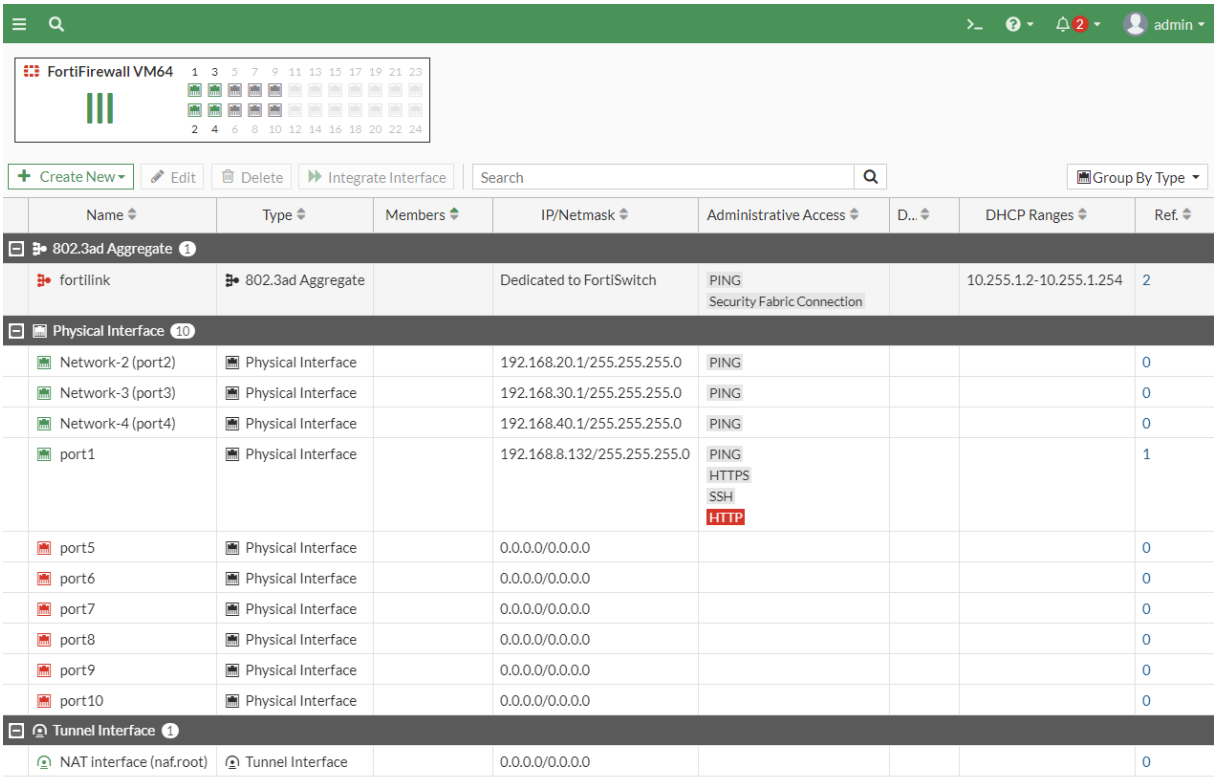
Interfaces - 1

Interface sekmesinde kullanıcıyı cihaz üzerindeki fiziksel portların bulunduğu bir tablo karşılıyor. Tablonun sütun kısmına sağ tık yapılıp 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

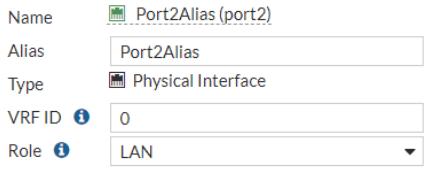
Listelenen portların arayüzlerine giriş yapılarak fiziksel portlara uygulanabilecek konfigürasyonlara bakıldığında;

