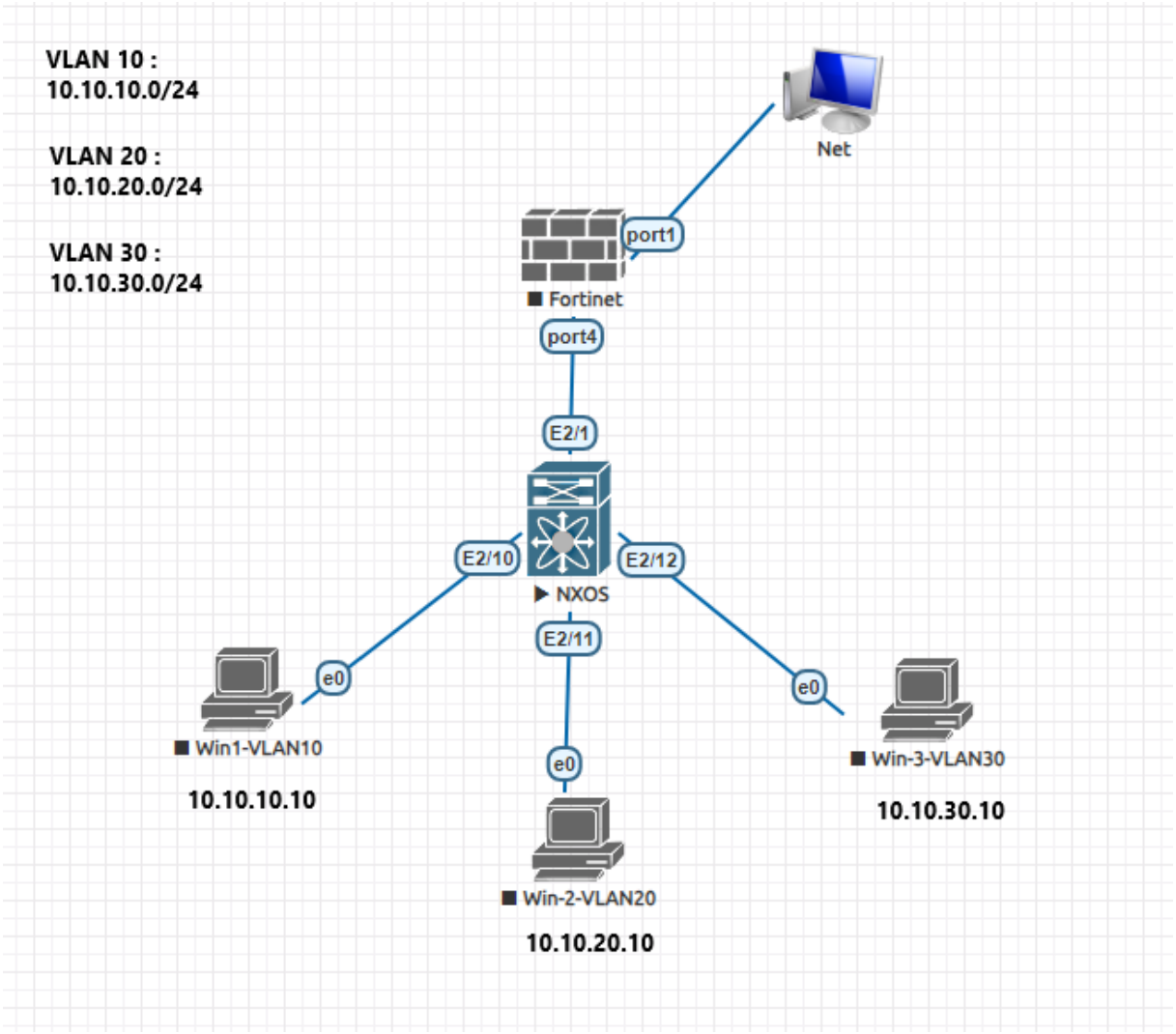
Trusted Host

Günümüzde ilk kurulum için Fortigate'lerin yönetim arayüzüne cihaz üzerinde yönetim arayüzüne erişim için konumlandırılmış Management portlarından bağlanılıyor. Management portun arayüzünde, varsayılanda 192.168.1.99 ip adresi atanmış ve bu porta bağlanacak istemcinin sorunsuzca ip alıp bağlanabilmesi için DHCP servisi açık bırakılmıştır. Her ne kadar Fortigate'in yönetim arayüzüne erişimi kolaylaştırıyor olsa da bu durum aynı zamanda bir güvenlik problemi oluşturmaktadır. Önlem olarak bu portta DHCP hizmeti kapatılıp varsayılanda gelen ip bloğu değiştirilebiliyor.

Fortigate üzerindeki Management portu üzerinden gerçekleştirilen bağlantılar için bu portun arayüzünde DHCP hizmetini devre dışı bırakıp kullanılan ip bloğunu değiştirmek belirli bir seviyede güvenlik sağlasa da farklı portlar/VLAN'lar veya uzak bağlantılar üzerinden de Fortigate'in yönetim arayüzüne bağlanmak gerekebiliyor. Bu durumda hangi networklerden gelen kullanıcıların Fortigate'in yönetim arayüzüne bağlanabileceğini belirlemek ve bunu özelleştirebilmek için Trusted Host özelliği kullanılıyor. Bu yazıda Trusted Host özelliğinin nasıl çalıştığı ve nasıl devreye alındığı açıklanmaya çalışılacaktır. Bu süreçte aşağıdaki topoloji üzerinden ilerlenecektir.



Topolojide; VLAN 10 FW ile ilgilenmesi gereken kullanıcıların bulunduğu, VLAN 20 yöneticilerin bulunduğu VLAN'dır. Bu durumda VLAN 10'daki bütün kullanıcıların, VLAN 20'deki 10.10.20.10/32 ip adresine sahip yöneticinin (IT Manager) yönetim arayüzüne erişebilmesi isteniyor. Bu süreçte Management portu üzerinden erişilebilirliğin kaybedilmesi de istenmiyor.

