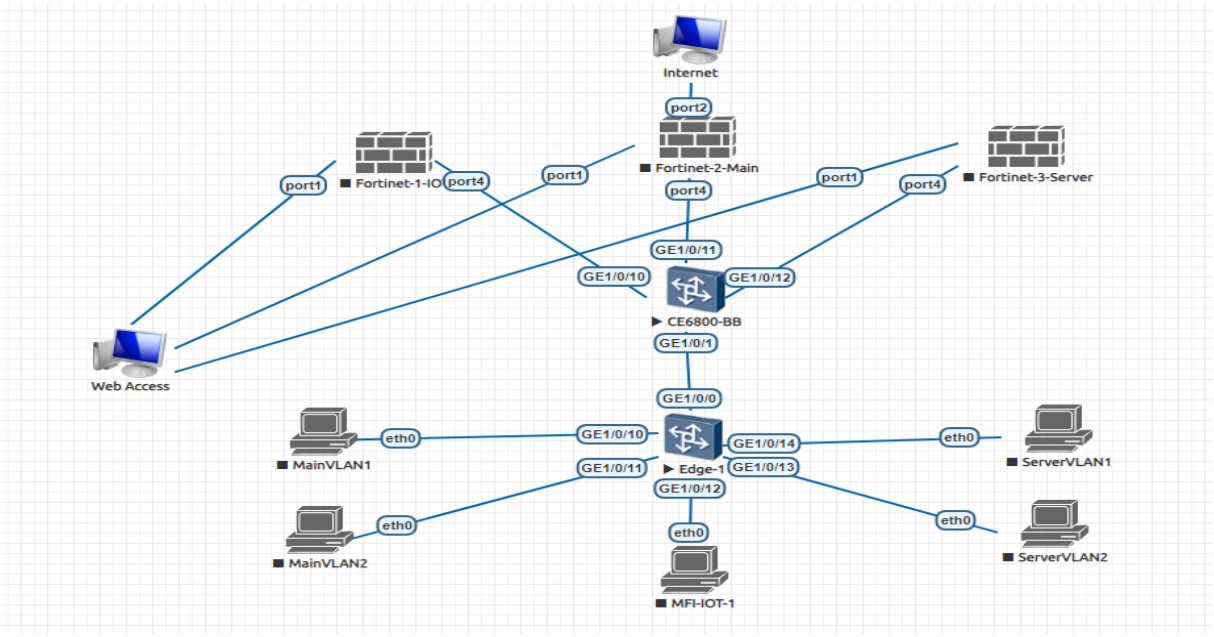
FW MGMT Configuration

Büyük topolojilerde yapıyı daha düzenli yönetebilmek için LAN içerisinde birden fazla FW kullanılması gerekebiliyor. Bu gibi yapılarda her FW'a farklı bir misyon yüklenerek iş yükü paylaştırılır. Örnek olarak sunucu tabanlı çalışan sistemleri diğer sistemlerden ayırabilmek ve sunuculara erişimi sürecini daha etkili yönetebilmek için farklı bir FW üzerinde konumlandırılabilir. Benzer şekilde IOT cihazların erişimlerini yönetmek için ayrıca bir FW konumlandırılabilir. Dolayısıyla LAN içerisinde kullanılan VLAN arayüzlerinin farklı FW'lar üzerinde tanımlanması gerekecektir. Bu durumda InterVLAN haberleşme sürecini yönetebilmek veya VLAN'ları internet ortamına çıkarabilmek için FW'lar arasında bağlantılara ihtiyaç duyulacaktır.

FW portları sınırlı olduğu için bazı durumlarda FW'lar arasında doğrudan bağlantı kurabilmek pek mümkün olmayabiliyor. Bu durumda haberleşme süreci bir L2 swtich kullanarak gerçekleştiriliyor. Bu yazıda aşağıdaki görselden de anlaşılacağı üzere 3 farklı FW üzerindeki VLAN'ların aralarında haberleşme sürecini bir yönetim arayüzü oluşturularak nasıl gerçekleştirildiği açıklamaya çalışılacaktır.



