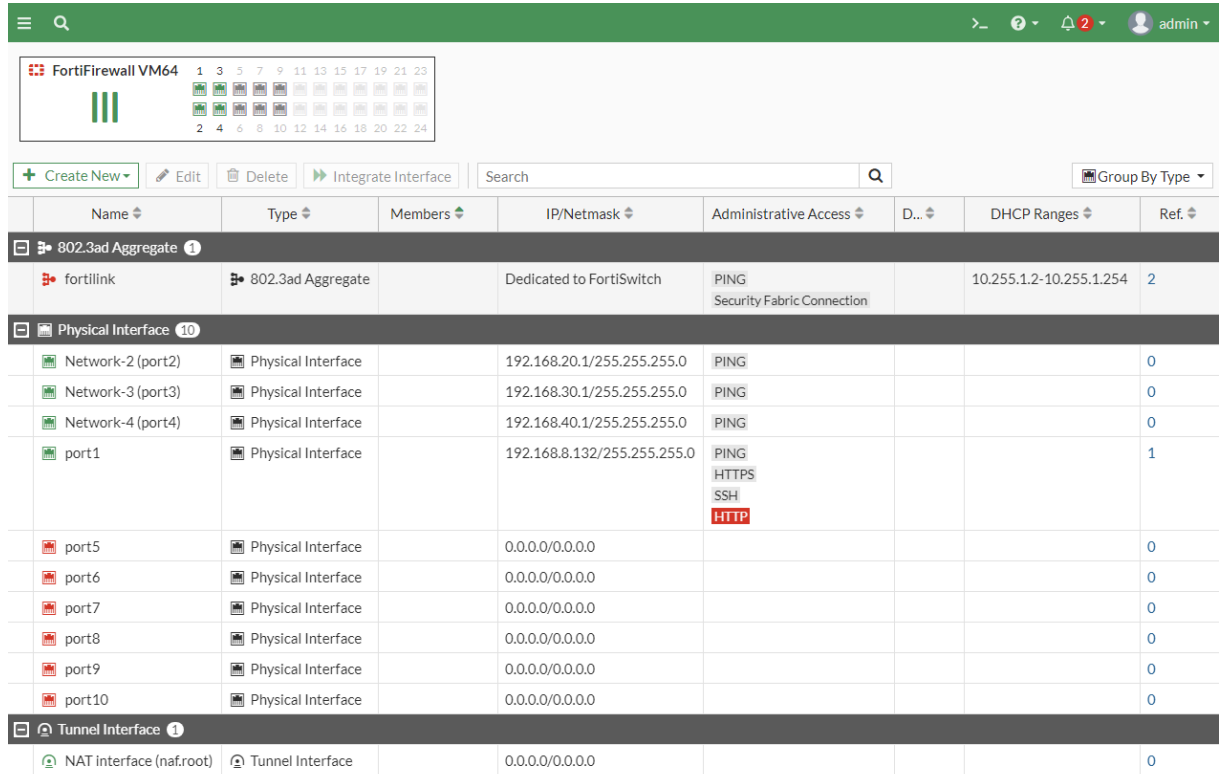


Interfaces - 1

Interface sekmesinde kullanıcıyı cihaz üzerindeki fiziksel portların bulunduğu bir tablo karşılıyor. Tablonun sütun kısmına sağ tık yapıp portlar hakkında tabloda görüntülenmesi istenen özellikler seçilerek sütunlar eklenmesi sağlanabiliyor.

Tablo üzerindeki satırlara tıklanarak ilgili port üzerinde düzenlemeler yapılabiliyor. Web arayüzü üzerinden yapılabilecek konfigürasyonlar kısıtlıdır. Bu nedenle web arayüzünün desteklemediği özelliklerin ayarlamaları CLI üzerinden yapılmaktadır.







