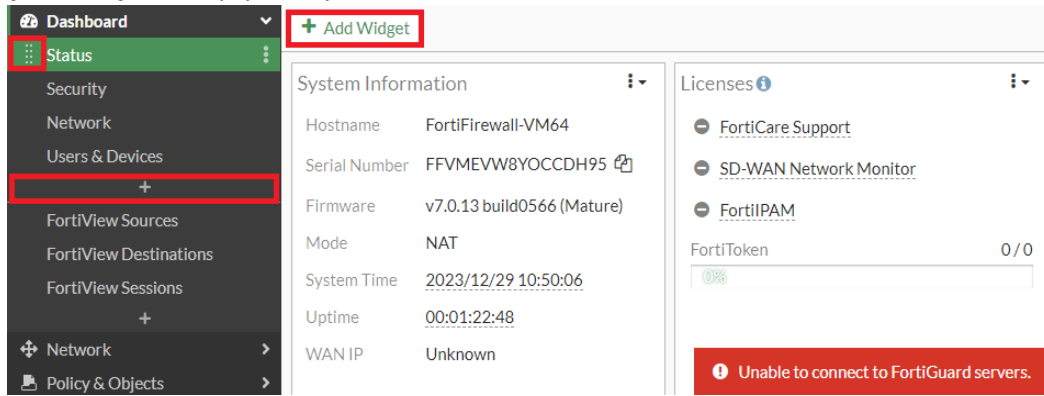
```

FortiGate-VM64-KVM # 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 aggregate enable
l2t.root   static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up   disable tunnel enable
naf.root   static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up   disable tunnel disable
port1      dhcp    0.0.0.0 0.0.0.0 192.168.0.103 255.255.255.0 up   disable physical enable
port2      static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up   disable physical enable
port3      static  0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 up   disable physical enable

```

Fortigate FW'un arayüzüne bağlandıktan sonra artık sol kısımdaki sekmelerden kısaca bahsedebiliriz.

- **Dashboard**, Fortigate cihazın arayüzüne bağlanıp oturum açıldığında kullanıcıyı karşılayan sekmedir (Status sekmesi). Bu sekmede cihazın genel durumu hakkında/istatistiksel bilgiler sağlayan Widget'lar bulunuyor. Mouse ile Widget'ların köşelerinden sürükleyerek yer değişikliği yapılabilirdiği gibi ekleme/çıkarma işlemleriyle özelleştirmeler de yapılabilir. Benzer şekilde Dashboard sekmesi altındaki sekmeler üzerinde de yer değişikliği veya ekleme çıkarma işlemleri yapılabilir