Bu yapıda FW'lar üzerinde oluşturulan VLAN tanımları aşağıdaki gibi olacaktır;

- Fortigate-1-IOT
  - IOT-1 -> VLAN 10 –> 10.10.1.1/24
  - FW_MGMT -> VLAN 220 –> 10.10.220.1/24
- Fortigate-2-Main
  - MainVLAN1 -> VLAN 20 –> 10.10.2.1/24
  - MainVLAN2 -> VLAN 30 –> 10.10.3.1/24
  - FW_MGMT -> VLAN 220 –> 10.10.220.2/24
  - Internet-Connection -> 33.33.33.33/32
- Fortigate-3-Server
  - ServerVLAN1 -> VLAN 40 –> 10.10.4.1/24
  - ServerVLAN2 -> VLAN 50 –> 10.10.5.1/24
  - FW_MGMT -> VLAN 220 –> 10.10.220.3/24

Lab ortamını kurulum sürecinde FW'lar üzerinde VLAN tanımlamaları yapılmalıdır. Özetle FW'lar üzerinde uygulanması gereken komutlar aşağıdaki gibi olmalıdır.

```
config system global
set hostname Fortigate-1-IOT
end

config system interface
edit IOT-1
set vdom root
set interface port4
set type vlan
set vlanid 10
set mode static
set ip 10.10.1.1 255.255.255.0
set allowaccess ping
next
edit FW_MGMT
set vdom root
set interface port4
set type vlan
set vlanid 220
set mode static
set ip 10.10.220.1 255.255.255.0
set allowaccess ping
end
```

```
config system global
set hostname Fortigate-2-Main
end

config system interface
edit MainVLAN1
set vdom root
set interface port4
set type vlan
set vlanid 20
set mode static
set ip 10.10.2.1 255.255.255.0
set allowaccess ping
next
edit MainVLAN2
set vdom root
set interface port4
set type vlan
set vlanid 30
set mode static
set ip 10.10.3.1 255.255.255.0
set allowaccess ping
next
edit FW_MGMT
set vdom root
set interface port4
set type vlan
set vlanid 220
set mode static
set ip 10.10.220.2 255.255.255.0
set allowaccess ping
end
```

```
config system global
set hostname Fortigate-3-Server
end

config system interface
edit ServerVLAN1
set vdom root
set interface port4
set type vlan
set vlanid 40
set mode static
set ip 10.10.4.1 255.255.255.0
set allowaccess ping
next
edit ServerVLAN2
set vdom root
set interface port4
set type vlan
set vlanid 50
set mode static
set ip 10.10.5.1 255.255.255.0
set allowaccess ping
next
edit FW_MGMT
set vdom root
set interface port4
set type vlan
set vlanid 220
set mode static
set ip 10.10.220.3 255.255.255.0
set allowaccess ping
end
```