Lab çalışmasına switch üzerinde VLAN tanımları yapıldıktan sonra istemci portlarına ilgili VLAN atamalarını yaparak başlanabilir. Cisco switch ve FW arasındaki bağlantının yapıldığı port Trunk moduna alınması yeterlidir. Cisco switchlerde Trunk moduna alınan portlar varsayılanda tüm VLAN'ları geçirecektir.

```
CiscoSW(config)# vlan 10
CiscoSW(config-vlan)# name FW_MGMT_VLAN
CiscoSW(config-vlan)# exit
CiscoSW(config)# vlan 20
CiscoSW(config-vlan)# name YT_VLAN
CiscoSW(config-vlan)# exit
CiscoSW(config)# vlan 30
CiscoSW(config-vlan)# name Finance_VLAN
CiscoSW(config-vlan)# exit
CiscoSW(config)# int ethernet 2/1
CiscoSW(config-if)# switchport
CiscoSW(config-if)# switchport mode trunk
CiscoSW(config-if)# exit
```

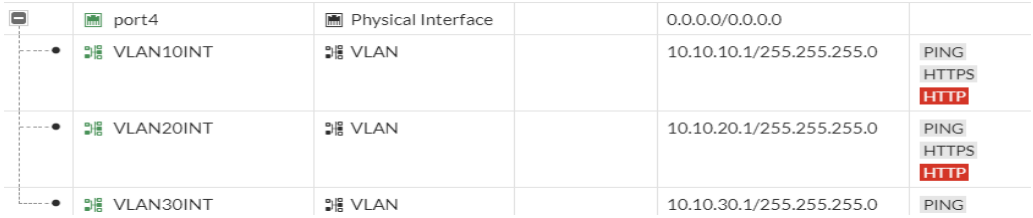
```
CiscoSW(config)# int ethernet 2/10
CiscoSW(config-if)# switchport
CiscoSW(config-if)# switchport mode access
CiscoSW(config-if)# switchport access vlan 10
CiscoSW(config-if)# no shutdown
CiscoSW(config-if)# exit
CiscoSW(config)# int ethernet 2/11
CiscoSW(config-if)# switchport
CiscoSW(config-if)# switchport mode access
CiscoSW(config-if)# switchport access vlan 20
CiscoSW(config-if)# no shutdown
CiscoSW(config-if)# exit
CiscoSW(config)# int ethernet 2/12
CiscoSW(config-if)# switchport
CiscoSW(config-if)# switchport mode access
CiscoSW(config-if)# switchport access vlan 30
CiscoSW(config-if)# no shutdown
CiscoSW(config-if)# exit
```