- **Alias**, kısmıyla porta takma ad belirlemek için kullanılıyor.
    - 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 dâhil edilmesi gerekiyor.
    - 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.
  - **LAN,** iç networke (LAN) bağlanmak için kullanılan roldür. Yeni arayüzler için varsayılanda gelen roldür.
  - **WAN,** internete bağlanmak için kullanılan roldür.
  - **DMZ,** DMZ'ye bağlanmak için kullanılan roldür.
  - 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
```



- **Addressing Mode**, cihaz arayüzüne ip adresi tanımlamak için kullanılan alandır. Dört farklı şekilde ip adresi tanımlanabiliyor. Bu seçeneklere bakıldığında;
  - **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.

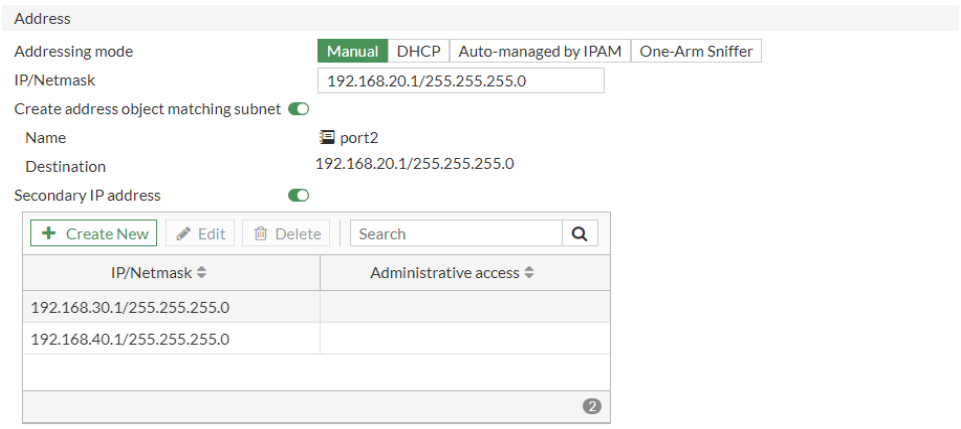
```
FortiGate-VM64-KVM # config system interface

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.
      - Bu özelliği devreye almak için herhangi bir portun arayüzü altında ip adresi tanımlandıktan sonra "**config firewall address**", "**edit <Addr Name>**", "**set type interface-subnet**" ve "**set interface port<Port Id>**" komutları kullanılarak arayüz Subnet Firewall adres tanımının yapılması gerekiyor. Bu tanım altında tanım/adres tipi ve hangi arayüzle eşleştirileceğinin belirtilmesi gerekiyor. 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 FWAddrPort2
new entry 'FWAddrPort2' added

FortiGate-VM64-KVM (FWAddrPort2) # set type interface-subnet

FortiGate-VM64-KVM (FWAddrPort2) # set interface port2

FortiGate-VM64-KVM (FWAddrPort2) # end
```

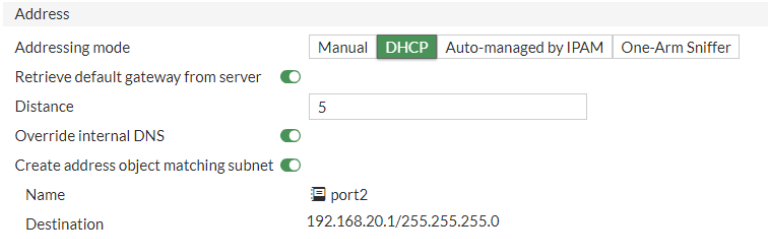
- **Secondary Ip Address**, fiziksel porta üzerinde kullanılabilecek ikinci bir ip adresi tanımlamak için kullanılıyor. Bu özellik kullanılarak aynı anda iki farklı networke hizmet verebiliyor. Farklı bir kullanım örneği olarak tek bir arayüz üzerinde farklı ip adreslerine ihtiyaç duyan hizmetler devreye 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 tanımı 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
```



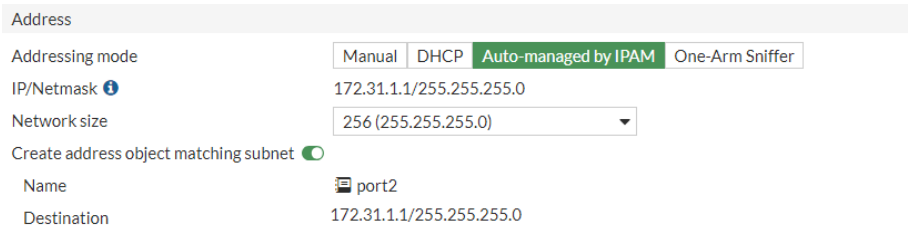
- **DHCP**, arayüzün bağlı olduğu network üzerindeki bir DHCP sunucusundan ip bilgilerini aldığı seçenektir.
  - **Retrieve default gateway from server Distance**, ADSL hatlar üzerinden internete çıkabilmek için PPPoE özelliğiyle birlikte bu özelliğin de devrede olması gerekiyor. Detaylı bilgi ve örnek 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.
    - İlgili 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
```



- **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 (Sanırım Windows cihazlardaki APIPA adresler gibi).
  - 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
```