FW üzerindeki tanımlamalar tanımlandıktan sonra BB ve Edge switch üzerinde de her bir VLAN tanımını yapılmalıdır. Switchler arasındaki portlar Trunk moda alınarak izin verilecek VLAN'lar belirtilmelidir. Benzer şekilde BB switch iler FW'lar arasındaki bağlantılar da Trunk moduna alınarak geçirilecek VLAN'lar belirtilmelidir. Son adımda Edge switch portlarına bağlı istemcileri ilgili VLAN'lara dâhil etmelisin. Özetle switchler üzerinde uygulanması gereken komutlar aşağıdaki gibi olmalıdır.

```
[~CE6800-BB]vlan 10
[~CE6800-BB-vlan10]description IOT-1
[~CE6800-BB-vlan10]vlan 20
[~CE6800-BB-vlan20]description MainVLAN1
[~CE6800-BB-vlan20]vlan 30
[~CE6800-BB-vlan30]description MainVLAN2
[~CE6800-BB-vlan30]vlan 40
[~CE6800-BB-vlan40]description ServerVLAN1
[~CE6800-BB-vlan40]vlan 50
[~CE6800-BB-vlan50]description ServerVLAN2
[~CE6800-BB-vlan50]vlan 220
[~CE6800-BB-vlan220]description FW_MGMT
[~CE6800-BB-vlan220]quit
[~CE6800-BB]
[~CE6800-BB]int g 1/0/10
[~CE6800-BB-GE1/0/10]port link-type trunk
[~CE6800-BB-GE1/0/10]port trunk allow-pass vlan 10 220
[~CE6800-BB-GE1/0/10]quit
[~CE6800-BB]int g 1/0/11
[~CE6800-BB-GE1/0/11]port link-type trunk
[~CE6800-BB-GE1/0/11]port trunk allow-pass vlan 20 30 220
[~CE6800-BB-GE1/0/11]quit
[~CE6800-BB]int g 1/0/12
[~CE6800-BB-GE1/0/12]port link-type trunk
[~CE6800-BB-GE1/0/12]port trunk allow-pass vlan 40 50 220
[~CE6800-BB-GE1/0/12]quit
[~CE6800-BB]
[~CE6800-BB]int g 1/0/1
[~CE6800-BB-GE1/0/1]port link-type trunk
[~CE6800-BB-GE1/0/1]port trunk allow-pass vlan 10 20 30 40 50
[~CE6800-BB-GE1/0/1]quit
[~CE6800-BB]commit
```

```
[~Edge-1]vlan 10
[~Edge-1-vlan10]description IOT-1
[~Edge-1-vlan10]vlan 20
[~Edge-1-vlan20]description MainVLAN1
[~Edge-1-vlan20]vlan 30
[~Edge-1-vlan30]description MainVLAN2
[~Edge-1-vlan30]vlan 40
[~Edge-1-vlan40]description ServerVLAN1
[~Edge-1-vlan40]vlan 50
[~Edge-1-vlan50]description ServerVLAN2
[~Edge-1-vlan50]quit
[~Edge-1]
[~Edge-1]int g 1/0/0
[~Edge-1-GE1/0/0]port link-type trunk
[~Edge-1-GE1/0/0]port trunk allow-pass vlan 10 20 30 40 50
[~Edge-1-GE1/0/0]quit
[~Edge-1]
[~Edge-1]int g 1/0/10
[~Edge-1-GE1/0/10]port link-type access
[~Edge-1-GE1/0/10]port default vlan 20
[~Edge-1-GE1/0/10]quit
[~Edge-1]int g 1/0/11
[~Edge-1-GE1/0/11]port link-type access
[~Edge-1-GE1/0/11]port default vlan 30
[~Edge-1-GE1/0/11]quit
[~Edge-1]int g 1/0/12
[~Edge-1-GE1/0/12]port link-type access
[~Edge-1-GE1/0/12]port default vlan 10
[~Edge-1-GE1/0/12]quit
[~Edge-1]int g 1/0/13
[~Edge-1-GE1/0/13]port link-type access
[~Edge-1-GE1/0/13]port default vlan 50
[~Edge-1-GE1/0/13]quit
[~Edge-1]int g 1/0/14
[~Edge-1-GE1/0/14]port link-type access
[~Edge-1-GE1/0/14]port default vlan 40
[~Edge-1-GE1/0/14]quit
[~Edge-1]commit
```

Bu tanımlar yapıldıktan sonra artık VLAN'lar arası haberleşme sürecinin nasıl gerçekleştirileceğini açıklamaya başlayabiliriz.

Topolojiden den anlaşılacağı üzere bütün trafik BB switch üzerinden akmaktadır. Kenar switch portlarında gerçekleştirilen VLAN atamaları BB switch üzerine geldiğinde VLAN arayüzü hangi FW üzerinde tanımlıysa o portu üzerinden ilgili FW'a yönlendiriliyor.

Farklı FW üzerinde bulunan VLAN'ların aralarında haberleşmesi gerektiğinde trafiği FW'lar arasında taşıyabilmek için FW'lar üzerinde ayrıca bir VLAN tanımı yapılması gerekiyor. Biz yazımızda bu VLAN'a FW_MGMT VLAN diyeceğiz. FW_MGMT VLAN'ı FW'lar arasında trafiği aktarmak için ara VLAN görevi görecektir. Bu yapıyı bir örnek üzerinden açıklamak gerekirse;

