LAG and InterVLAN Communication

Günümüzde InterVLAN haberleşmesi L3 switch veya routerlar kullanılarak gerçekleştirilebildiği gibi Firewall'lar üzerinden de gerçekleştirilebiliyor. Bu yazıda Fortigate FW üzerinde InterVLAN Communication uygulaması açıklanmaya çalışılacaktır. Uygulama sürecinde Fortigate FW ile Huawei CE6800 model switch kullanılmıştır.

Switch VLAN and LAG Configuration

1- Fortigate üzerinde yapılması gereken tanımlara geçmeden önce Fortigate'e bağlanacak switch üzerinde ilgili VLAN tanımlarının oluşturulması ve ilgili portların bu VLAN'lara dâhil edilmesi gerekiyor.

```
[~CE6800-1]vlan batch 10 20 30
[~CE6800-1]int ge 1/0/10
[~CE6800-1-GE1/0/10]port link-type access
[~CE6800-1-GE1/0/10]port default vlan 10
[~CE6800-1-GE1/0/10]int ge 1/0/11
[~CE6800-1-GE1/0/11]port link-type access
[~CE6800-1-GE1/0/11]port default vlan 20
[~CE6800-1-GE1/0/11]int ge 1/0/12
[~CE6800-1-GE1/0/12]port link-type access
[~CE6800-1-GE1/0/12]port default vlan 30
[~CE6800-1-GE1/0/12]int ge 1/0/13
[~CE6800-1-GE1/0/13]port link-type access
[~CE6800-1-GE1/0/13]port default vlan 10
[~CE6800-1-GE1/0/13]q
```

(Huawei CE6800 model switch üzerinde uygulanan VLAN tanımı verilmiştir).

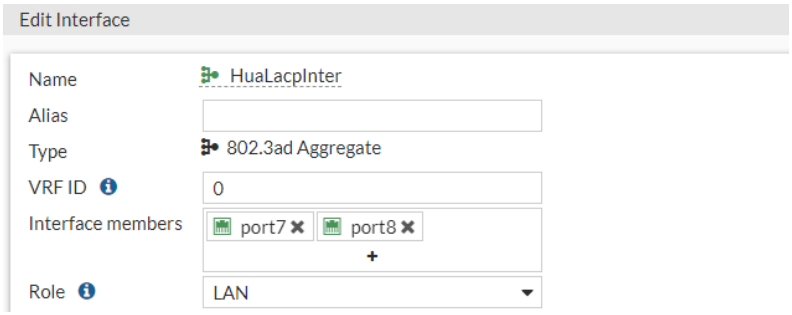
2- Switch ve Fortigate arasında kullanılacak bağlantı üzerinden birçok VLAN'a ait trafik taşınacağı için bu bağlantıların yedekli olması istenir. Bu yedekli yapıyı sağlayabilmek için LAG özelliği kullanılıyor. LAG tanımı için yine switch ve Fortigate arası bağlanacak iki fiziksel port için mantıksal bir arayüz oluşturulur ve bu mantıksal arayüze bağlanacak fiziksel portlar dâhil edilmelidir (Fiziksel portların dâhil edilebilmesi için port altında herhangi bir tanımın bulunmaması gerekiyor. Herhangi bir tanım bulunuyorsa bu tanımların başına "**undo**" kelimesi eklenerek tanımların geri alınması gerekiyor. Aksi takdirde fiziksel portlar Eth-Trunk arayüzü altına dâhil edilemez).

```
[~CE6800-1]int Eth-Trunk 1
[~CE6800-1-Eth-Trunk1]port link-type trunk
[~CE6800-1-Eth-Trunk1]port trunk allow-pass vlan 2 to 4094
Info: Some VLANs are not created. Please create them to make the configuration take effect.
[~CE6800-1-Eth-Trunk1]mode lacp-static
[~CE6800-1-Eth-Trunk1]q
[~CE6800-1]int ge 1/0/0
[~CE6800-1-GE1/0/0]eth-trunk 1
[~CE6800-1-GE1/0/0]int ge 1/0/1
[~CE6800-1-GE1/0/1]eth-trunk 1
[~CE6800-1-GE1/0/1]q
```

(Huawei CE6800 model switch üzerinde uygulanan Eth-Trunk tanımı verilmiştir. Eth-Trunk ile yedekli yapı oluşturulmak istenmediği durumda VLAN tanımlarını Fortigate'e bağlanacak tek bir fiziksel port altında tanımlamak yeterli olacaktır).