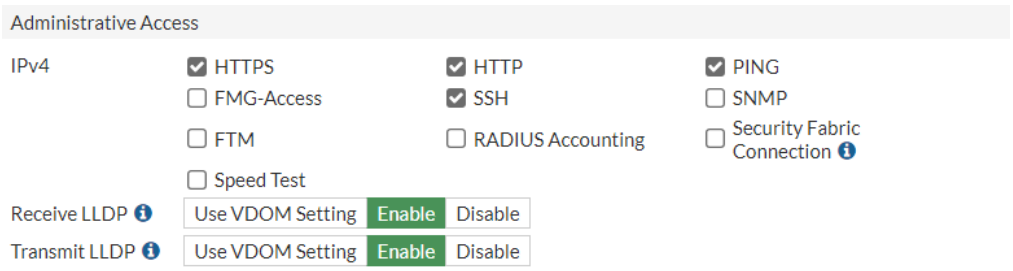
- **One-Arm Siffer**, port üzerinde uygulanabilecek güvenlik özellikleridir. Bu özellikler ayarlanarak porta gelen trafiğin kontrol edilmesi ve tanımlanan güvenlik politikalarına göre değerlendirilmesi sağlanıyor. Konfigürasyonu ve uygulamaları **Interfaces – 2 – One Arm Sniffer** isimli yazıda detaylıca 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).
  - CLI ekranında ilgili arayüz altına girildikten sonra "**set allowaccess <Protocol Names>**" komutuyla izinler tanımlanabiliyor.
  - Bu kısımdan izin verilmediği sürece port üzerinde tanımlı ip adreslerine Ping dahi atılamadığını 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
```

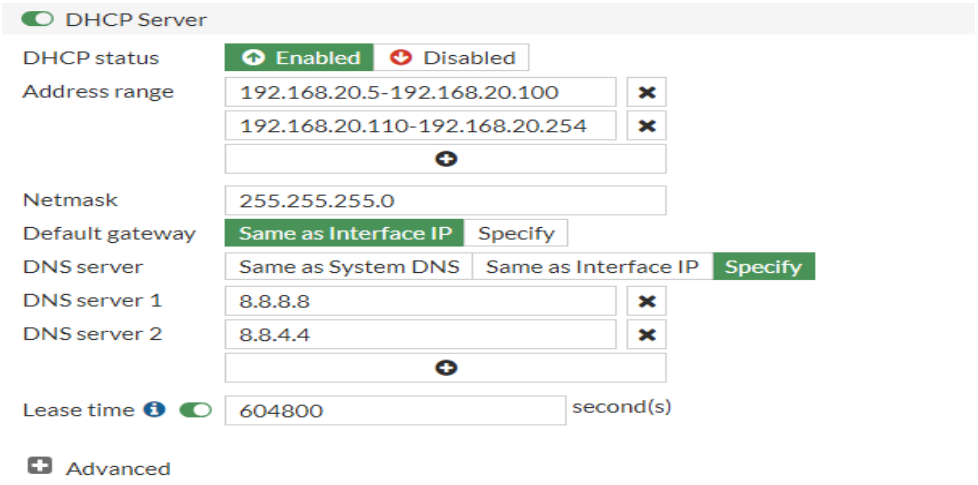
- **Received LLDP and Transmit LLDP (Link Layer Discovery Protocol)**, network üzerindeki cihazları keşfetmek için kullanılan protokoldür (Cisco marka cihazlardaki CDP protokolü gibi). Bu özellik aktif edilerek LLDP mesajların alınıp gönderilmesi sağlanabiliyor. Bu özellik Global, Interface ve VDOM olmak üzere üç farklı şekilde devreye alınabilir. CLI üzerinde;
  - 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.
  - 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
```



- **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 Gareway** 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.
    - 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).
    - 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 pavuzu 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 # config system dhcp server