- MainVLAN1 VLAN'ında bulunan istemci ServerVLAN2 VLAN'ındaki istemciye erişmesi gerektiğinde yapılması gereken birkaç adım bulunuyor. Bu adımlar;
  - İlk adımda Fortigate-2-Main FW üzerinde tanımlanacak Policy'lerde kullanılmak üzere Ip adres tanımlarının yapılması gerekiyor.

```
Fortigate-2-Main (address) # edit MainVLAN1_Addr
new entry 'MainVLAN1_Addr' added

Fortigate-2-Main (MainVLAN1_Addr) # set type ipmask

Fortigate-2-Main (MainVLAN1_Addr) # set subnet 10.10.2.1/24

Fortigate-2-Main (MainVLAN1_Addr) # next

Fortigate-2-Main (address) # edit ServerVLAN2_Addr
new entry 'ServerVLAN2_Addr' added

Fortigate-2-Main (ServerVLAN2_Addr) # set type ipmask

Fortigate-2-Main (ServerVLAN2_Addr) # set subnet 10.10.5.1/24

Fortigate-2-Main (ServerVLAN2_Addr) # end
```

```
Fortigate-3-Server (address) # edit MainVLAN1_Addr
new entry 'MainVLAN1_Addr' added

Fortigate-3-Server (MainVLAN1_Addr) # set type ipmask

Fortigate-3-Server (MainVLAN1_Addr) # set subnet 10.10.2.1/24

Fortigate-3-Server (MainVLAN1_Addr) # next

Fortigate-3-Server (address) # edit ServerVLAN2_Addr
new entry 'ServerVLAN2_Addr' added

Fortigate-3-Server (ServerVLAN2_Addr) # set type ipmask

Fortigate-3-Server (ServerVLAN2_Addr) # set subnet 10.10.5.1/24

Fortigate-3-Server (ServerVLAN2_Addr) # end
```

  - Adres tanımları yapıldıktan sonra Fortigate-2-Main üzerinde MainVLAN1 VLAN'dan FW_MGMT VLAN'a doğru Policy tanımı yapılması gerekiyor (Eğer ki istemcilerin arasında karşılıklı haberleşmesi isteniyorsa bu Policy'nin tersi de oluşturulmalıdır). Burada kaynak ip adresi MainVLAN1 VLAN adresi olurken hedef ip adresi ServerVLAN2 VLAN adresi olarak belirlenmelidir.

```
Fortigate-2-Main # config firewall policy

Fortigate-2-Main (policy) # edit 10
new entry '10' added

Fortigate-2-Main (10) # set name MVLAN1_to_SVLAN2

Fortigate-2-Main (10) # set srcintf MainVLAN1

Fortigate-2-Main (10) # set dstintf FW_MGMT

Fortigate-2-Main (10) # set srcaddr MainVLAN1_Addr

Fortigate-2-Main (10) # set dstaddr ServerVLAN2_Addr

Fortigate-2-Main (10) # set action accept

Fortigate-2-Main (10) # set schedule always

Fortigate-2-Main (10) # set service ALL

Fortigate-2-Main (10) # next
```

```
Fortigate-2-Main (policy) # edit 11
new entry '11' added

Fortigate-2-Main (11) # set name SVLAN2_to_MVLAN1

Fortigate-2-Main (11) # set srcintf FW_MGMT

Fortigate-2-Main (11) # set dstintf MainVLAN1

Fortigate-2-Main (11) # set srcaddr ServerVLAN2_Addr

Fortigate-2-Main (11) # set dstaddr MainVLAN1_Addr

Fortigate-2-Main (11) # set action accept

Fortigate-2-Main (11) # set schedule always

Fortigate-2-Main (11) # set service ALL

Fortigate-2-Main (11) # end
```

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
MVLAN1_to_SVLAN2	MainVLAN1	FW_MGMT	MainVLAN1_Addr	ServerVLAN2_Addr	always	ALL	ACCEPT	Disabled
SVLAN2_to_MVLAN1	FW_MGMT	MainVLAN1	ServerVLAN2_Addr	MainVLAN1_Addr	always	ALL	ACCEPT	Disabled
Implicit Deny	any	any	all	all	always	ALL	DENY	

- Policy tanımı yapıldıktan sonra Fortigate-2-Main FW'dan 10.10.5.1/24 (ServerVLAN2) hedef adresine doğru Static Route tanımı yapılması gerekiyor. Burada Gateway adresi olarak Fortigate-3-Server FW'un FW_MGMT adresi yazılmalıdır (Bu durumda FW_MGMT arayüzünü kendiliğinden seçecektir). Bu tanımla beraber Fortigate-2-Main FW üzerinde yapılması gereken tanımlar tamamlanacaktır.

```
Fortigate-2-Main # config router static

Fortigate-2-Main (static) # edit 1
new entry '1' added

Fortigate-2-Main (1) # set dst 10.10.5.1/24

Fortigate-2-Main (1) # set gateway 10.10.220.3

Fortigate-2-Main (1) # set device FW_MGMT

Fortigate-2-Main (1) # end
```