Fortigate LAG Configuration

1- Switch üzerinde konfigürasyonlar tamamlandıktan sonra Fortigate üzerinde ayarlamalara başlanabilir. Fortigate üzerinde ilk olarak LAG tanımı yapılması gerekiyor. Bunun için Web arayüzü üzerinde "**Network -> Inerface -> Create New -> Interface**" yolu takip edilerek temelde **Name**, **Type**, **Interface Members** ve **Role** alanlarının doldurulması yeterlidir (altında VLAN tanımları oluşturulacağı için LAG arayüzüne ayrıca ip adresi tanımlamak gerekmiyor). Bu tanımlar komut satırı üzerinde yapılmak istendiğinde aşağıdaki komutlar da uygulanabilir.



(Fortigate Web arayüzü üzerinde LAG tanımını oluşturma)

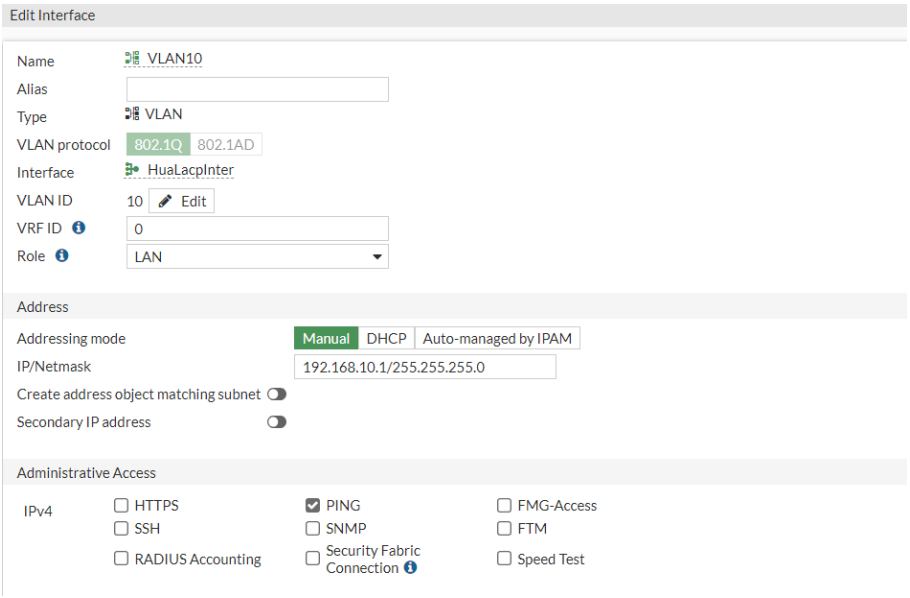
```
FortiGate-VM64-KVM # config system interface

FortiGate-VM64-KVM (interface) # edit HuaLacpInter
new entry 'HuaLacpInter' added

FortiGate-VM64-KVM (HuaLacpInter) # set vdom root

FortiGate-VM64-KVM (HuaLacpInter) # set type aggregate

FortiGate-VM64-KVM (HuaLacpInter) # set member port7 port8

FortiGate-VM64-KVM (HuaLacpInter) # set role lan

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

(Fortigate komut satırı üzerinde LAG tanımını oluşturma)

(LAG tanımı çıktısı)

Fortigate InterVLAN Communication Configuration

1- Link Aggregate tanımı yapıldıktan sonra oluşturulan LAG tanımı altında VLAN'lara hizmet verebilmek için VLAN tanımlarının oluşturulması gerekiyor. Bunun için Web arayüzü üzerinde "**Network -> Inerface -> Create New -> Interface**" yolu takip edilerek temelde **Name**, **Type**, **VLAN Protocol**, **Interface**, **VLAN ID**, **Role** ve **IP/Netmask** kısımlarının ayarlanması gerekiyor (İsteğe bağlı olarak erişimi kontrol edebilmek için Ping paketlerine de izin verilebilir. Interface tanımı VLAN'ın hangi arayüz üzerinden hizmet vereceğini belirlemek için tanımlanıyor. Burada yedekli çalışabilmesi için oluşturduğumuz LAG arayüzü seçilmelidir). Bu tanımlar komut satırı üzerinde yapılmak istendiğinde aşağıdaki komutlar da uygulanabilir.



(Fortigate Web arayüzü üzerinde VLAN tanımını oluşturma)

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

FortiGate-VM64-KVM (interface) # edit VLAN10
new entry 'VLAN10' added

FortiGate-VM64-KVM (VLAN10) # set vdom root

FortiGate-VM64-KVM (VLAN10) # set vlanid 10

FortiGate-VM64-KVM (VLAN10) # set ip 192.168.10.1 255.255.255.0

FortiGate-VM64-KVM (VLAN10) # set allowaccess ping

FortiGate-VM64-KVM (VLAN10) # set role lan

FortiGate-VM64-KVM (VLAN10) # set interface HuaLacpInter

FortiGate-VM64-KVM (VLAN10) # next
```