Name	Type	Members	IP/Netmask	Administrative Access	D...	DHCP Ranges	Ref.
802.3ad Aggregate 1							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
Physical Interface 10							
Network-2 (port2)	Physical Interface		192.168.20.1/255.255.255.0	PING			0
Network-3 (port3)	Physical Interface		192.168.30.1/255.255.255.0	PING			0
Network-4 (port4)	Physical Interface		192.168.40.1/255.255.255.0	PING			0
port1	Physical Interface		192.168.8.132/255.255.255.0	PING HTTPS SSH HTTP			1
port5	Physical Interface		0.0.0.0/0.0.0.0				0
port6	Physical Interface		0.0.0.0/0.0.0.0				0
port7	Physical Interface		0.0.0.0/0.0.0.0				0
port8	Physical Interface		0.0.0.0/0.0.0.0				0
port9	Physical Interface		0.0.0.0/0.0.0.0				0
port10	Physical Interface		0.0.0.0/0.0.0.0				0
Tunnel Interface 1							
NAT Interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

Listelenen portların arayüzlerine giriş yapılarak fiziksel portlara uygulanabilecek konfigürasyonlara bakıldığında;

- **Alias**, kısmıyla porta takma ad belirlemek için kullanılıyor.
 - o Herhangi bir portun arayüzü altında “**set alias <Alias>**” komutuyla ayarlanıyor.
- **VRF ID** (virtual routing/forwarding), öncelikle VRF teknolojisinin nasıl çalıştığına bakıldığında **CCNP - ENCORE/CCNP - 04 - IP Routing Essentials /IP Routing Essentials.pdf** notlarında da bahsedildiği gibi fiziksel bir router üzerinde birden fazla yönlendirme tablosu oluşturulmasına (bir tür sanal routerlar oluşturmak anlamına geliyor) imkan veren bir teknolojiydi. Bu sayede tek bir router kullanılarak (aynı ip bloğunu kullanılsa dahi) birden fazla kurumun trafiği birbirinden izole şekilde yönlendirilebiliyordu. Fortinet cihazında ise varsayılanda VRF etkin gelmektedir (Tüm portlar VRF 0’da). Bu alanı özelleştirmek için ise 0-31 arasında bir VRF ID değeri belirlemek gerekiyor. Bu değer belirlendikten sonra bu portla aynı yönlendirme tablosunu kullanacak portların da aynı VRF ID değerine dahil edilmesi gerekiyor.
 - o Herhangi bir portun arayüzü altında “**set vrf <VRF-ID>**” komutuyla set edilebiliyor.

- **Role**, cihazın üzerindeki fiziksel portların kullanım şeklini belirlemek için kullanılıyor. Burada seçilen role göre arayüz üzerinde desteklenen özelliklerin arayüz üzerinde görünmesi sağlanıyor (LAN, WAN, DMZ). Herhangi bir rol seçilmediği durumda varsayılanda LAN rolü için desteklenen bütün özellikler listelenmektedir.
 - o **LAN**, iç networke (LAN) bağlanmak için kullanılan roldür. Yeni arayüzler için varsayılanda gelen roldür.
 - o **WAN**, internete bağlanmak için kullanılan roldür.
 - o **DMZ**, DMZ'ye bağlanmak için kullanılan roldür.
 - o Herhangi bir portun arayüzü altında “**set role <Role>**” komutuyla role seçimi yapılabiliyor.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set alias Port2Alias
FortiGate-VM64-KVM (port2) # set vrf
vrf      Enter an integer value from <0> to <31>.
FortiGate-VM64-KVM (port2) # set vrf 0
FortiGate-VM64-KVM (port2) # set role
lan      Connected to local network of endpoints.
wan      Connected to Internet.
dmz      Connected to server zone.
undefined Interface has no specific role.
FortiGate-VM64-KVM (port2) # set role lan
FortiGate-VM64-KVM (port2) # end
```

Name	 Port2Alias (port2)
Alias	<input type="text" value="Port2Alias"/>
Type	 Physical Interface
VRF ID 	<input type="text" value="0"/>
Role 	<input type="text" value="LAN"/>

- **Addressing Mode**, cihaz arayüzüne ip adresi tanımlamak için kullanılan alandır. Dört farklı şekilde ip adresi tanımlanabiliyor. Bu seçeneklere bakıldığında;
 - o **Manual**, kullanıcının manuel olarak ip bilgilerini tanımladığı seçenektir. Komut satırından ip adresi atamak için ilgili portun arayüzüne giriş yapılarak “**set ip <Ip Address> <Subnet Mask>**” komutu kullanılmalıdır.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set ip 192.168.20.1 255.255.255.0
FortiGate-VM64-KVM (port2) # end
```