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

FortiGate-VM64-KVM (2) # set dns-service specify

FortiGate-VM64-KVM (2) # set dns-server1 8.8.8.8

FortiGate-VM64-KVM (2) # set dns-server2 8.8.4.4

FortiGate-VM64-KVM (2) # set default-gateway 192.168.20.1

FortiGate-VM64-KVM (2) # set netmask 255.255.255.0

FortiGate-VM64-KVM (2) # config ip-range

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

FortiGate-VM64-KVM (1) # set start-ip 192.168.20.5

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 192.168.20.110

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

FortiGate-VM64-KVM (2) # end

FortiGate-VM64-KVM (2) # set interface port2

FortiGate-VM64-KVM (2) # set status enable

FortiGate-VM64-KVM (2) # end
```



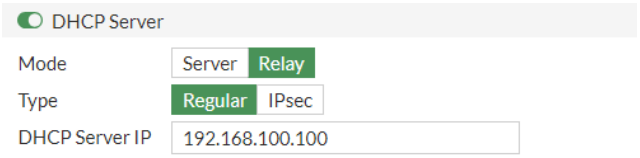
|→ **Address Range** alanında aynı ip bloğu altında birden fazla aralık tanımı yapılarak belirli aralıklardaki ip adresler Exclude edilebiliyor (Örnek olarak 192.168.20.10-192.168.20.20 ve 192.168.20.50-192.168.20.254 tanımı yapılarak 192.168.20.21-192.168.20.49 aralığındaki ip adresleri Exclude edilebilir). 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 **Advaced** 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 inceleyebilirsin).
    - Relay seçeneği seçildiğinde DHCP paketlerinin yönlendirileceği DHCP sunucusunun ip adresinin girilmesi gerekiyor.
    - Relay Agent özelliğinin konfigürasyonu için devreye alınacağı fiziksel portun arayüzü altında "**set dhcp-relay-service {enable | disable}**" komutuyla devreye alınması gerekiyor. Ardından "**set dhcp-relay-ip <DHCP Ip Address>**" komutuyla yönlendirilecek DHCP sunucusunun ip adresinin tanımlanması gerekiyor. İsteğe bağlı olarak Cisco switchlerde DHCP Snooping özelliği (option 82 in RFC 3046) olarak bilinen güvenlik çözümünün devreye alınması için "**set dhcp-relay-agent-option {enable | disable}**" komutu kullanılabilir (DHCP Relay Agent özelliğiyle DHCP sunuculuğunun aynı anda yapılamadığını unutma).
- **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).

```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set dhcp-relay-service enable

FortiGate-VM64-KVM (port2) # set dhcp-relay
dhcp-relay-interface-select-method    Specify how to select outgoing interface to reach server.
dhcp-relay-service                    Enable/disable allowing this interface to act as a DHCP relay.
dhcp-relay-ip                         DHCP relay IP address.
dhcp-relay-request-all-server         Enable/disable sending of DHCP requests to all servers.
dhcp-relay-type                       DHCP relay type (regular or IPsec).
dhcp-relay-agent-option               Enable/disable DHCP relay agent option.

FortiGate-VM64-KVM (port2) # set dhcp-relay-ip 192.168.100.100
FortiGate-VM64-KVM (port2) # set dhcp-relay-agent-option enable

FortiGate-VM64-KVM (port2) # end
```



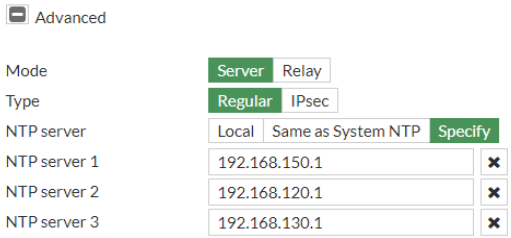
- **NTP Server**, İstemcilere NTP sunucusunun ip adresi de DHCP sunucusu üzerinden öğretilebiliyor. NTP sunucusu için 3 farklı ip adresi tanımlanabiliyor.
    - DHCP sunucusu üzerinde NTP Server ip bilgisi de öğretebilmek için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında giriş yapılarak "**set ntp-service {local | default | specify}"** komutuyla NTP sunucusunun ip bilgisinin kaynağı belirtilmelidir. Burada **Specify** seçeneği seçildiğinde "**set {ntp-server1 | ntp-server2 | ntp-server3} <NTP Server Ip Address >**" komutuyla 3 farklı NTP Server ip adresi tanımlanabiliyor.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # set ntp-service specify

FortiGate-VM64-KVM (5) # set ntp-server1 192.168.150.1

FortiGate-VM64-KVM (5) # set ntp-server2 192.168.120.1

FortiGate-VM64-KVM (5) # set ntp-server3 192.168.130.1

FortiGate-VM64-KVM (5) # end
```

|→ **Local**, DHCP sunucusunun eklendiği arayüzün IP adresi, istemcinin NTP sunucu ip adresi olur.

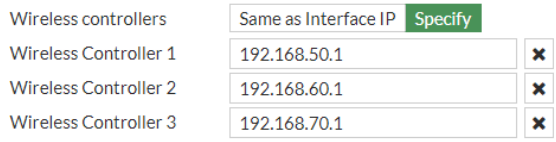
|→ **Default**, İstemcilere FortiGate'in yapılandırılmış NTP sunucuları atanır.

|→ **Specify**, DHCP sunucusu yapılandırmasında en fazla üç NTP sunucusu belirtilir.