Switch portları ayarlandıktan sonra artık Fortigate üzerindeki konfigürasyonlara geçilebilir. Fortigate üzerinde arayüz tanımları oluşturulurken Fortigate'in yönetim arayüzüne bağlanılabilmesi için ilgili Interface tanımı altında "**set allowaccess http https**" komutuyla Fortigate'in yönetim arayüzüne erişimin izin verilmesi gerekiyor.

```
Fortigate # config system interface

Fortigate (interface) # edit VLAN10INT
new entry 'VLAN10INT' added

Fortigate (VLAN10INT) # set vdom root

Fortigate (VLAN10INT) # set interface port4

Fortigate (VLAN10INT) # set type vlan

Fortigate (VLAN10INT) # set vlanid 10

Fortigate (VLAN10INT) # set mode static

Fortigate (VLAN10INT) # set ip 10.10.10.1 255.255.255.0

Fortigate (VLAN10INT) # set allowaccess ping http https

Fortigate (VLAN10INT) # next
```

```
Fortigate (interface) # edit VLAN20INT
new entry 'VLAN20INT' added

Fortigate (VLAN20INT) # set vdom root

Fortigate (VLAN20INT) # set interface port4

Fortigate (VLAN20INT) # set type vlan

Fortigate (VLAN20INT) # set vlanid 20

Fortigate (VLAN20INT) # set mode static

Fortigate (VLAN20INT) # set ip 10.10.20.1 255.255.255.0

Fortigate (VLAN20INT) # set allowaccess ping http https

Fortigate (VLAN20INT) # next
```

```
Fortigate (interface) # edit VLAN30INT
new entry 'VLAN30INT' added

Fortigate (VLAN30INT) # set vdom root

Fortigate (VLAN30INT) # set interface port4

Fortigate (VLAN30INT) # set type vlan

Fortigate (VLAN30INT) # set vlanid 30

Fortigate (VLAN30INT) # set mode static

Fortigate (VLAN30INT) # set ip 10.10.30.1 255.255.255.0

Fortigate (VLAN30INT) # set allowaccess ping

Fortigate (VLAN30INT) # end
```