- **Create Address Object Matching Subnet**, arayüz üzerinde atanan ip adresi ile subnet bilgisinin eşlenmesini sağlayan özelliktir. Bu özellik sayesinde arayüze atanan ip adresi güncellendiğinde, subnet bilgisini de bu doğrultuda otomatik olarak güncellenerek subnete uygulanan politikaların herhangi bir konfigürasyona ihtiyaç duyulmadan uygulanmaya devam edilmesini sağlıyor.
 - Herhangi bir port arayüzü altında ip adresi tanımlandıktan sonra “**config firewall address**”, “**edit port<Port Id>**”, “**set type interface-subnet**” ve “**set interface port<Port Id>**” komutları kullanılarak oluşturulan subnetin bir arayüze bağlanmsı sağlanıyor. Varsayılanda ip bilgisi otomatik olarak arayüze atanan ip adresiyle oluşturuluyor ama isteğe bağlı olarak burada “**set subnet <Ip Address> <Subnet Mask>**” komutuyla ayrıca ip bilgisi de belirtilebiliyor.

```

FortiGate-VM64-KVM # config firewall address

FortiGate-VM64-KVM (address) # edit port2
new entry 'port2' added

FortiGate-VM64-KVM (port2) # set type interface-subnet

FortiGate-VM64-KVM (port2) # set interface port2

FortiGate-VM64-KVM (port2) # next

FortiGate-VM64-KVM (address) # end

```

- **Secondary Ip Address**, fiziksel porta üzerinde kullanılabilecek ikinci bir ip adresi tanımlamak için kullanılıyor. Bu özellik kullanılarak aynı anda iki farklı networke hizmet verebiliyor. Farklı bir kullanım örneği olarak tek bir arayüz üzerinde farklı ip adreslerine ihtiyaç duyan hizmetler devreye alınmak istenebilir (Bu özellik için ön şart arayüze kendi ip adresi atanmasıdır).
- Konfigürasyonu için ilgili portun altına giriş yapılarak “**set secondary-IP {Enable | Disable}**” komutuyla ikinci ip adres tanımlama devreye alındıktan sonra “**config secondaryip**” komutuyla ikinci ip adresi tanımlama arayüzüne giriş yapılıyor. Burada “**edit port1**”, “**set ip <Ip Address> <Subnet Mask>**” ve “**next**” komutlarıyla birden fazla sanal port oluşturularak ip adresleri tanımlanabiliyor.

```

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set secondary-IP
enable      Enable secondary IP.
disable     Disable secondary IP.

FortiGate-VM64-KVM (port2) # set secondary-IP enable

FortiGate-VM64-KVM (port2) # config secondaryip

FortiGate-VM64-KVM (secondaryip) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set ip 192.168.30.1 255.255.255.0

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (secondaryip) # edit 2
new entry '2' added

FortiGate-VM64-KVM (2) # set ip 192.168.40.1 255.255.255.0

FortiGate-VM64-KVM (2) # next

FortiGate-VM64-KVM (secondaryip) # end

FortiGate-VM64-KVM (port2) # end


```

Address

Addressing mode Manual DHCP Auto-managed by IPAM One-Arm Sniffer

IP/Netmask

Create address object matching subnet ☒

Name  port2

Destination 192.168.20.1/255.255.255.0

Secondary IP address ☒

+ Create New

Edit

Delete

Search

Q

IP/Netmask	Administrative access
192.168.30.1/255.255.255.0	
192.168.40.1/255.255.255.0	