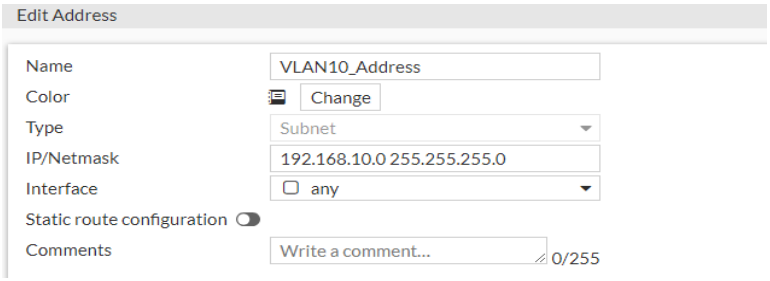
(Fortigate komut satırı üzerinde VLAN tanımını oluşturma)

802.3ad Aggregate 5

fortilink	802.3ad Aggregate		Dedicated to FortiSwitch	PING Security Fabric Connection
HuaLacpInter	802.3ad Aggregate	port7 port8	0.0.0.0/0.0.0.0	
VLAN10	VLAN		192.168.10.1/255.255.255.0	PING
VLAN20	VLAN		192.168.20.1/255.255.255.0	PING
VLAN30	VLAN		192.168.30.1/255.255.255.0	PING

(VLAN tanımını çıktısı)

2- Fortigate üzerinde VLAN tanımları oluşturulduktan sonra VLAN'ların aralarında haberleşebilmeleri için Policy tanımlarının yapılması gerekiyor. Policy tanımında oluşturulan VLAN'ların ip adreslerinin ifade edilebilmesi için "**Policy & Access -> Addresses -> Create New -> Address**" yolu izlenerek adres tanılarının yapılması gerekiyor (Alternatif olarak VLAN tanımları Web arayüzü üzerinde yapılıyorsa VLAN tanımının oluşturulduğu kısımda "**Create address object matching subnet**" özelliği devreye alındığında bu adres tanımı otomatik olarak ekleniyor). Komut satırı üzerinde adres tanımı oluşturulmak istendiğinde aşağıdaki komutlar da uygulanabilir.



(Fortigate Web arayüzü üzerinde Firewall Address tanımını oluşturma)

```
FortiGate-VM64-KVM # config firewall address

FortiGate-VM64-KVM (address) # edit VLAN10_Address
new entry 'VLAN10_Address' added

FortiGate-VM64-KVM (VLAN10_Address) # set type ipmask

FortiGate-VM64-KVM (VLAN10_Address) # set subnet 192.168.10.1/24

FortiGate-VM64-KVM (VLAN10_Address) # next
```

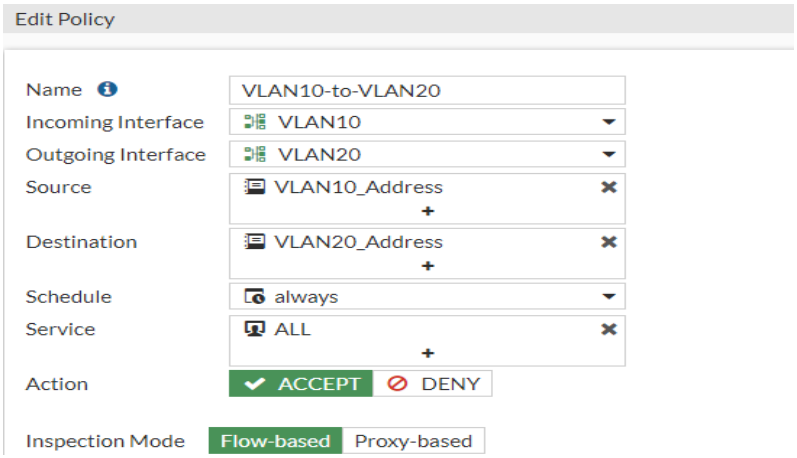
(Fortigate komut satırı üzerinde Firewall Address tanımını oluşturma)

IP Range/Subnet 8	
FABRIC_DEVICE	0.0.0.0/0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210
VLAN10_Address	192.168.10.0/24
VLAN20_Address	192.168.20.0/24
VLAN30_Address	192.168.30.0/24

(Firewall Address tanımını çıktısı)