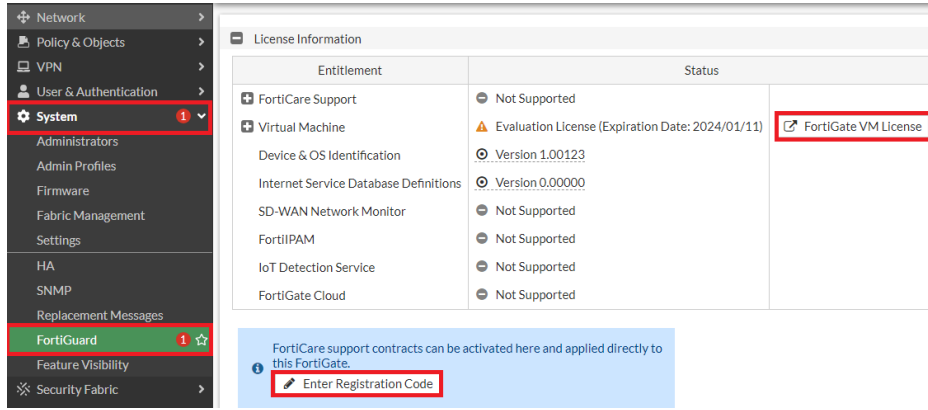


- **Network**, cihaz üzerindeki arayüz konfigürasyonları, yönlendirme işlemleri gibi network tabanlı ayarlamaların yapıldığı sekmedir.
- **Policy & Objects**, trafik şekillendirme, güvenlik duvarı politikalarının tanımlanması gibi işlemlerin gerçekleştirildiği sekmedir.
- **VPN**, IPsec ve SSL VPN ayarlamalarının yapıldığı sekmedir.
- **User & Authentication**, cihaz üzerindeki kullanıcı hesapları üzerinde ayarlamalar yapmak için kullanılan sekmedir. Güvenlik duvarı üzerinde Local kullanıcı oluşturulabildiği gibi Active Directory veya Radius gibi uzak bir kimlik doğrulama sunucusundan da kimlik doğrulama işlemi yapılabilir.
- **System**, genel sistem ayarlarının yapıldığı sekmedir.
- **Security Fabric**, çeşitli network cihazlarıyla bir bütün halde çalışabilmek için ayarlamaların yapıldığı sekmedir. Network üzerindeki FortiGate, FortiAnalyzer, FortiClient, FortiSandbox, FortiAP, FortiSwitch ve FortiClient Enterprise Management Server (EMS) dahil olmak üzere farklı Fortinet ürünlerinin davranışını koordine etmek için kullanılabilir.
- **Log & Report**, VPN, Wifi veya sistem hakkındaki logları ve raporları görüntüleyebilmek için kullanılan sekmedir.

İlk Konfigürasyon

Fortigate güvenlik duvarını kullanılmaya başlamadan önce cihaz üzerinde birkaç ayarlamamanın yapılması gerekiyor. Bu ayarlamalar;

- 1- Fortigate lisansını aktive etmek gerekiyor. Bunun için **System-> Fortiguard** yolu takip edilerek lisans detayları ve desteklenen özellikler görüntülenebilir. Lisans dosyasını yüklemek için **“Fortigate VM License”** kısmı kullanılabileceği gibi **“Enter the License Code”** kısmında verilen lisans numarası girilerek de cihaz lisansı devreye alınabiliyor (Fiziksel cihazlarda arayüze bağlanıp ilk kez oturum açıldığında kayıt işlemleri için bir ekranı çıkıyor. Burada daha önce kayıt olduysanız oturum açabilir, kayıt olmadıysanız yeni kayıt oluşturabilirsiniz).
 - o Normalde bu sayfada lisanslama ile birlikte gelen özelliklerin (Web filtreleme, Antivirüs ve IPS güncellemelerin alınabilmesi gibi daha pek çok özellik) ayarlamaları yapılabiliyor ama deneme sürümünde bu özellikler bulunmadığı için deneme şansımız bulunmuyor.



- 2- Lisanslama işlemi sonlandıktan sonra **System-> Settings** sekmesine gelinerek (komut satırında **“config system global”** ile bu arayüze giriş yapılabilir);
 - **Hostname** alanında, kısmıyla cihaza benzersiz bir isim tanımlanması gerekiyor. Komut satırı üzerinde **“set hostname <Hostname>”** ve **“end”** komutlarıyla cihaz ismi değiştirilebiliyor.

```
FortiGate-VM64-KVM # config system global
FortiGate-VM64-KVM (global) # set hostname FGFW-1
FortiGate-VM64-KVM (global) # end
FGFW-1 #
```

- **System Time** alanında, Time Zone seçimi yapıldıktan sonra zaman bilgisinin güncel tutulması için kullanılacak kaynağın belirtilmesi gerekiyor. Varsayılanda NTP sunucusu olarak FortiGuard üzerinden her 60 saniyede bir senkronize edilecek şekilde geliyor. İsteğe bağlı olarak CLI üzerinde farklı bir NTP tanımı (farklı bir NTP sunucusunun ip adresi) veya PTP tanımı yapılabileceği gibi Manuel olarak da ayarlanabilir (Sistem günlüklerini kayıt altına alma ve raporlama sürecinde zaman damgalarının doğru eklenebilmesi adına önemli bir adımdır).
 - o Saat ve tarih bilgilerini komut satırında manuel olarak ayarlayabilmek için **“execute time <hh:mm:ss>”** ve **“execute date <YYYY-DD-MM>”** komutları kullanılıyor.
 - o Timezone üzerinde saat ve tarih bilgisi belirlemek için **“set timezone <Timezone Number>”** komutu kullanılıyor.

```
FGFW-1 # config system global
FGFW-1 (global) # set timezone 85
FGFW-1 (global) # end
```

