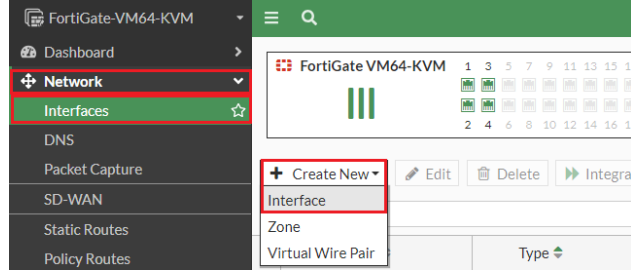


Interfaces - 3

Cihaz üzerinde Loopback Interface tanımı, fiziksel arayüzler üzerinde Redundancy, VLAN, Link Aggregation veya SSL-VPN gibi konfigürasyonları yapabilmek için “Interfaces -> Create New -> Interface” yolu takip edilmelidir. Bu yazıda arayüzler üzerinde bu özelliklerin nasıl devreye alınabileceği açıklanmaya çalışılacaktır.



LACP Konfigürasyonu (802.3ad Aggregate - Link Aggregation)

Fortigate arayüzlerinde LACP konfigürasyonu yapabilmek için ilk olarak “**configure system interface**” arayüzü altında “**edit <Interface Name>**” komutuyla bir arayüz tanımı yapılması gerekiyor. Bu arayüz altında;

- İlk adımda arayüzün çalışacağı VDOM “**set vdom <VDOM Name>**” komutuyla belirtilmelidir.
- VDOM tanımı yapıldıktan sonra “**set member <Physical Interface Id's>**” komutuyla bu arayüze/gruba dâhil edilecek fiziksel arayüzlerin eklenmesi gerekiyor.
 - o Eklencek fiziksel arayüzlerde ip adreslerinin tanımlanmamış olması gerekiyor. Dâhil edilen fiziksel arayüzlere dair bütün konfigürasyonlar burada oluşturulan arayüz içerisinde tanımlanıyor (Zaten konfigürasyon sonrasında fiziksel portlar “**Physical Interface**” kısmından kaldırılarak “**802.3ad Aggregate**” kısmına taşınacaktır).
- Dâhil edilecek arayüzler tanımlandıktan sonra oluşturulan arayüz tanımının modu “**set type {vlan | aggregate | redudant | loopback | wimesh | emac-vlan | ssl }**” komutuyla belirtilmelidir.
- Son olarak oluşturulan arayüzün çalışacağı rol “**set role <lan | wan | dmz | unified>**” komutuyla belirtilmelidir.

LACP konfigürasyonu için bu ayarlamalar yapıldıktan sonra fiziksel portların arayüzlerine uygulanmak istenen tanımlamalar burada oluşturulan arayüz/LACP grubu altında tanımlanmalıdır (Bu portlara bağlanacak switch portlarında da karşılıklı olarak LACP protokolü devrede olmalıdır).

```
FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit LACPInterface
FortiGate-VM64-KVM (LACPInterface) # set vdom root
FortiGate-VM64-KVM (LACPInterface) # set member port3 port4
FortiGate-VM64-KVM (LACPInterface) # set type aggregate
FortiGate-VM64-KVM (LACPInterface) # set role lan
FortiGate-VM64-KVM (LACPInterface) # end
```

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate							
fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection		10.255.1.2-10.255.1.254	2
LACPIInterface (Arayüzün Up olduğu görülüyor)	802.3ad Aggregate	port3 port4	0.0.0.0/0.0.0.0				0
Physical Interface							
port1	Physical Interface		192.168.0.100/255.255.255.0	PING HTTPS SSH HTTP			2
port2	Physical Interface		192.168.20.1/255.255.255.0	PING HTTPS	1	192.168.20.5-192.168.20.100 192.168.20.110-192.168.20.254	6
Tunnel Interface							
NAT interface (naf.root)	Tunnel Interface		0.0.0.0/0.0.0.0				0

Edit Interface

Name	LACPIInterface
Alias	
Type	802.3ad Aggregate
VRF ID	0
Interface members	port3 x port4 x +
Role	LAN