2

- **DHCP**, arayüzün bağlı olduğu network üzerindeki bir DHCP sunucusundan ip bilgilerini aldığı seçenektir.
 - **Retrieve default gateway from server Distance**, ADSL hatlar üzerinden internete çıkabilmek için PPPoE özelliğiyle birlikte bu özelliğin de devrede olması gerekiyor. Detaylı bilgi ve örnek için <https://www.bilisimasistani.com/fortigate-adsl-hatlar-icin-trafik-yonlendirme/> adresini ziyaret edebilirsiniz.
 - **Override internal DNS**, DHCP sunucusundan ip bilgileriyle DNS sunucusunun bilgisi de alınacaktır. Bu özellik devreye alındığında DHCP sunucusundan öğrenilen DNS sunucusunun yanı sıra Fortigate üzerindeki DNS sekmesinde ayarlanan DNS bilgisinin de kullanılmasını sağlayacaktır.
 - ilgili arayüz altına giriş yapılarak “**set dns-server-override {enable | disable}**” komutuyla bu özellik devreye alınabiliyor.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set dns-server-override
enable      Use DNS acquired by DHCP or PPPoE.
disable     No not use DNS acquired by DHCP or PPPoE.
FortiGate-VM64-KVM (port2) # set dns-server-override enable
FortiGate-VM64-KVM (port2) # end
```

Address	
Addressing mode	Manual DHCP Auto-managed by IPAM One-Arm Sniffer
Retrieve default gateway from server	<input checked="" type="checkbox"/>
Distance	<input type="text" value="5"/>
Override internal DNS	<input checked="" type="checkbox"/>
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	<input type="text" value="port2"/>
Destination	<input type="text" value="192.168.20.1/255.255.255.0"/>

- **Auto-Managed by IPAM**, Fortigate üzerinde varsayılanda mevcut olan bir özelliktir. Devreye alındığında **IPAM** isimli sunucusundan (ayrıca belirtilmediği sürece 172.31.0.1/24 ile ip dağıtmaya başlanıyor) otomatik ip/network bilgisi atanmaktadır. Ip adres tanımı otomatik olarak verilse de subnet bilgisi isteğe bağlı olarak değiştirilebiliyor.
 - IPAM konfigürasyonu için “**config system ipam**” ve “**set status {enable | disable}**” komutlarıyla IPAM sunucusunun devreye alınması gerekiyor. Burada isteğe bağlı olarak “**set pool-subnet <class IP and netmask>**” komutuyla A veya B sınıfı ip adresleri tanımlanabiliyor. Devreye alındıktan sonra IPAM sunucusundan ip adresi alması istenen arayüze giriş yapılarak “**set ip-managed-by-fortiipam {enable | disable}**” komutunun kullanılması gerekiyor.

```
FortiGate-VM64-KVM # config system ipam
FortiGate-VM64-KVM (ipam) # set status enable
FortiGate-VM64-KVM (ipam) # end
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set ip-managed-by-fortiipam enable
The IP address for this interface will be cleared.
A new address will be automatically set once it has been allocated by FortiIPAM.
Do you want to continue? (y/n)y
```

Address	
Addressing mode	Manual DHCP Auto-managed by IPAM One-Arm Sniffer
IP/Netmask ⓘ	172.31.1.1/255.255.255.0
Network size	256 (255.255.255.0)
Create address object matching subnet	<input checked="" type="checkbox"/>
Name	port2
Destination	172.31.1.1/255.255.255.0

- **One-Arm Siffer**, port üzerinde uygulanabilecek güvenlik özellikleridir. Bu özellikler ayarlanarak porta gelen trafiğin kontrol edilmesi ve tanımlanan güvenlik politikalarına göre değerlendirilmesi sağlanıyor. Konfigürasyonu ve uygulamaları **Interfaces – 2 – One Arm Sniffer** isimli yazıda detaylıca açıklanmaktadır.
- **IPv4**, arayüze erişim izni verilecek protokollerin belirlendiği alandır. Bu alan için cihazın yönetim arayüzüne bağlanılırken kullanılan port üzerinde https, ssh ve ping paketlerine izin verilmesi yeterli olurken diğer portlarda ihtiyaç duyulmadığı sürece bu paketlere izin verilmemesi gerekiyor (Özellikle WAN bacağında açılmaması gerekiyor).
 - o CLI ekranında ilgili arayüz altına girildikten sonra **“set allowaccess <Protocol Names>”** komutuyla izinler tanımlanabiliyor.
 - o Bu kısımdan izin veirlmediği sürece port üzerinde tanımlı ip adreslerine Ping dahi atılmadığını unutma. Konfigürasyonlarda dikkatinden kaçabilir.

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit port2
FortiGate-VM64-KVM (port2) # set allowaccess
ping          PING access.
https         HTTPS access.
ssh           SSH access.
snmp          SNMP access.
http          HTTP access.
telnet        TELNET access.
fgfm          FortiManager access.
radius-acct   RADIUS accounting access.
probe-response Probe access.
fabric        Security Fabric access.
ftm           FTM access.
speed-test    Speed test access.

FortiGate-VM64-KVM (port2) # set allowaccess ping ssh http https
FortiGate-VM64-KVM (port2) # end
```