- **Wireless Controllers**, NTP sunucusu gibi DHCP protokolü üzerinden AC'ların ip adresleri de öğretilebiliyor.
  - DHCP sunucusu üzerinden AC'lerin ip bilgisini öğretebilmek için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında giriş yapılar "**set wifi-ac-service {specify | local}**" komutuyla ip bilgisinin nasıl belirleneceği tanımlanıyor. Burada NTP Server tanımında olduğu gibi **Specify** seçeneği seçildiğinde "**set {wifi-ac1 | wifi-ac2 | wifi-ac3} <AC Ip Address>**" komutuyla 3 farklı AC ip adresi tanımlanabiliyor.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # set wifi-ac-service specify

FortiGate-VM64-KVM (5) # set wifi-ac1 192.168.50.1

FortiGate-VM64-KVM (5) # set wifi-ac2 192.168.60.1

FortiGate-VM64-KVM (5) # set wifi-ac3 192.168.70.1

FortiGate-VM64-KVM (5) # end
```



- **TimeZone,** istemcilere gönderilecek zaman dilimi bilgisini ayarlamak için kullanılıyor.
  - Konfigürasyonu için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında giriş yapılar "**set timezone-option {default | specify | disable}**" komutuyla zaman dilimi bilgisinin nereden alınacağı belirleniyor. Burada NTP **Specify** seçeneği seçildiğinde "**set timezone <Timezone (1-20 arası)>**" komutuyla özel bit zaman dilimi ayarlanabiliyor.

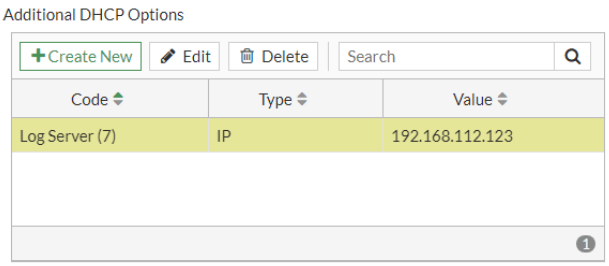
```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # set timezone-option specify

FortiGate-VM64-KVM (5) # set timezone 12

FortiGate-VM64-KVM (5) # end
```

- **Next Bootstrap Server**,

- **Additional DHCP Options** kısmında DHCP Option Code'lar kullanılarak NTP, WLC gibi daha pek çok ip bilgisi DHCP sunucusu üzerinden öğretilebiliyor. DHCP Option Code listesi için https[:]//www.iana.org/assignments/bootp-dhcp-parameters/bootp-dhcp-parameters.xhtml adresini ziyaret edebilirsin.
  - Konfigürasyonu için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında "**config option**" komutuyla Opton Code arayüzüne giriş yapılıyor. Burada "**edit <Option Code Identifier>**" komutuyla bir Option Code tanımı oluşturuluyor. Bu tanım altında "**set code <Option Code>**" komutuyla Option Code değeri, "**set type {hex | string | ip | fqdn}**" komutuyla öğretilecek değerin tipi, "**set value <String>**" ve "**set ip <Ip Address>**" komutlarıyla öğretilecek değer girildikten sonra "**next**" kelimesiyle aynı prosedür uygulanarak ikinci bir Option Code tanımı yapılabilir.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # config options

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

FortiGate-VM64-KVM (1) # set code 7

FortiGate-VM64-KVM (1) # set type ip

FortiGate-VM64-KVM (1) # set ip 192.168.112.123

FortiGate-VM64-KVM (1) # next

FortiGate-VM64-KVM (options) # end

FortiGate-VM64-KVM (5) # end
```

|→ Örnek olarak Log sunucusunun ip adresi için tanım yapılmıştır. Web arayüzü üzerinden de tanım yapılabilir.



- "**IP Address Assignment Rules**" kısmıyla belirli MAC adreslerinin sabit ip bilgisi alabilmesi için MAC-Ip eşlemesi tanımlanabiliyor. Bu sayede istemciler ip bilgisi istediğinde, istemci için tanımlı satır tespit edilir ve rezerve edilen ip adresi sunulur (Bu ip adresi DHCP sunucusunun ip havuzunun dışında (Excluded) bulunan bir ip adres olmalı. Aksi takdirde

DHCP sunucusu bu ip adresini farklı bir istemciye kiralarsa, rezerve edilen istemci sunucudan başka bir ip bilgisi alamayacağı için networke bağlanamaz).