VLAN Konfigürasyonu

Fortigate üzerindeki fiziksel portlarda VLAN'lar için Sub-Interface tanımları yapılarak VLAN'ların internete çıkarılması sağlanabiliyor. Sub-Interface tanımı için ilk olarak **"configure system interface"** arayüzü altında **"edit <VLAN Name>"** komutuyla bir arayüz tanımı yapılması gerekiyor. Bu arayüz altında (<https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/402940/vlans>);

- İlk adımda arayüzün çalışacağı VDOM **"set vdom <VDOM Name>"** komutuyla belirtilmelidir.
- VDOM tanımı yapıldıktan sonra **"set interface <Interface Id>"** komutuyla oluşturulan Sub-Interface tanımının hangi fiziksel arayüz altında çalışacağı belirtilmelidir.
- Oluşturulan arayüz tanımının modu **"set type {vlan | aggregate | redundant | loopback | wimesh | emac-vlan | ssl}"** komutuyla belirtilmelidir.
- Oluşturulan arayüzün modu belirlendikten sonra bu arayüze gelecek paketlere hangi VLAN etiketinin ekleneceği **"set vlanid <VLAN Id>"** komutuyla belirtilmelidir.
- VLAN etiket bilgisi tanımlandıktan sonra artık VLAN'ın dahil olduğu network bilgisi ile ilişkilendirmek üzere öncelikle **"set mode {static | dhcp | pppoe}"** komutuyla ip adresinin nasıl belirleneceği (statik) belirtilerek bu doğrultuda Sub-Interface'in ip bilgisi alması sağlanmalıdır (statik tanım için **"ip set <Ip Address> <Subnet Mask>"** komutuyla ip adresi tanımlanmalıdır).

Temelde bu ayarlamalar yapıldıktan sonra VLAN'lara uygulanmak istenen tanımlamalar burada oluşturulan VLAN arayüzlerine tanımlanmalıdır (Bu portlara bağlanacak switch portlarının Trunk modunda olması gerekiyor ki tek bir Sub-Interface üzerinde birden fazla VLAN'a hizmet verilebilsin).

Physical Interface 10							
port1	Physical Interface		192.168.0.100/255.255.255.0	PING HTTPS SSH HTTP			
port2	Physical Interface		0.0.0.0/0.0.0.0	PING HTTPS			
VLAN100	VLAN		192.168.100.1/255.255.255.0				
VLAN200	VLAN		192.168.200.1/255.255.255.0				

```

FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit VLAN100
FortiGate-VM64-KVM (VLAN100) # set vdom root
FortiGate-VM64-KVM (VLAN100) # set interface port2
FortiGate-VM64-KVM (VLAN100) # set type vlan
FortiGate-VM64-KVM (VLAN100) # set vlanid 100
FortiGate-VM64-KVM (VLAN100) # set mode static
FortiGate-VM64-KVM (VLAN100) # set ip 192.168.100.1 255.255.255.0
FortiGate-VM64-KVM (VLAN100) # next
FortiGate-VM64-KVM (interface) # edit VLAN200
FortiGate-VM64-KVM (VLAN200) # set vdom root
FortiGate-VM64-KVM (VLAN200) # set interface port2
FortiGate-VM64-KVM (VLAN200) # set type vlan
FortiGate-VM64-KVM (VLAN200) # set vlanid 200
FortiGate-VM64-KVM (VLAN200) # set mode static
FortiGate-VM64-KVM (VLAN200) # set ip 192.168.200.1 255.255.255.0
FortiGate-VM64-KVM (VLAN200) # end

```

Loopback Interface Konfigürasyonu

Cihaz ayakta olduğu sürece herhangi bir aktif fiziksel portu üzerinden erişim sağlanabilmesi için kullanılan sanal arayüzdür. Loopback Interface tanımı için ilk olarak “**configure system interface**” arayüzü altında “**edit <Loopback Interface Name>**” komutuyla bir arayüz tanımı yapılması gerekiyor. Bu arayüz altında;

- İlk adımda arayüzün çalışacağı VDOM “**set vdom <VDOM Name>**” komutuyla belirtilmelidir.
- VDOM tanımı yapıldıktan sonra “**ip set <Ip Address> <Subnet Mask>**” komutuyla Loopback arayüzüne ip adresinin tanımlanması gerekiyor.
- Son olarak oluşturulan arayüz tanımının modu “**set type {vlan | aggregate | redundant | loopback | wimesh | emac-vlan | ssl }**” komutuyla belirtilmelidir.