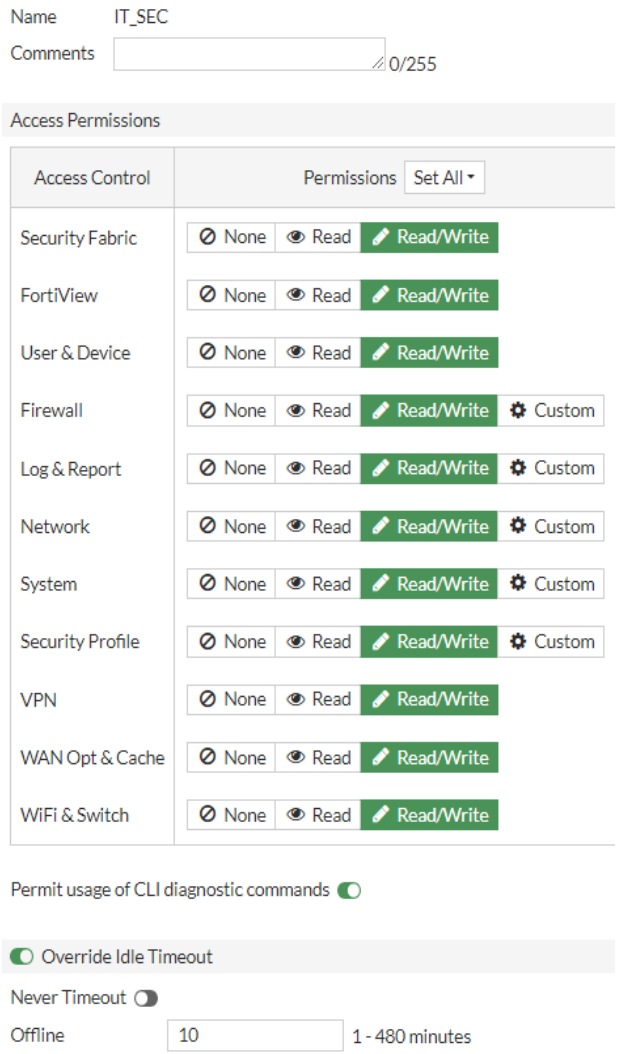
Fortigate üzerinde arayüz tanımları yapıldıktan sonra artık VLAN10 ve VLAN20'ye bağlı istemcilerin tamamı Fortigate'in yönetim arayüzüne erişebilir duruma gelecektir. Burada sadece 10.10.20.10/32 ip adresine sahip istencinin yönetim arayüzüne erişebilmesi için "**System –> Administrators**" yolu takip edilerek Trusted Host tanımı yapılması gerekiyor.

Trusted Host tanımında **Administrator**, **REST API Admin** ve **SSO Admin** olmak üzere uygulanabilecek 3 seçenek bulunuyor. Bu seçeneklerin neler olduğunu bakıldığında;

- **Administrator**, **Fortigate üzerinde cihaz yönetimini sağlamak üzere kullanıcı hesapları oluşturup bu kullanıcıların yönetimini sağlamak için kullanılan seçenektir**. Bu hesaplar üzerinde izin seviyeleri tanımlanarak erişim kontrolleri sınırlandırılabiliyor. Konfigürasyonu için;
    - İlk adımda kullanıcı oluşturulmadan önce kullanıcıya verilecek izin kapsamını belirlemek için "**System –> Admin Profile**" yolu takip edilerek Admin Profile tanımı oluşturulması gerekiyor. İsteğe bağlı olarak ilgili kullanıcının bazı sekmeler altında erişilebileceği kısımlar özelleştirilebiliyor.

```
Fortigate # config system accprofile

Fortigate (accprofile) # edit IT_SEC
new entry 'IT_SEC' added

Fortigate (IT_SEC) # set
comments                Comment.
secfabgrp               Security Fabric.
ftviewgrp               FortiView.
authgrp                 Administrator access to Users and Devices.
sysgrp                  System Configuration.
netgrp                  Network Configuration.
loggrp                  Administrator access to Logging and Reporting including viewing log messages.
fwgrp                   Administrator access to the Firewall configuration.
vpngrp                  Administrator access to IPsec, SSL, PPTP, and L2TP VPN.
utmgrp                  Administrator access to Security Profiles.
wanoptgrp               Administrator access to WAN Opt & Cache.
wifi                    Administrator access to the WiFi controller and Switch controller.
admintimeout-override   Enable/disable overriding the global administrator idle timeout.
system-diagnostics      Enable/disable permission to run system diagnostic commands.

Fortigate (IT_SEC) # set secfabgrp
none          No access.
read          Read access.
read-write    Read/write access.
```

```
Fortigate # config system accprofile

Fortigate (accprofile) # edit IT_SEC

Fortigate (IT_SEC) # set secfabgrp read-write

Fortigate (IT_SEC) # set ftviewgrp read-write

Fortigate (IT_SEC) # set authgrp read-write

Fortigate (IT_SEC) # set sysgrp read-write

Fortigate (IT_SEC) # set netgrp read-write

Fortigate (IT_SEC) # set loggrp read-write

Fortigate (IT_SEC) # set fwgrp read-write

Fortigate (IT_SEC) # set vpngrp read-write

Fortigate (IT_SEC) # set utmgrp read-write

Fortigate (IT_SEC) # set wanoptgrp read-write

Fortigate (IT_SEC) # set wifi read-write

Fortigate (IT_SEC) # set admintimeout-override enable

Fortigate (IT_SEC) # set system-diagnostics enable

Fortigate (IT_SEC) # end
```