- **Received LLDP and Transmit LLDP (Link Layer Discovery Protocol)**, network üzerindeki cihazları keşfetmek için kullanılan protokoldür (Cisco marka cihazlardaki CDP protokolü gibi). Bu özellik aktif edilerek LLDP mesajların alınıp gönderilmesi sağlanabiliyor. Bu özellik Global, Interface ve VDOM olmak üzere üç farklı şekilde devreye alınabilir. CLI üzerinde;
 - o Global bazda devreye alınmak istendiğinde **“config system global”** arayüzü altında, VDOM bazında devreye alınmak istendiğinde **“config system setting”** arayüzü altında **“set lldp-reception {enable | disable}”** ve **“set lldp-transmission {enable | disable}”** komutları kullanılıyor.
 - o Interface bazında devreye alınmak istendiğinde **“config system interface”, “edit <Port Number>”, “set lldp-reception {enable | disable}”** ve **“set lldp-transmission {enable | disable}”** komutları kullanılıyor.

```

FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set lldp-reception enable

FortiGate-VM64-KVM (port2) # set lldp-transmission enable

FortiGate-VM64-KVM (port2) # end

```

Administrative Access

IPv4	<input checked="" type="checkbox"/> HTTPS	<input checked="" type="checkbox"/> HTTP	<input checked="" type="checkbox"/> PING
	<input type="checkbox"/> FMG-Access	<input checked="" type="checkbox"/> SSH	<input type="checkbox"/> SNMP
	<input type="checkbox"/> FTM	<input type="checkbox"/> RADIUS Accounting	<input type="checkbox"/> Security Fabric Connection ⓘ
	<input type="checkbox"/> Speed Test		
Receive LLDP ⓘ	Use VDOM Setting	Enable	Disable
Transmit LLDP ⓘ	Use VDOM Setting	Enable	Disable