- Bir NTP sunucusu üzerinden zaman bilgilerini çekmesi isteniyorsa “**config system ntp**”, “**set type {fortiguard | custom}**”, “**set ntpsync enable**” komutları kullanılarak kullanılacak NTP server tipi belirlenerek NTP üzerinden zaman senkronizasyonunun devreye alınması sağlanıyor. Devamında NTP sunucularının ip adreslerini tanımlamak için “**config ntpserver**”, “**edit <Edit Number>**”, “**set server <NTP Server Ip Address>**” ve “**end**” komutları kullanılıyor (Birden fazla NTP sunucusu tanımlanmak isteniyorsa aşağıdaki görselde de gösterildiği üzere tanımlar arasında “**next**” komutu kullanılıyor).


```
FGFW-1 # config system ntp
FGFW-1 (ntp) # set type custom
FGFW-1 (ntp) # set ntpsync enable
FGFW-1 (ntp) # config ntpserver
FGFW-1 (ntpserver) # edit 1
new entry '1' added
FGFW-1 (1) # set server 192.168.0.200
FGFW-1 (1) # next
FGFW-1 (ntpserver) # edit 2
new entry '2' added
FGFW-1 (2) # set server 192.168.0.201
FGFW-1 (2) # end
FGFW-1 (ntp) # end
FGFW-1 #
```

Host name

System Time	
Current system time	2024/02/24 11:19:10
Time zone	(GMT-3:00) Buenos Aires
Set Time	<input checked="" type="radio"/> NTP <input type="radio"/> PTP <input type="radio"/> Manual settings
Select server	FortiGuard <input checked="" type="radio"/> Custom <input type="text" value="192.168.0.200"/>
Sync interval	<input type="text" value="60"/> Minutes (1 - 1440)
Setup device as local NTP server	<input checked="" type="checkbox"/>
Listen on Interfaces	<div><div>fortilink</div><div>+</div></div>

- **Administrative Settings** alanında, cihaza erişim için kullanılan protokollerin port bilgileri belirleniyor (Güvenlik nedeniyle varsayılanda gelen portların değiştirilmesi faydalı olacaktır). “**Idle Timeout**” seçeneği ile açılan oturumda işlem yapılmadığı takdirde kaç dakikada oturumun sonlanacağı belirleniyor. “**Allow Concurrent Sessions**” seçeneği ile “**admin**” hesabıyla aynı anda birden fazla oturum açılıp açılmayacağı belirleniyor.
 - Kullanılan protokollerin port bilgilerini güncellemek için “**set {admin-ssh-port <Port Number> | set admin-telnet-port <Port Number> | set admin-sport <Port Number>}**” komutları kullanılıyor (Bu konfigürasyonu web arayüzü üzerinde yapılıyorsa HTTP protokolünün portu (“**set admin-port <Port Number>**”) değiştirilirse bağlantınız kopacaktır).
 - Oturumların zaman aşımı üstesini belirlemek için “**set admintimeout <Minute>**” komutu kullanılıyor.

```
FGFW-1 # config system global
FGFW-1 (global) # set admin-ssh-port 456
FGFW-1 (global) # set admin-telnet-port 457
FGFW-1 (global) # set admin-sport 459
FGFW-1 (global) # set admintimeout 30
FGFW-1 (global) # end
```

Administration Settings	
HTTP port	80
HTTPS port	459
HTTPS server certificate	 self-sign
<p>You are using a default built-in certificate, which will not be able to verify your server's domain name (your users will see a warning). Let's Encrypt can be used to easily generate a trusted certificate if you do not have one.</p> <p>Create Certificate</p>	
SSH port	456
Telnet port	457
Idle timeout	30 Minutes (1 - 480)
ACME interface	+
Allow concurrent sessions	<input checked="" type="checkbox"/>
FortiCloud Single Sign-On	<input type="checkbox"/>