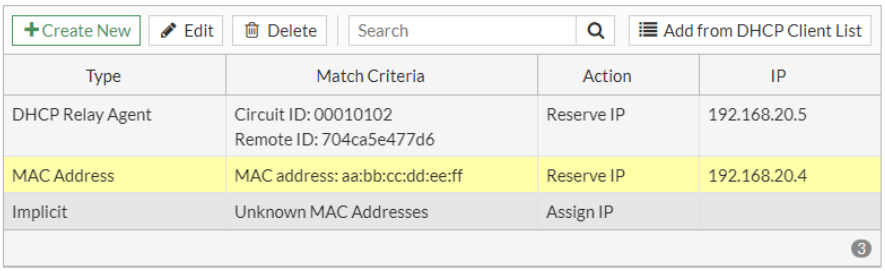
- IP-MAC adres rezervasyonu konfigürasyonu için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında "**config reserved-address**" komutuyla reserved-address arayüzüne giriş yapılıyor. Burada "**edit <Reserved Address Identifier>**" komutuyla bir rezerve adres tanımı oluşturuluyor. Oluşturulan rezerve adres tanımının tipini belirlemek için "**set type <mac | option82>"** komutu kullanılıyor. Bu doğrultuda rezerve edilecek bilgileri ayarlamak için "**set ip <Ip Address>**", "**set mac <MAC Address>**" komutlarıyla rezerve istemci bilgileri tanımlanır.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # config reserved-address

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

FortiGate-VM64-KVM (2) # set type mac

FortiGate-VM64-KVM (2) # set ip 192.168.20.4

FortiGate-VM64-KVM (2) # set mac AA:BB:CC:DD:EE:FF

FortiGate-VM64-KVM (2) # end

FortiGate-VM64-KVM (5) # end
```

- Ip Address Assignment Rule kısmında DHCP Relay Agent özelliği üzerine konfigürasyon yapabilmek için DHCP Server arayüzünde tanımlanan DHCP sunucusu altında "**config reserved-address**" komutuyla reserved-address arayüzüne giriş yapılıyor. Burada "**edit <Reserved Address Identifier>**" komutuyla bir rezerve adres tanımı oluşturuluyor. Oluşturulan rezerve adres tanımının tipini belirlemek için "**set type <mac | option82>"** komutu kullanılıyor. Son adıma "**set ip <Ip Address>**", "**set circuit-id-type {string | hex}**", "**set circuit-id <Circuit Id>**", "**set remote-id-type {string | hex}**" ve "**set remote-id <Remote Id>**" komutları kullanılarak rezerve adres tanımı uygulanır.

```
FortiGate-VM64-KVM # config system dhcp server

FortiGate-VM64-KVM (server) # edit 5

FortiGate-VM64-KVM (5) # config reserved-address

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

FortiGate-VM64-KVM (1) # set type option82

FortiGate-VM64-KVM (1) # set ip 192.168.20.5

FortiGate-VM64-KVM (1) # set circuit-id-type hex

FortiGate-VM64-KVM (1) # set circuit-id "00010102"

FortiGate-VM64-KVM (1) # set remote-id-type hex

FortiGate-VM64-KVM (1) # set remote-id "704ca5e477d6"