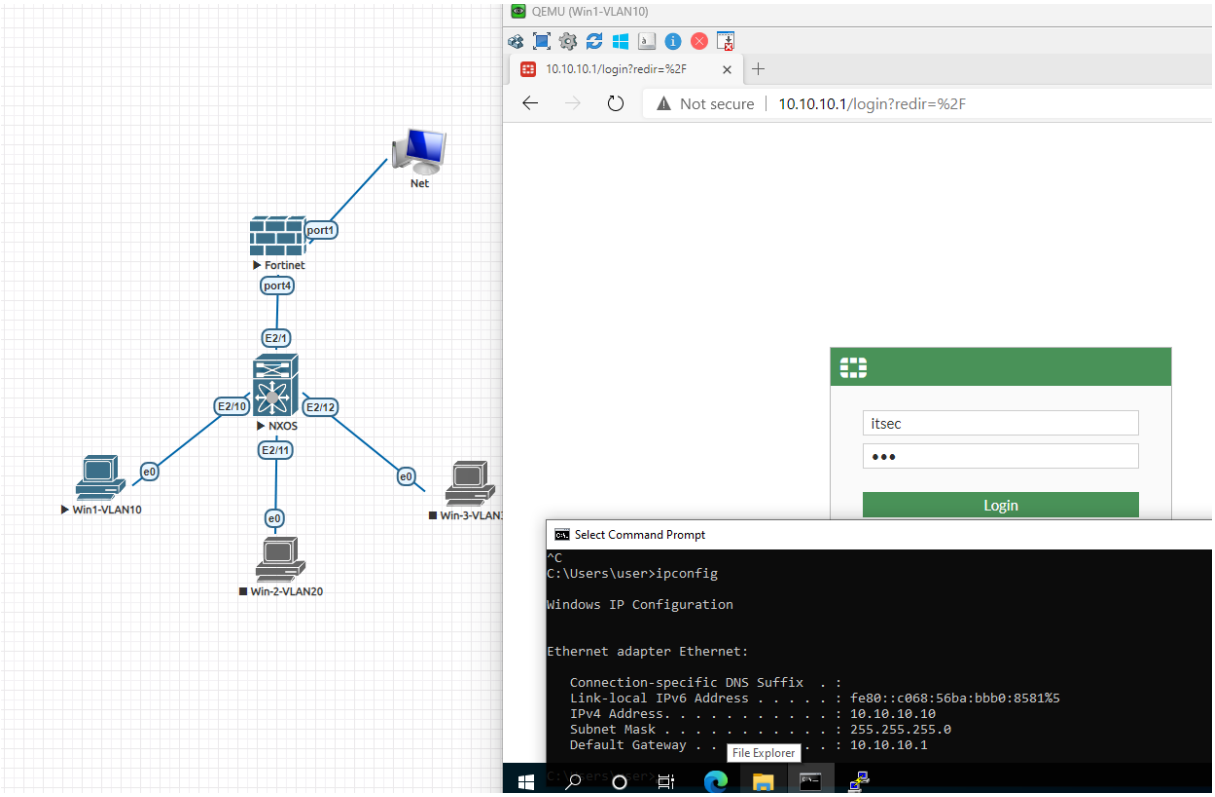


- Oluşturulacak kullanıcıya tanımlanacak Admin Profile tanımı hazırlandıktan sonra "**System -> Administrator -> Create New -> Administrator**" yolu izlenerek kullanıcı hesabı p-oluşturulmaya başlanabilir. Burada kullanıcının cihaz üzerinde mi oluşturulacağı yoksa harici bir kimlik denetimi sunucusundan (LDAP, RADIUS,TACACS…) mı çekileceği belirtilmelidir (Uzak kimlik denetimi sunucularına erişimin kesilmesi ihtimaline karşın cihaz üzerinde bir kullanıcı tanımlanması daha sağlıklı olacaktır). Lab ortamında imkanlar dahilinde kullanıcı cihaz üzerinde oluşturulacaktır. Cihaz üzerinde kullanıcı oluşturmak için temel anlamda kullanıcı adı ve parola tanımıyla oluşturulan Administrator Profile tanımının yapılması yeterli oluyor. İsteğe bağlı olarak burada;
  - İsteğe bağlı olarak oluşturulan kullanıcıya bir TOKEN bağlanarak oturumlarda 2FA kullanılması sağlanabiliyor.
  - İsteğe bağlı olarak admin hesaplarının yalnızca misafir hesapları oluşturabilmesini sağlanabiliyor.