- **Password Policy** alanında, admin hesapları ve IPsec sürecinde kimlik doğrulama süreci için belirlenecek parolalara yönelik ayrı ayrı veya her ikisi için de geçerli olacak şekilde politika belirlenebilir.
 - o Kullanılacak parolaları belirlenirken uyulacak politika bilgilerinin hangi mekanizmaya uygulanacağını belirlemek için ilk olarak **“config system password-policy”** altında **“set status {enable | disable}”** komutuyla devreye alınması gerekiyor (aksi takdirde diğer komutlar algılanmıyor/kullanılmıyor). Daha sonra **“set apply-to {admin-password | ipsec-preshared-key}”** komutuyla tanımlanacak politikaların hangi mekanizma için kullanılacağını seçilmesi gerekiyor. kullanılıyor. Artık aşağıdaki görselde de görüleceği üzere bu süreçte uyulması istenen kurallar set edilebiliyor.

```
FGFW-1 # config system password-policy
FGFW-1 (password-policy) # set status enable
FGFW-1 (password-policy) # set apply-to admin-password
FGFW-1 (password-policy) # set
status Enable/disable setting a password policy for locally defined administrator passwords and IPsec VPN pre-shared keys.
apply-to Apply password policy to administrator passwords or IPsec pre-shared keys or both. Separate entries with a space.
minimum-length Minimum password length (8 - 128, default = 8).
min-lower-case-letter Minimum number of lowercase characters in password (0 - 128, default = 0).
min-upper-case-letter Minimum number of uppercase characters in password (0 - 128, default = 0).
min-non-alphanumeric Minimum number of non-alphanumeric characters in password (0 - 128, default = 0).
min-number Minimum number of numeric characters in password (0 - 128, default = 0).
min-change-characters Minimum number of unique characters in new password which do not exist in old password (0 - 128, default = 0. This attribute overrides reuse-password if both are enabled).
expire-status Enable/disable password expiration.
reuse-password Enable/disable reuse of password. If both reuse-password and min-change-characters are enabled, min-change-characters overrides.
FGFW-1 (password-policy) # set minimum-length 10
FGFW-1 (password-policy) # end
```

- **Workflow Management** alanında, cihaz üzerinde yapılan değişikliklerin otomatik olarak kaydedilip istenip istenmediği belirleniyor.
 - o Konfigürasyonların kaydedilme seçeneği **“set cfg-save {automatic | manual | revert}”** komutu kullanılarak gerçekleştirilebilir.

```
FGFW-1 # config system global

FGFW-1 (global) # set cfg-save
automatic    Automatically save config.
manual      Manually save config.
revert       Manually save config and revert the config when timeout.

FGFW-1 (global) # set cfg-save automatic
```

Password Policy

Password scope ⓘ	<input type="button" value="Off"/> <input checked="" type="button" value="Admin"/> <input type="button" value="IPsec"/> <input type="button" value="Both"/>
Minimum length	<input type="text" value="10"/>
Minimum number of new characters	<input type="text" value="0"/>
Character requirements	<input type="checkbox"/>
Allow password reuse	<input checked="" type="checkbox"/>
Password expiration	<input type="checkbox"/>

Workflow Management

Configuration save mode ⓘ	<input checked="" type="button" value="Automatic"/> <input type="button" value="Workspace"/>
---------------------------	--