Burada uygulama yaparken ilgili arayüzün Loopback arayüzüne erişebilmesi için bir Firewall politikasının tanımlı olmasına dikkat edilmelidir. Aksi takdirde “Implicit Deny” satırıyla eşleşecektir.

İsteğe bağlı olarak bu arayüz üzerinde de çeşitli özellikler devreye alınabiliyor.

```

FortiGate-VM64-KVM # config system interface
FortiGate-VM64-KVM (interface) # edit LoopbackInter
FortiGate-VM64-KVM (LoopbackInter) # set vdom root
FortiGate-VM64-KVM (LoopbackInter) # set ip 192.168.50.10 255.255.255.255
FortiGate-VM64-KVM (LoopbackInter) # set type loopback
FortiGate-VM64-KVM (LoopbackInter) # end

```

Create New

Edit

Delete

Integrate Interface

Search

Group By Type

Name	Type	Members	IP/Netmask	Administrative Access	DHCP Clients	DHCP Ranges	Ref.
802.3ad Aggregate							
Loopback Interface							
LoopbackInter	Loopback Interface		192.168.50.10/255.255.255.255	PING			2

FortiGate-VM64-KVM

Dashboard

Network

Policy & Objects

Firewall Policy

IPv4 DoS Policy

Addresses

Internet Service Database

Services

Schedules

Create New

Edit

Delete

Policy Lookup

Search

Export

Interface Pair View

By Sequence

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
port12 -> LoopbackInter									
Loopback Access VLAN200	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	0 B
VLAN100 -> LoopbackInter									
Loopback Access VLAN100	all	all	always	ALL	ACCEPT	Enabled	no-inspection	UTM	240 B
Implicit									
Implicit Deny	all	all	always	ALL	DENY			Disabled	180 B

| → VLAN konfigürasyonu ile birlikte denemek için oluşturulan Firewall Policy tanımlarıdır.

Software Switch Konfigürasyonu

Fortigate üzerindeki portlara bağlı istemcilerin aralarında bir switch varmış gibi haberleşebilmelerini sağlamak üzere yazılım temelinde switch görevi gören özelliktir (Bu sayede ek bir Firewall konfigürasyonuna gerek kalmadan iki farklı arayüze bağlı istemciler aralarında haberleşebilecektir – arayüzlerde ip konfigürasyonu yapılmadığı ve istemcilerin aynı networke dâhil olmaları şartıyla).

Özellik isminden de anlaşılacağı üzere anahtarlama işlemini donanım temeli yerine yazılım temelinde gerçekleştirilmektedir. Yani bu süreçte CPU tüketiyor. Bu nedenle bu özellik devreye alınırken dikkatli olunmalıdır.

Software Switch tanımı için ilk olarak “**config system switch-interface**” arayüzü altında “**edit < Software Switch Name>**” komutuyla bir arayüz tanımı yapılması gerekiyor. Bu arayüz altında;

- Arayüzün çalışacağı VDOM “**set vdom <VDOM Name>**” komutuyla belirtilmelidir.
- VDOM tanımı yapıldıktan sonra “**set member <Physical Interface Id's>**” komutuyla bu arayüze/gruba dâhil edilecek fiziksel arayüzlerin eklenmesi gerekiyor.
 - o Burada eklenecek fiziksel arayüzlere ip adresleri atanmamış olması gerekiyor (Konfigürasyon komut satırında yapıldığında ip adresi atanmış portlar görünmüyor).
- Son olarak oluşturulan arayüz tanımının modu “**set type switch**” komutuyla belirtilmelidir.

Software Switch konfigürasyonu için temelde bu ayarlamalar yapıldıktan sonra normal bir fiziksel arayüze uygulanmak istenen tanımlamalar burada oluşturulan Software Switch arayüzüne tanımlanmalıdır.

```
FortiGate-VM64-KVM # config system switch-interface
FortiGate-VM64-KVM (switch-interface) # edit SofSwitInter
new entry 'SofSwitInter' added
FortiGate-VM64-KVM (SofSwitInter) # set vdom root
FortiGate-VM64-KVM (SofSwitInter) # set type switch
FortiGate-VM64-KVM (SofSwitInter) # set member port5 port6
FortiGate-VM64-KVM (SofSwitInter) # end
```