- **DHCP Server**, arayüzün bağlı olduğu networke DHCP sunuculuğu yapmasını sağlayan özelliktir. DHCP konfigürasyonu için ilk olarak **Address Range** kısmıyla bir ip havuzunun başlangıç ve bitiş adresi ve network maskesi tanımlanmalıdır. **Default Gateway** kısmı için istemcilere Fortigate arayüzüne tanımlanan ip adresi verilebileceği gibi (**Same as Interface IP**) farklı bir ip adresi de (**Specify**) tanımlanabiliyor. Benzer şekilde **DNS Server** kısmıyla istemcilere verilecek DNS bilgisinin arayüz üzerinde tanımlı ip adresi verilebilir, sistem üzerinde tanımlı DNS bilgisiyle aynı ip bilgisi verilebilir veya farklı bir ip bilgisi de tanımlanabiliyor. **“Lease Time”** kısmıyla istemcilere ip adresinin ne kadar süreyle kiralanacağı belirleniyor. Son olarak **DHCP Status** durumu **Enable** seçilerek DHCP sunucusu devreye alınmalıdır. Burada **“+”** kısmıyla tek bir arayüz üzerinde birden fazla ip havuzu veya birden fazla DNS Server bilgisinin tanımlanabileceği de unutulmamalıdır.
 - o DHCP sunucusunun ilk adımda devreye alınmama nedeni, DHCP sunucusuna yönelik ayarlamalar tamamlanmadan devreye alınırsa ve bu süreçte bir istemci DHCP sunucusunda ip bilgisi talep ederse istemciye eksik bilgilerin sunulacak olmasıdır (örnek olarak DNS bilgisi ayarlanmadığı için istemci DNS Server ip adresi alamayacaktır).
 - o DHCP konfigürasyonu için **“config system dhcp server”** arayüzü altında **“edit <DHCP Server Number>”** komutuyla bir DHCP Server tanımlayıcısının oluşturulması gerekiyor. DHCP Server tanımı oluşturulduktan sonra **“set dns-service {local | default | specify}”** komutuyla DNS Server ip bilgisinin nereden alınacağı ayarlanabilir. Ardından **“set default-gateway <Gateway Ip Address>”** komutuyla Default Gateway adresi, **“set netmask <Netmask>”** komutuyla Subnet maskesi tanımlanabilir. Artık **“config ip-range”** ve **“edit <IPool Id>”** komutlarıyla bir ip havuzu tanımı oluşturularak **“set start-ip <Start Ip Address>”** ve **“set end-ip <End Ip Address>”** komutlarıyla başlangıç ve bitiş ip adres aralıkları belirtilebilir. Tanım sonunda **“next”** anahtar sözcüğünün kullanılması gerekiyor. Aynı prosedür uygulanarak farklı ip havuzları da oluşturulabilir (tanımlanacak ip havuzu aralıklarının arayüz ile aynı ip/subnet içerisinde olması gerekiyor). Ip havuzu tanımını sonlandırmak için **“next”** anahtar kelimesinden sonra ip havuzu tanımlanan arayüzden çıkış yapabilmek için **“end”** anahtar kelimesinin kullanılması gerekiyor.
- Son adımda tanımlanan DHCP Server konfigürasyonunu bir fiziksel arayüze uygulamak için **“set interface <Port Id>”** komutu ve DHCP sunucusunu devreye almak için **“set status {enable | disable}”** komutu kullanılıyor.

```

FortiGate-VM64-KVM (server) # edit 5
new entry '5' added

FortiGate-VM64-KVM (5) # set dns-service default

FortiGate-VM64-KVM (5) # set default-gateway 192.168.20.1

FortiGate-VM64-KVM (5) # set netmask 255.255.255.0

FortiGate-VM64-KVM (5) # config ip-range

FortiGate-VM64-KVM (ip-range) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set start-ip 192.168.20.10

FortiGate-VM64-KVM (1) # set end-ip 192.168.20.100

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (ip-range) # edit 2
new entry '2' added

FortiGate-VM64-KVM (2) # set start-ip 192.168.20.101

FortiGate-VM64-KVM (2) # set end-ip 192.168.20.254

FortiGate-VM64-KVM (2) # next

FortiGate-VM64-KVM (ip-range) # end

FortiGate-VM64-KVM (5) # set interface port2

FortiGate-VM64-KVM (5) # set status enable

FortiGate-VM64-KVM (5) # end

```

☒ DHCP Server

DHCP status

Address range

Netmask

Default gateway

DNS server

Lease time ☒ second(s)

Advanced

| → **Address Range** alanında aynı ip bloğu altında birden fazla aralık tanımlanarak belirli aralıklardaki ip adresler Exclude edilebiliyor (Örnek olarak 192.168.20.10-192.168.20.20 ve 192.168.20.50-192.168.20.254 tanımlanarak 192.168.20.21-192.168.20.49 aralığındaki ipa adresleri Exclude edilebilir). CLI üzerinden yapılmak istendiğinde ise “**config exclude-range**” komutuyla Exclude edilmek istenen aralıklar doğrudan tanımlanabiliyor.

DHCP Advanced

Bu tanımlamalar kullanılarak bir DHCP sunucusu ayarlanabileceği gibi **Advanced** kısmıyla DHCP sunucusu özelleştirilebiliyor.

- **Mode** kısmındaki **Server** seçeneğiyle ip bilgilerini kendi üzerinden çalışan DHCP sunucusundan gönderebileceği gibi **Relay** seçeneğiyle DHCP paketlerini uzak bir DHCP sunucusuna yönlendirmesi de sağlanabiliyor (Bu özellik DHCP Relay Agent olarak biliniyor. Detaylı bilgi için CCNA - 2.07 - DHCPv4 notlarını inceleyebilirsiniz).
 - Relay seçeneği seçildiğinde DHCP paketlerinin yönlendirileceği DHCP sunucusunun ip adresinin girilmesi gerekiyor.