- **Wiev Settings** alanında, cihazda kullanılacak dil seçimi ve arayüzde kullanılan renklerin/temasının seçimi belirleniyor.
 - Cihaz üzerinde kullanılan dili değiştirmek için “**set language <Language>**” komutu, Web arayüzünde kullanılan tema seçimi için “**set gui-theme <Colour>**” komutu, arayüz üzerinde kullanılan zaman bilgisinin kaynağını belirlemek için “**set gui-date-time-source {system | browser}**” komutu kullanılıyor. Arayüzün daha pek çok niteliği komut satırı üzerinden özelleştirilebiliyor.

```
FGFW-1 # config system global

FGFW-1 (global) # set language english

FGFW-1 (global) # set gui-theme jade

FGFW-1 (global) # set gui-date-time-source system

FGFW-1 (global) # set gui-
gui-allow-default-hostname    Enable/disable the factory default hostname warning on the GUI setup wizard.
gui-certificates              Enable/disable the System > Certificate GUI page, allowing you to add and configure certificates from the GUI.
gui-custom-language           Enable/disable custom languages in GUI.
gui-date-format               Default date format used throughout GUI.
gui-date-time-source          Source from which the FortiGate GUI uses to display date and time entries.
gui-device-latitude           Add the latitude of the location of this FortiGate to position it on the Threat Map.
gui-device-longitude          Add the longitude of the location of this FortiGate to position it on the Threat Map.
gui-display-hostname          Enable/disable displaying the FortiGate's hostname on the GUI login page.
gui-firmware-upgrade-warning  Enable/disable the firmware upgrade warning on the GUI.
gui-forticare-registration-setup-warning  Enable/disable the FortiCare registration setup warning on the GUI.
gui-fortigate-cloud-sandbox   Enable/disable displaying FortiGate Cloud Sandbox on the GUI.
gui-ipv6                      Enable/disable IPv6 settings on the GUI.
gui-local-out                 Enable/disable Local-out traffic on the GUI.
gui-replacement-message-groups  Enable/disable replacement message groups on the GUI.
gui-rest-api-cache            Enable/disable REST API result caching on FortiGate.
gui-theme                    Color scheme for the administration GUI.
gui-wireless-opensecurity     Enable/disable wireless open security option on the GUI.

FGFW-1 (global) # end
```

- Date/Time Display alanında “**FortiGate Timezone**” seçeneği seçildiğinde System Time alanında seçilen ayarlar geçerli olacaktır. “**Browser Timezone**” seçeneği seçildiğinde ise System Time alanında yapılan ayarlamalar geçersiz sayılarak tarayıcı üzerindeki saat ve tarih bilgisi kullanılacaktır.

- Varsayılanda cihazlar daylight özelliğiyle yaz saatine otomatize uyum sağlar ayarlama yapıyor. Yaz saati uygulamasına uymayan ülkeler için bu özellik “**config system global**” ve “**set sdt <Disable | Enable>**” komutuyla devreye alınabiliyor veya devre dışı bırakılabilir.
- Sistem üzerinde NGFW modunu belirlemek için “**config system settings**” altında “**set ngfw-mode {profile-based | policy-based}**” komutu kullanılıyor.

```
FGFW-1 # config system settings
FGFW-1 (settings) # set ngfw-mode profile-based
FGFW-1 (settings) # end
```

- **StartUp Settings** alanında, güç kesintisi durumunda dosya sistemindeki hataların otomatik olarak kontrol edilmesinin istenip istenmediği ayarlanabiliyor. Ek olarak cihaz yeniden başlatıldığında bir USB cihaz üzerinden yazılım güncellemelerinin veya konfigürasyon dosyalarının otomatik olarak yüklenebilmesi için ayarlamalar da yapılabilir.

- Dosya sistemindeki hataların otomatik olarak kontrol edilmesini sağlamak için “**set autorun-log-fsck {enable | disable}**” komutu kullanılıyor.

```
FGFW-1 # config system global
FGFW-1 (global) # set autorun-log-fsck enable
FGFW-1 (global) # end
```

- USB üzerinden yükleme işlemi için öncelikle “**config system auto-install**” altında konfigürasyon dosyasından yüklenmesi için “**set auto-install-config {enable | disable}**” komutunu ve/veya bir image dosyasından başlatılacaksa “**set auto-install-image {enable | disable}**” komutu kullanılarak devreye alınması gerekiyor. Başlatma şekline göre hizmetler devreye alındıktan sonra konfigürasyon dosyasından başlatılacaksa “**set default-config-file <File Name>**” komutuyla, image dosyasından başlatılacaksa “**set default-image-file <File Name>**” komutuyla dosya isimleri tanımlanıyor.

```
FGFW-1 # config system auto-install
FGFW-1 (auto-install) # set auto-install-config enable
FGFW-1 (auto-install) # set auto-install-image enable
FGFW-1 (auto-install) # set default-config-file fgt_system.conf
FGFW-1 (auto-install) # set default-image-file image.out
FGFW-1 (auto-install) # end
```

View Settings

Language English
Theme Jade
Date/Time display FortiGate timezone Browser timezone

NGFW Mode Profile-based Policy-based
Central SNAT

Start Up Settings

Auto file system check
USB auto-install
Detect configuration fgt_system.conf
Detect firmware image.out

- **Email Service** alanında, yöneticileri/kullanıcıları mail hizmetini kullanarak cihaz üzerindeki olaylar hakkında bilgilendirilmesini sağlamak için ayarlamaların yapıldığı alandır. Cihaz üzerinde bir problem yaşanması durumunda hızlı tepki verebilmek adına önemli olacaktır. Bu hizmet varsayılanda devre dışında gelmektedir.