Destination	Gateway IP	Interface	Status
10.10.5.0/24	10.10.220.3	FW_MGMT	Enabled

- Fortigate-2-Main FW üzerinde yapılması gereken tanımlamaları tamamladıktan sonra Fortigate-3-Server üzerinde öncelikle ServerVLAN2 ve MainVLAN1 VLAN için adres tanımlarının yapılması gerekiyor.

```
Fortigate-3-Server (address) # edit MainVLAN1_Addr
new entry 'MainVLAN1_Addr' added

Fortigate-3-Server (MainVLAN1_Addr) # set type ipmask

Fortigate-3-Server (MainVLAN1_Addr) # set subnet 10.10.2.1/24

Fortigate-3-Server (MainVLAN1_Addr) # next

Fortigate-3-Server (address) # edit ServerVLAN2_Addr
new entry 'ServerVLAN2_Addr' added

Fortigate-3-Server (ServerVLAN2_Addr) # set type ipmask

Fortigate-3-Server (ServerVLAN2_Addr) # set subnet 10.10.5.1/24

Fortigate-3-Server (ServerVLAN2_Addr) # end
```

- Adres tanımları yapıldıktan sonra FW_MGMT VLAN'dan ServerVLAN2 VLAN'a doğru Policy tanımı yapılması gerekiyor (Eğer ki istemcilerin arasında karşılıklı haberleşmesi isteniyorsa bu Policy'nin tersi de oluşturulmalıdır). Burada kaynak ip adresi ServerVLAN2 VLAN adresi olurken hedef ip adresi MainVLAN1 VLAN adresi olarak belirlenmelidir.

```
Fortigate-3-Server # config firewall policy

Fortigate-3-Server (policy) # edit 10
new entry '10' added

Fortigate-3-Server (10) # set name SVLAN2_to_MVLAN1

Fortigate-3-Server (10) # set srcintf ServerVLAN2

Fortigate-3-Server (10) # set dstintf FW_MGMT

Fortigate-3-Server (10) # set srcaddr ServerVLAN2_Addr

Fortigate-3-Server (10) # set dstaddr MainVLAN1_Addr

Fortigate-3-Server (10) # set action accept

Fortigate-3-Server (10) # set schedule always

Fortigate-3-Server (10) # set service ALL

Fortigate-3-Server (10) # next
```

```
Fortigate-3-Server (policy) # edit 11
new entry '11' added

Fortigate-3-Server (11) # set name MVLAN1_to_SVLAN2

Fortigate-3-Server (11) # set srcintf FW_MGMT

Fortigate-3-Server (11) # set dstintf ServerVLAN2

Fortigate-3-Server (11) # set srcaddr MainVLAN1_Addr

Fortigate-3-Server (11) # set dstaddr ServerVLAN2_Addr

Fortigate-3-Server (11) # set action accept

Fortigate-3-Server (11) # set schedule always

Fortigate-3-Server (11) # set service ALL

Fortigate-3-Server (11) # end
```

Name	From	To	Source	Destination	Schedule	Service	Action	NAT
SVLAN2_to_MVLAN1	ServerVLAN2	FW_MGMT	ServerVLAN2_Addr	MainVLAN1_Addr	always	ALL	ACCEPT	Disabled
MVLAN1_to_SVLAN2	FW_MGMT	ServerVLAN2	MainVLAN1_Addr	ServerVLAN2_Addr	always	ALL	ACCEPT	Disabled
Implicit Deny	any	any	all	all	always	ALL	DENY	

- Son adımda ise Fortigate-3-Server FW'dan 10.10.2.1/24 (MainVLAN1) hedef adresine doğru Static Route tanımı yapılması gerekiyor. Burada Gateway adresi olarak Fortigate-2-Main FW'un FW_MGMT adresi yazılmalıdır (Bu durumda FW_MGMT arayüzünü kendiliğinden seçecektir).

```
Fortigate-3-Server # config router static

Fortigate-3-Server (static) # edit 1
new entry '1' added

Fortigate-3-Server (1) # set dst 10.10.2.1/24

Fortigate-3-Server (1) # set gateway 10.10.220.2

Fortigate-3-Server (1) # set device FW_MGMT

Fortigate-3-Server (1) # end
```

Destination	Gateway IP	Interface	Status
10.10.2.0/24	10.10.220.2	FW_MGMT	Enabled

SONUÇ;