FortiGate-VM64-KVM (1) # end

FortiGate-VM64-KVM (5) # end
```

IP Address Assignment Rules

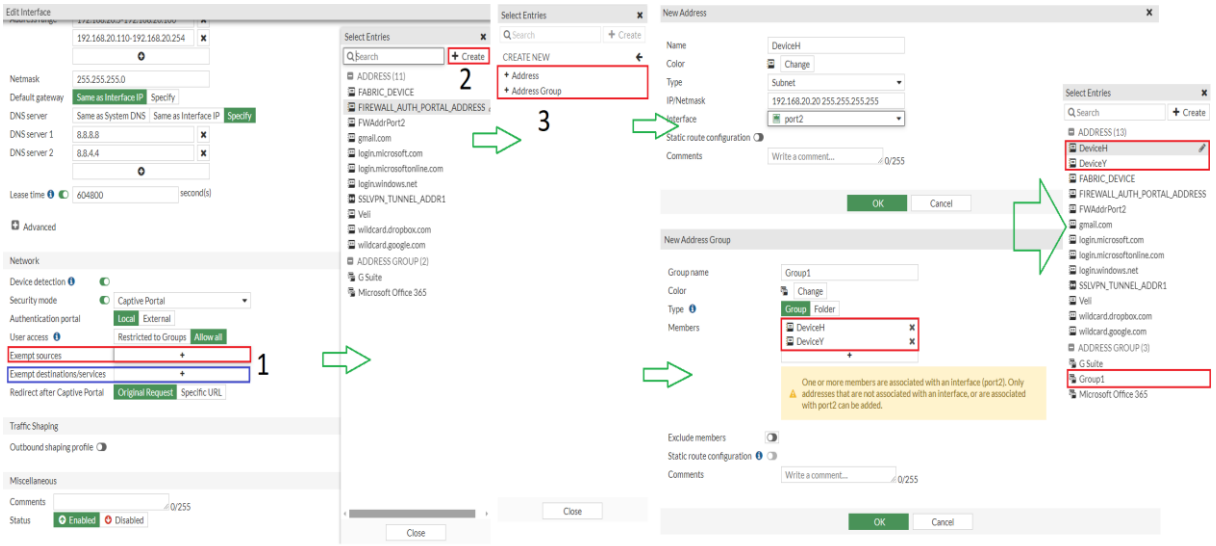


Type	Match Criteria	Action	IP
DHCP Relay Agent	Circuit ID: 00010102 Remote ID: 704ca5e477d6	Reserve IP	192.168.20.5
MAC Address	MAC address: aa:bb:cc:dd:ee:ff	Reserve IP	192.168.20.4
Implicit	Unknown MAC Addresses	Assign IP	

- **Network Detection**, LAN rolündeki portlara bağlı cihazlar hakkında bilgi toplamak için kullanılan bir özelliktir (WAN bacağında açıldığında bağlı istemcilerin kullandığı işletim sistemleri belirlenemeyebiliyormuş). Toplanan bilgileri görüntülemek için **Dashboard –> User&Device** kısmı kontrol edilebilir.
- **Security Mode**, bu port üzerinden bağlanan istemcilerin bir Captive Portal (web sayfası) üzerinden kimlik denetimine tabi tutulmasını sağlayan özelliktir.
  - Konfigürasyonu için fiziksel portun arayüzüne giriş yapılarak "**set security-mode {none | captive-portal}**" komutuyla güvenlik modu belirlenir. Güvenlik modu belirlendikten sonra "**set security-external-web <URL>**" komutuyla kimlik doğrulama işlemi için yönlendirilecek Captive Portal adresi (kimlik doğrulama işlemi harici bir adres üzerinde yapılacaksa – Local olarak/Fortigate üzerinde de kimlik doğrulama işlemi yapılabiliyor), "**set security-redirect-url <URL>"** komutuyla kimlik doğrulama gerçekleştirildikten sonra kullanıcının yönlendirileceği web sayfasının adresi, "**set security-exempt-list <Extempt-List>**" komutuyla kimlik doğrulama sürecinden muaf tutulacak kullanıcı bilgileri (Bunun için bir Extemt-List tanımı oluşturulmalıdır), "**security-external-logout <URL>**" komutuyla kullanıcı oturumunu sonlandırdığında yönlendirileceği adres bilgisi, "**set security-groups <group(s)>"** komutuyla Captive Portal üzerinden kimlik doğrulama işlemi yapabilecek kullanıcı grupları tanımlanabiliyor.

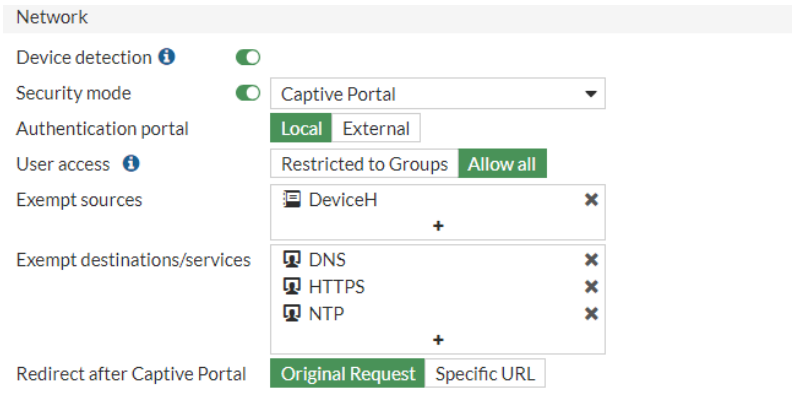
```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit port2