- o Konfigürasyonu için “**config system email-server**” komutu altında “**set type custom**” komutu kullanılarak başlanır. Ardından “**set security {none | smtp | starttls}**” komutuyla kullanılacak mail protokolü seçilmelidir. Bağlantıda kullanılabilecek en düşük protokol sürümünü belirlemek için “**set ssl-min-proto-version {default | SSL3 | TLS1}**” komutu kullanılabilir. Bu tanımlamalardan sonra “**set server <Mail Server Name>**” ve “**set reply-to <Destination Mail Address>**” komutlarıyla kullanılacak mail sunucusunu ve mail gönderilecek adres bilgileri tanımlanır. Son adımda “**set source-ip <Source Ip Address>**” ve “**set port <SMTP Port Number>**” komutlarıyla mail gönderilecek kaynak ip adresi ve SMTP sunucusunun port bilgileri tanımlanır (İsteğe bağlı olarak konfigürasyon süreci kimlik denetimini devreye almak gibi daha da özelleştirilebilir).

```
FGFW-1 # config system email-server
FGFW-1 (email-server) # set type custom
FGFW-1 (email-server) # set security starttls
port is set to default 25.
FGFW-1 (email-server) # set ssl-min-proto-version default
FGFW-1 (email-server) # set server "smtp.mailservername.com"
FGFW-1 (email-server) # set reply-to "deneme@fortinet.com"
FGFW-1 (email-server) # set source-ip 192.168.0.103
FGFW-1 (email-server) # set port 587
FGFW-1 (email-server) # end
```

- o Konfigürasyon burada tamamlanmıyor. Alarm oluşması durumunda gönderilecek mail bilgileri tanımlandı ama gönderilecek alarmlara dair tanımlamaların yapılması da gerekiyor. Bunun için şimdilik buradaki bağlantıyı inceleyebilirsin. İlerleyen süreçte uygulaması ayrıca yapılacaktır (<https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/526019/email->

- **Debug Logs** alanında, cihaz üzerinde sorun giderme sürecine yardımcı olacak hata ayıklama kayıtları indirilebilir.
- **Disk Settings** alanında, Fortigate üzerinde sabit diske sahipse bunu Local Log kayıtlarını tutmak için ya da WAN Optimizasyonu için kullanılabilir. Her iki hizmet de çalışmak için disk alanına ihtiyaç duyuyor ama aynı anda ikisi de devreye alınamıyor. Bu kısımda disk alanının hangi hizmet için kullanılacağı belirleniyor.

Yedekleme ve Yedekten Dönme

- İsteğe bağlı olarak yedekler şifreli şekilde alınabiliyor. Şifreli yedekleme alındığında yedekten geri dönebilmek için şifrenin unutulmaması gerekiyor.
- Yedekten dönmek için ise yine aynı yol üzerindeki “**Restore**” seçeneği kullanılıyor. Bu secenekten sonra yedek alınan dosya seçilir ve cihaz yeniden başlatılır.

The screenshot shows the FortiGate web interface. At the top, there's a green header bar with navigation icons and a user profile 'admin'. Below the header, a sidebar menu on the left contains options like 'Backup', 'Restore', 'Revisions', and 'Scripts'. The 'Backup' option is selected, leading to the 'Backup System Configuration' page. This page has a sub-header 'Backup System Configuration' and two main sections. The first section, 'Backup to', has a toggle for 'Local PC' (which is active) and 'USB Disk'. The second section, 'Encryption', has a toggle that is turned 'On'. Below these are two input fields for 'Password' and 'Confirm password', both of which are currently empty.