  - İsteğe bağlı olarak **Trusted Host** kısmı devreye alınarak sadece belirli ip adreslerine sahip istemcilerin bu kullanıcı bilgileriyle oturum açabilmesi sağlanabiliyor. Biz VLAN 10'un tamamını ve VLAN 20'deki 10.10.20.10/32 adresine izin vereceğiz.

```
Fortigate # config system admin

Fortigate (admin) # edit itsec
new entry 'itsec' added

Fortigate (itsec) # set password eve

Fortigate (itsec) # set accprofile IT_SEC

Fortigate (itsec) # set trusthost1 10.10.10.0/24

Fortigate (itsec) # set trusthost2 10.10.20.10/32

Fortigate (itsec) # end
```

Name	Trusted Hosts	Profile	Type	Two-factor Authentication
System Administrator 2				
admin		super_admin	Local	Disabled
itsec	10.10.10.0/24 10.10.20.10/32	IT_SEC	Local	Disabled

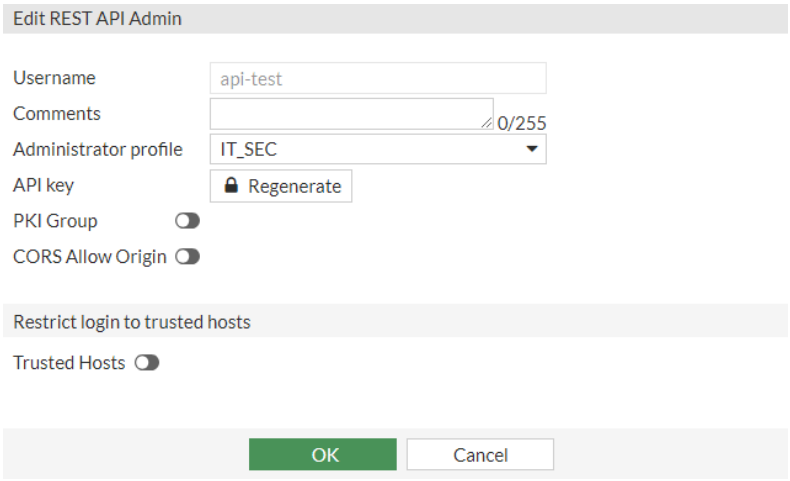
Konfigürasyon sonrasında VLAN 10 üzerinden ve VLAN 20'ye 10.10.20.10/32 ip adresinden bağlanan kullanıcı oluşturulan kullanıcı bilgileriyle arayüze erişim sağlayarak oturum açabilir duruma gelecektir (burada 10.10.20.10/32 ip adresini VLAN 20 arayüzü altında DHCP servisini açıp IT MANAGER'a Bind etmeyi unutma. Aksi takdirde bu ip adresini alan istemci Fortigate'in yönetim arayüzüne erişebilir).