Software Switch 1			
SofSwitInter	Software Switch	port5 port6	0.0.0.0/0.0.0.0

Edit Interface

Name SofSwitInter
Alias
Type Software Switch
VRF ID 0
Interface members port5 port6
Role Undefined

Software Switch özelliği için oluşturulan arayüz üzerinde (web arayüzünde görüldüğü kadarıyla var olan diğer fiziksel arayüzlerde veya oluşturulan sanal arayüzlerde bulunmuyor) SPAN port özelliği de bulunuyor. SPAN port konfigürasyonu için yine “**config system switch-interface**” arayüzü altında “**edit < Software Switch Name>**” komutuyla bir arayüz tanımı yapılması gerekiyor. Bu arayüz altında;

- Arayüzün çalışacağı VDOM “**set vdom <VDOM Name>**” komutuyla belirtilmelidir.
- VDOM tanımı yapıldıktan sonra “**set member <Physical Interface Id’s>**” komutuyla bu arayüze edilecek/kullanılacak fiziksel arayüzlerin eklenmesi gerekiyor (Burada arayüze eklenen fiziksel portlar ilerleyen süreçte kaynak veya hedef SPAN port olarak seçiliyor – Aşağıdaki görselde Port5 ve Port6 gibi).
- Span özelliğini devreye almak için “**set span {enable | disable}**” komutunun kullanılması gerekiyor.
- Span özelliği devreye alındıktan sonra “**set span-source-port <Physical Source Port>**” komutuyla kopyalanacak kaynak port bilgisi, “**set span-dest-port <Physical Destination Port>**” komutuyla trafiğin bir kopyasının gönderileceği hedef port bilgisi tanımlanmalıdır.
- Son adımda “**set span-direction {both | Tx | Rx}**” komutuyla kaynak olarak belirlenen porta sadece giriş yönündeki trafiklerin bir kopyasının mı, sadece çıkış yönündeki trafiklerin bir kopyasının mı yoksa her ikisinin de mi alınacağı belirtilmelidir.

Aşağıda Software Switch için oluşturulan arayüz üzerinde SPAN port özelliği devreye alınmıştır. Ayrıca bir arayüz tanımı oluşturulup bu arayüze farklı fiziksel portlar eklenerek SPAN port özelliği devreye alınabilir (Fiziksel portlar sadece tek bir arayüz tanımına üye olarak eklenebilir).

```

FortiGate-VM64-KVM # config system switch-interface
FortiGate-VM64-KVM (switch-interface) # edit SofSwitInter
FortiGate-VM64-KVM (SofSwitInter) # set vdom root
FortiGate-VM64-KVM (SofSwitInter) # set member port5 port6
FortiGate-VM64-KVM (SofSwitInter) # set span enable
FortiGate-VM64-KVM (SofSwitInter) # set span-source-port port5
FortiGate-VM64-KVM (SofSwitInter) # set span-dest-port port6
FortiGate-VM64-KVM (SofSwitInter) # set span-direction both
FortiGate-VM64-KVM (SofSwitInter) # end

```

☒ SPAN (Port Mirroring)

Source Port port5
Destination Port port6
Direction Both Traffic Out Traffic In

Notlar

- Fiziksel portların arayüzleri altında “**set device-identification {enable |disable}**” komutu kullanılarak bu arayüzlere bağlı cihazlardan pasif tarama ile bilgi toplanması sağlanabilir.

Kaynaklar

- <https://docs.fortinet.com/document/fortigate/6.2.1/cli-reference/7620/system-interface>
- <https://docs.fortinet.com/document/fortigate/6.2.0/new-features/226063/lacp-support-on-entry-level-e-series-devices-6-2-1>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/402940/vlans>
- <https://docs.fortinet.com/document/fortivoice-enterprise/6.4.0/lldp-and-manual-vlan-technical-note/959138/configure-the-vlan-interfaces-on-fortivoice-and-fortigate>
- <https://docs.fortinet.com/document/fortigate/6.2.16/cookbook/265750/configure-loopback-interface>
- <https://docs.fortinet.com/document/fortigate/7.4.3/administration-guide/277799/software-switch>
- <https://community.fortinet.com/t5/FortiGate/Technical-Tip-SPAN-Port-Mirroring-using-ports-associated-to/ta-p/198276>