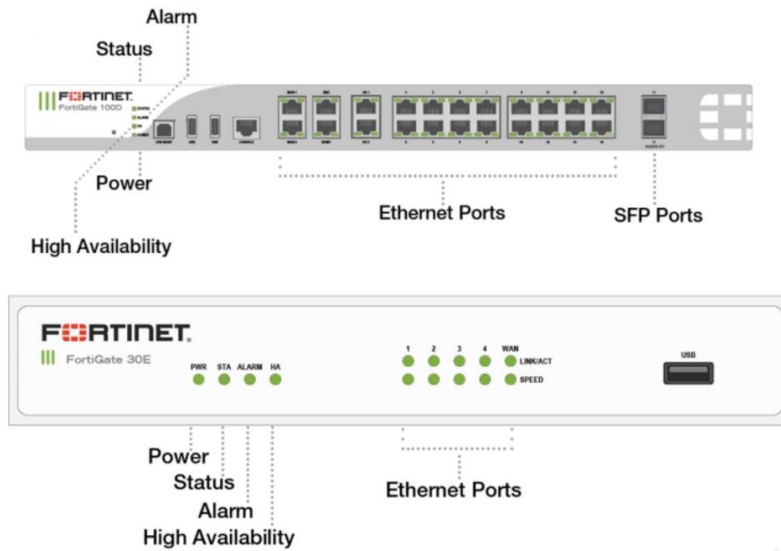
Cihaz Üzerindeki Ledlerin Özellikleri

Sahada cihazların durumu hakkında genel bir fikir sahibi olabilmek konusunda cihaz üzerinde bulunan ledler faydalı olabiliyor. Ledleri cihazın genel durumu hakkında bilgilendirmek üzere kullanılan ledler ve portların durumu hakkında bilgilendiren ledler olarak iki başlık altında inceleyebiliriz. Cihazın genel durumu hakkında bilgi veren birkaç ledin anlamlarına bakıldığında;

- Power Led
 - o Yeşil yanıyorsa, cihazın açık olduğunu gösterir.
 - o Yanmıyorsa, cihazın kapalı olduğunu gösterir.
- Status Led
 - o Yeşil, sorunsuz çalıştığını gösterir.
 - o Yeşil (yanıp/sönen), cihazda önyükleme olduğunu gösteriyor.
 - o Turuncu cihazın doğru çalışmadığını, bir hata oluştuğunu gösterir,
 - o Kırmızı, cihazın doğru çalışmadığını, kritik bir alarm olduğunu gösterir.
- Alarm Led
 - o Kapalı cihazda alarmlık bir durum olmadığını gösterir.
 - o Sarı (Koyu), cihazın büyük bir alarm olduğunu gösterir
 - o Kırmızı, cihazın kritik bir alarmı olduğunu gösterir
- High Availability Led
 - o Yeşil, HA kmesinde çalıştığını gösterir
 - o Turuncu/Kırmızı, yük devretme durumunun oluştuğunu gösterir.
 - o Kapalı, HA yapısının yapılandırılmadığını gösterir.
- PoE Led
 - o Yeşil, PoE cihazının bağlı olduğunu ve güç aldığını gösterir.
 - o Turuncu, bir sorun oluştuğunu gösterir.
 - o Kapalı, PoE cihazının bağlı olmadığını veya güç almadığını gösterir.
- Power Supply Led
 - o Yeşil, güç sağlayıcının sağlıklı bir şekilde çalıştığını gösterir.
 - o Yeşil (yanıp/sönen), güç sağlayıcısının algılandığı ama güç sağlamadığını (bekleme moduna alındığını) gösterir.
 - o Turuncu, güç kaynağı hatası olduğunu veya giriş gücünün olmadığını ancak yedek beslemenin açık olduğunu gösterir.
 - o Turuncu (yanıp/sönen), güç kaynağı hatası olduğunu ve güç kaynağının değiştirilmesi gerektiğini gösterir.
 - o Kırmızı, gücün kesildiğini gösterir.
 - o Kırmızı (yanıp/sönen), güç sağlayıcısının uyarı verdiğini gösterir.
 - o Kapalı, güç sağlayıcısının tespit edilmediğini gösterir.
- Fan Led
 - o Yeşil, fanların normal çalıştığını gösterir.
 - o Turuncu, problem olduğunu gösterir.
 - o Turuncu (yanıp/sönen), fan değiştirme/başlatma işleminin devam ettiğini gösterir.
 - o Kırmızı, dönme hızlarının (RPM) çok yüksek veya çok düşük olduğunu gösterebileceği gibi fan setlerinin en az bir hataya sahip olduklarını gösterir.
 - o Kırmızı (yanıp/sönen), bir fan setinde en az bir uyarı olduğunu gösterir.
 - o Kapalı, fanların kapalı olduğunu veya hata oluştuğunu gösterir.