FortiGate-VM64-KVM (port2) # set security-mode captive-portal

FortiGate-VM64-KVM (port2) # set security-exempt-list MyExetmpList

FortiGate-VM64-KVM (port2) # end
```

  - Kimlik doğrulama sürecinden muaf tutulacak Extempt listesi oluşturmak için "**config user security-exempt-list**" komutu kullanılarak Extemt-List arayüzüne giriş yapılıp "**edit <Extempt List Name>**" komutuyla bir liste tanımı oluşturulmalıdır. Oluşturulan liste tanımı altında "**config rule**" komutuyla kural tanımı arayüzüne giriş yapılarak "**edit <Rule Id>**" komutuyla kural tanımları oluşturulmaya başlanabilir. Oluşturulan kural tanımları altında "**set srcaddr <Source Addresses>**","**set dstaddr <Destination Addresses>","set service <Services>**" komutlarıyla kimlik denetiminden muaf olacak kaynak adres, hedef adres veya servis tanımlamalar yapılmalıdır.
    - Burada kullanılmak üzere kullanıcı ve grup tanımları oluşturmak için arayüz üzerinde "+ -> Create -> Address veya Address Group" yolu takip edilmelidir. Oluşturulan kullanıcı ve grup tanımları Exemtp tanımlarında kullanılabilmektedir.



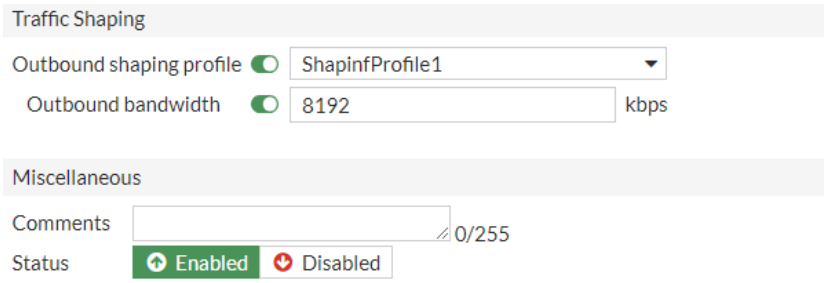
- Web arayüzü üzerinden kullanıcı ve grup tanımlarının nasıl yapıldığı adımlar üzerinden ifade edilmeye çalışılmıştır.

```
FortiGate-VM64-KVM # config user security-exempt-list

FortiGate-VM64-KVM (security-exempt-list) # edit MyExetmpList
new entry 'MyExetmpList' added

FortiGate-VM64-KVM (MyExetmpList) # config rule

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

FortiGate-VM64-KVM (1) # set srcaddr DeviceH

FortiGate-VM64-KVM (1) # set service HTTPS DNS NTP

FortiGate-VM64-KVM (1) # end

FortiGate-VM64-KVM (MyExetmpList) # end
```



|→ Konfigürasyondan da anlaşılacağı üzere herhangi bit External URL belirtilmediği sürece varsayılanda cihaz üzerindeki Captive Portal kullanılıyor.

- **Outbound Shaping Profile**, port üzerindeki trafiği şekillendirmek üzere kullanılan özelliktir. Bu alan Policy&Object alanı altındaki Traffic Shaping sekmesinde oluşturulan profil tanımlarını portlara uygulamak için kullanılmaktadır. Bu özellik **Policy&Object -> Traffic Shaping** konusunda detaylandırılacaktır.
- **Miscellaneous**, fiziksel portu açıp kapatmak için kullanılmaktadır.



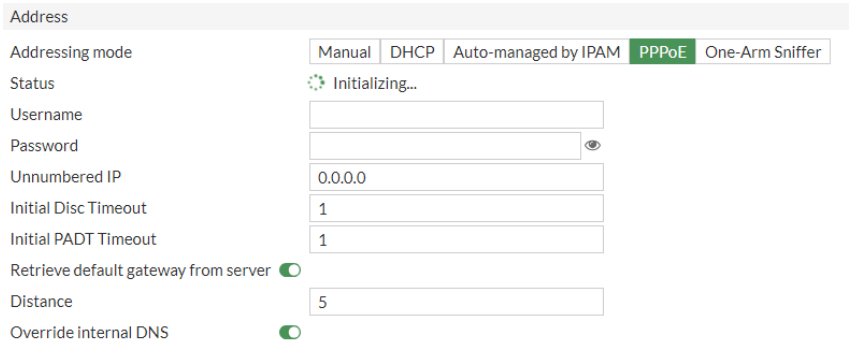
NOTLAR

- Varsayılanda Fortigate FW portları L2 trafiğini geçirmiyor. 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 sonlandırılabiliyor. ISP'nin verdiği kullanıcı adı, parola bilgisi ve ip adresi girilerek ADSL modem üzerinden internete çıkılabiliyor).

```
FortiFirewall-VM64 # config system interface

FortiFirewall-VM64 (interface) # edit port2

FortiFirewall-VM64 (port2) # set mode pppoe

FortiFirewall-VM64 (port2) # end
```



- Uygulanan konfigürasyonları görüntülemek için herhangi bir arayüze giriş yapılıp 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
- https[:]//docs.fortinet.com/document/fortigate/6.2.4/cli-reference/59620/system-dhcp-server
- https[:]//docs.ansible.com/ansible/latest/collections/fortinet/fortios/fortios_system_dhcp_server_module.html
- https[:]//docs.fortinet.com/document/fortigate/6.2.4/cli-reference/59620/system-dhcp-server
- https[:]//docs.fortinet.com/document/fortigate/7.4.3/administration-guide/934626/captive-portals
- https[:]//docs.fortinet.com/document/fortigate/7.0.1/cli-reference/515620/config-user-security-exempt-list
- https[:]//docs.fortinet.com/document/fortigate/6.2.1/cli-reference/423620/user-security-exempt-list