|→ **"Administrators" sekmesi altında tanımlı kullanıcılardan hepsinde Trusted Host özelliği devreye alındığı durumda Trusted Host olarak belirtilmeyen kaynak ip adreslerine sahip istemcilerin kullanıcı adı ve parola bilgisini kullanması bir yana, İlgili arayüz üzerinde HTTP ve HTTPS protokollerine izin verilse dahi Fortigate'in Web arayüzüne erişim sağlanamayacaktır. Bu nedenle Trusted host tanımlarına Management portu için kullanılan network adresi eklenmezse Managament portundan dahi cihazın yönetim arayüzüne erişim sağlanamayacaktır.**

- **REST API Admin**, Fortigate'in yönetimini ve yapılandırmasını otomatikleştirmek için kullanılıyor. Bu özellik Fortigate'in farklı yazılımlar ve araçlar ile birlikte çalışabilmesine imkân veriyor. Konfigürasyonu için;
    - İlk adımda Administrators tanımında olduğu gibi entegre çalışılacak API'nin Foritgate üzerindeki yetki kapsamını belirlemek adına verilecek izin kapsamını belirlemek için "**System –> Admin Profile**" yolu takip edilerek Admin Profile tanımı oluşturulması gerekiyor.
    - Admin Profile tanımı yapıldıktan sonra "**System -> Administrator -> Create New -> REST API Admin**" yolu izlenerek burada kullanım amacına yönelik bir isim ve Admin Profile tanımı yapılması yeterli oluyor. Bu tanımlar yapıldıktan sonra oluşturulan REST API Admin tanımı kullanılarak bir API Key oluşturulur ve Fortigate ile birlikte çalışması istenen yazılıma uygulanır.
        - İsteğe bağlı olarak **PKI (Public Key Infrastructure) Group**, **Trusted Host** veya **CORS Allow Origin** özellikleri devreye alınabilir.
        - ***PKI Group****, Public Key Infrastructure (PKI) yani Kamu Anahtar Altyapısı ile ilgili işlemleri yönetmek için kullanılan bir grup yapılandırmasıdır. PKI, dijital sertifikaların oluşturulması, dağıtılması ve yönetimi için bir çerçeve sağlar ve güvenli iletişim, kimlik doğrulama gibi amaçlarla kullanılır.*
        - ***CORS Allow Origin****, Cross-Origin Resource Sharing (CORS) politikalarının bir parçasıdır ve web uygulamalarının bir alan adı üzerinden kaynakları (örneğin, API istekleri) başka bir alan adından yüklemesine izin verir. Bu özellik, web tabanlı uygulamalar ve REST API'ler arasında güvenli veri paylaşımını sağlamak için önemlidir. Örnek Senaryo olarak bir web uygulamanız var ve bu uygulama Fortigate API'sini kullanıyorsa, CORS Allow Origin ayarını doğru bir şekilde yapılandırmanız gerekir. Örneğin, uygulamanızın barındırıldığı alan adı https[:]//myapp.com ise, bu alan adını CORS ayarlarına eklemelisiniz.*

```
Fortigate # config system api-user

Fortigate (api-user) # edit api-test
new entry 'api-test' added

Fortigate (api-test) # set accprofile IT_SEC

Fortigate (api-test) # set vdom root

Fortigate (api-test) # end

Fortigate # execute api-user generate-key api-test

New API key: 84QG49d4Ht35k0yr4NqQhcmhkGpr00

NOTE: The bearer of this API key will be granted all access privileges assigned
to the api-user api-test.
```



- **SSO Admin**,

Kaynak

- https[:]//help.fortinet.com/fadc/4-4-0/cli/Content/FortiADC/cli-ref/config_system_admin.htm
- https[:]//docs.fortinet.com/document/fortigate/7.6.0/administration-guide/399023/rest-api-administrator
- https[:]//community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-create-a-REST-API-Admin-user-and-assign-it/ta-p/247199
- https[:]//www.youtube.com/watch?v=oZshavqa4aE
- https[:]//www.youtube.com/watch?v=rhrFS0997JU
- https[:]//www.beyaz.net/tr/guvenlik/makaleler/fortinet_fsso_kurulumu.html