Cihaz üzerindeki portlar hakkında bilgi veren birkaç ledin anlamlarına bakıldığında;

- Ethernet Led
 - o Yeşil, 1Gbps hızında çalıştığını gösterir (Her renk için yanıp sönüyor olması çalıştığı bant genişliğinde veri iletimi yaptığını gösteriyor).
 - o Turuncu, 10/100Mbps hızında çalıştığını gösterir.
 - o Kapalı, bağlantı olmadığını gösterir.
- SFP Led
 - o Yeşil, 1Gbps hızında çalıştığını gösterir (Her renk için yanıp sönüyor olması çalıştığı bant genişliğinde veri iletimi yaptığını gösteriyor).
 - o Kapalı, bağlantı olmadığını gösterir.
- PoE Led
 - o Yeşil, PoE cihazının sorunsuz şekilde güç aldığını gösterir.
 - o Kırmızı, PoE cihazının bağlı olduğunu ancak güç sağlayamadığını gösterir.
 - o Kapalı, PoE gücünün kapalı olduğunu veya güç alacak bağlı cihazın olmadığını gösterir.



Detaylı bilgi ve daha fazlası için Fortigate'in kendi sitesini ziyaret edebilirsiniz
(<https://docs.fortinet.com/document/fortigate/7.4.1/administration-guide/997251/leds>).

NOTLAR:

- PTP (Precision Time Protocol)
- System sekmesi altındaki ayarlamaları CLI ekranından yapılmak istendiğinde komutlar **"config system global"** komutu altında uygulanıyor.
- Kullanılabilecek birkaç faydalı link
 - o <https://www.fortiguard.com/webfilter> - bir web sitesinin kategorisini öğrenmek için kullanılabiliyor.
 - o <https://www.fortiguard.com/encyclopedia> - zararlı yazılımlarla ilgili bilgiler bulunuyor.
 - o <https://www.fortiguard.com/appcontrol> - uygulamaların kategorisini öğrenmek için kullanılabiliyor.

- Komut satırı üzerinde “**get <Options>**” kalıbı kullanılarak uygulanan konfigürasyonlara dair bilgiler/servislerin durumlarına dair bilgiler görüntülenebiliyor.

Kontrol Komutları

- get system status
- get system email-server

Kaynaklar

- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/837328/changing-the-host-name>
- <https://docs.fortinet.com/document/fortigate/6.4.0/hardening-your-fortigate/948443/set-system-time-by-synchronizing-with-an-ntp-server>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/84878/checking-the-system-date-and-time>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/512210/setting-the-system-time>
- <https://docs.fortinet.com/document/fortigate/6.4.2/administration-guide/616955/configuring-ports>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/364729/password-policy#:~:text=To%20create%20a%20system%20password,Click%20Apply.>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Configuration-file-save-mode-for-configuration/ta-p/194054#:~:text=Configuration%20file%20save%20mode%20is,configuration%20if%20there%20are%20problems.>
- <https://docs.fortinet.com/document/fortigate/6.4.10/administration-guide/316105/changing-the-view-settings>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Automatic-installation-of-Firmware-and-system/ta-p/197938>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Firmware-Upgrade-and-Configuration-Restore-using-a/ta-p/197057>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-configure-alert-email-settings/ta-p/194102>
- <https://docs.fortinet.com/document/forticlient/7.2.3/ems-administration-guide/385506/configuring-smtp-server-settings>