- **Type** kısmıyla IPsec VPN yapılan istemcilere mi yoksa normal bağlanan istemcilere mi hizmet vereceğini belirlemek için kullanılıyor (Genelde IPsec üzerinden bağlı istemcileri DHCP Relay Agent özelliğiyle harici bir DHCP sunucusuna yönlendirilirken IPsec seçeneği kullanılmış).
- **NTP Server**, İstemcilere NTP sunucusunun ip adresi de DHCP sunucusu üzerinden öğretiliyor. NTP sunucusu için 3 farklı ip adresi tanımlanabiliyor.
- **Wireless Controllers**, NTP sunucusu gibi DHCP protokolü üzerinden WLC'lerin ip adresleri de öğretiliyor.
- **TimeZone**, istemcilere gönderilecek zaman dilimi bilgisini ayarlamak için kullanılıyor.
- **Additional DHCP Options** kısmında DHCP Option Code'lar kullanılarak NTP, WLC gibi daha pek çok ip bilgisi DHCP sunucusu üzerinden öğretiliyor. DHCP Option Code listesi için <https://www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml> adresini ziyaret edebilirsiniz.
- **"IP Address Assignment Rules"** kısmıyla belirli MAC adreslerinin sabit ip bilgisi alabilmesi için MAC-ip eşlemesi tanımlanabiliyor.

NOTLAR

- Varsayılanda Fortigate FW portları L2 trafiğini geçiriyor. Portlar üzerinde L2 işlemler yapabilmek için **"config system interface"**, **"edit <Port No>"**, **"set l2forward enable"** ve **"end"** komutlarının kullanılması gerekiyor
(<https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/287001/layer-2-interfaces> – <https://community.fortinet.com/t5/FortiGate/Technical-Tip-STP-forwarding/ta-p/191306>).

```
FortiFirewall-VM64 (port2) # set l2forward
enable      Enable L2 forwarding.
disable     Disable L2 forwarding.
```

- Ek olarak portlarda **PPPoE** modunu devreye almak için CLI üzerinde **"config system interface"**, **"edit <Port Number>"** ve **"set mode pppoe"** komutları kullanılıyor. Bu komut sonrasında PPPoE modu arayüzde de görünür hale geliyor (PPPoE modu kullanılarak ADSL modem varsa Bridge moda alınarak FW üzerinde sonlandırılabilir. ISP'nin verdiği kullanıcı adı, parola bilgisi ve ip adresi girilerek ADSL modem üzerinden internete çıkılabilir).

```
FortiFirewall-VM64 # config system interface
FortiFirewall-VM64 (interface) # edit port2
FortiFirewall-VM64 (port2) # set mode pppoe
FortiFirewall-VM64 (port2) # end
```

Address	
Addressing mode	Manual DHCP Auto-managed by IPAM PPPoE One-Arm Sniffer
Status	Initializing...
Username	
Password	
Unnumbered IP	0.0.0.0
Initial Disc Timeout	1
Initial PADT Timeout	1
Retrieve default gateway from server	<input checked="" type="checkbox"/>
Distance	5
Override internal DNS	<input checked="" type="checkbox"/>

- Uygulanan konfigürasyonları görüntülemek için herhangi bir arayüze giriş yapıp altında “**show full-configuration**” komutu kullanılıyor. Örnek olarak “**config system dhcp server**” arayüzü altında “**show full-configuration**” komutu çalıştırabilirsin.

Kaynaklar

- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/574723/interface-settings>
- <https://community.fortinet.com/t5/Support-Forum/Create-address-object-matching-subnet-is-no-longer-optional/m-p/246262>
- https://help.fortinet.com/fdb/5-0-0/html/source/tasks/t_network_configuration_cli.html
- <https://docs.fortinet.com/document/fortigate/7.2.4/administration-guide/259467/interface-subnet>
- <https://community.fortinet.com/t5/FortiGate/Troubleshooting-Tip-FortiGate-is-not-using-the-configured-DNS/ta-p/240785>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-Set-a-secondary-IP-on-a-FortiGate-interface/ta-p/226046>
- <https://www.bilisimasistani.com/fortigate-adsl-hatlar-icin-trafik-yonlendirme/>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/783526/dhcp-server>