3- Fortigate'in Firewall Policy tablosunda varsayılanda Implicit Deny satırı olduğu için yapılmak istenen her bir işlem için Policy tanımının yapılması gerekiyor. InterVLAN konfigürasyonu yapmak üzere Policy tanımı oluşturmak için "**Policy & Access –> Firewall Policy -> Create New**" yolu takip edilerek temelde **Name**, **Incoming Interface**, **Outgoing Interface**, **Source Address**, **Destination Address**, **Schedule**, **Service** ve **Action** kısımlarının tanımlanması gerekiyor. Fortigate üzerinde Policy oluşturulurken bilinmesi gereken önemli noktalardan birisi de ip adresi ve arayüz tanımlarından da anlaşılacağı üzere her Policy tek yönlü trafik akışı oluşturabilmek için oluşturuluyor. Yani Net1 ve Net2 olarak varsaydığımız iki networkün karşılıklı olarak haberleşebilmesi için Net1'den Net2'ye trafik akışı için bir Policy tanımı, Net2'den Net1'e trafik akışı için ikinci bir Policy tanımı yapılması gerekiyor.

   a. Burada oluşturulan tanımlarda dikkat edilmesi gereken önemli noktalardan birisi de her bir kural tanımında hedef ve kaynak network adresleri tek olmalıdır. Tek bir kural tanımı içerisinde birden fazla kaynak ve hedef network tanımları kullanılarak Policy tanımları yapıldığı takdirde Policy tanımı sayısı arttıkça yönetimi de zorlaştıracaktır. **Örnek üzerinden hatalı tanım açıklanmaya çalışıldığında** oluşturulan Policy tanımında kaynak network adres tanımı olarak VLAN10_Address, VLAN20_Address ve VLAN30_Address tanımları aynı ada eklenebilir. Aynı şekilde hedef network adres kısmına da VLAN10_Address, VLAN20_Address ve VLAN30_Address tanımları eklenerek tek bir Policy üzerinden bütün VLAN'ların aralarında haberleşmesi sağlanabilirdi.



(Fortigate Web arayüzü üzerinde Firewall Policy tanımını oluşturma)

```
FortiGate-VM64-KVM # config firewall policy
FortiGate-VM64-KVM (policy) # edit 1
new entry '1' added

FortiGate-VM64-KVM (1) # set name VLAN10-to-VLAN20

FortiGate-VM64-KVM (1) # set srcintf VLAN10

FortiGate-VM64-KVM (1) # set dstintf VLAN20

FortiGate-VM64-KVM (1) # set action accept

FortiGate-VM64-KVM (1) # set srcaddr VLAN10_Address

FortiGate-VM64-KVM (1) # set dstaddr VLAN20_Address

FortiGate-VM64-KVM (1) # set schedule always

FortiGate-VM64-KVM (1) # set service ALL

FortiGate-VM64-KVM (1) # next

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

FortiGate-VM64-KVM (2) # set name VLAN20-to-VLAN10

FortiGate-VM64-KVM (2) # set srcintf VLAN20

FortiGate-VM64-KVM (2) # set dstintf VLAN10

FortiGate-VM64-KVM (2) # set action accept

FortiGate-VM64-KVM (2) # set srcaddr VLAN20_Address

FortiGate-VM64-KVM (2) # set dstaddr VLAN10_Address

FortiGate-VM64-KVM (2) # set schedule always

FortiGate-VM64-KVM (2) # set service ALL

FortiGate-VM64-KVM (2) # next

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

(Fortigate komut satırı üzerinde Firewall Policy tanımını oluşturma)

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
VLAN10 → VLAN20 1									
VLAN10-to-VLAN20	VLAN10_Address	VLAN20_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN20 → VLAN10 1									
VLAN20-to-VLAN10	VLAN20_Address	VLAN10_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit 1									
Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

(Firewall Policy tanımını çıktısı)

Gerçekleştirdiğimiz uygulamada 3 VLAN'ı arasında haberleştirebilmek için aşağıda da görüleceği üzere toplamda 6 adet Policy tanımı oluşturulmuştur.

Name	Source	Destination	Schedule	Service	Action	NAT	Security Profiles	Log	Bytes
VLAN10 → VLAN20 1									
VLAN10-to-VLAN20	VLAN10_Address	VLAN20_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN10 → VLAN30 1									
VLAN10-to-VLAN30	VLAN10_Address	VLAN30_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN20 → VLAN10 1									
VLAN20-to-VLAN10	VLAN20_Address	VLAN10_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN20 → VLAN30 1									
VLAN20-to-VLAN30	VLAN20_Address	VLAN30_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN30 → VLAN10 1									
VLAN30-to-VLAN10	VLAN30_Address	VLAN10_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
VLAN30 → VLAN20 1									
VLAN30-to-VLAN20	VLAN30_Address	VLAN20_Address	always	ALL	ACCEPT	Disabled	SSL no-inspection	UTM	0 B
Implicit 1									
Implicit Deny	all	all	always	ALL	DENY			Disabled	0 B

Kaynaklar

- https[:]//community.fortinet.com/t5/FortiGate/Technical-Tip-Configure-Inter-VLAN-Routing/ta-p/275524