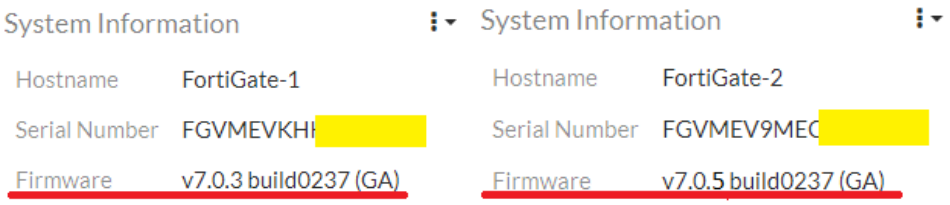
HA Configüration and Firmware Update

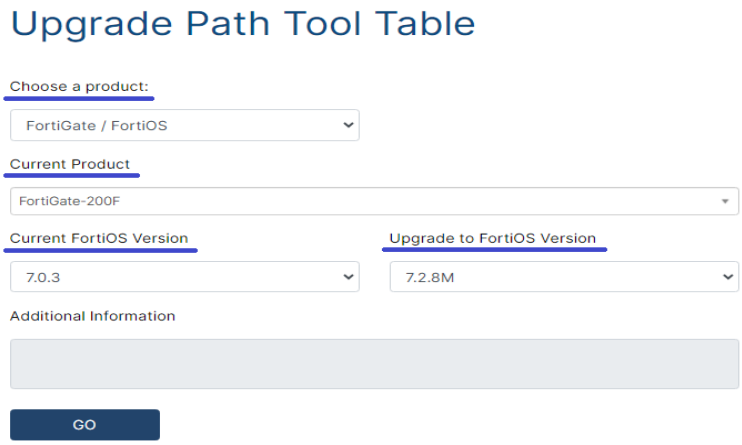
Network üzerinde kullanılan her çözümde olduğu gibi Fortigate cihazların da yedekliii çalışması istenmektedir. Fortigate cihazların aralarında yedekli çalışabilmesi için aralarında HA konfigürasyonu yapılması gerekiyor.

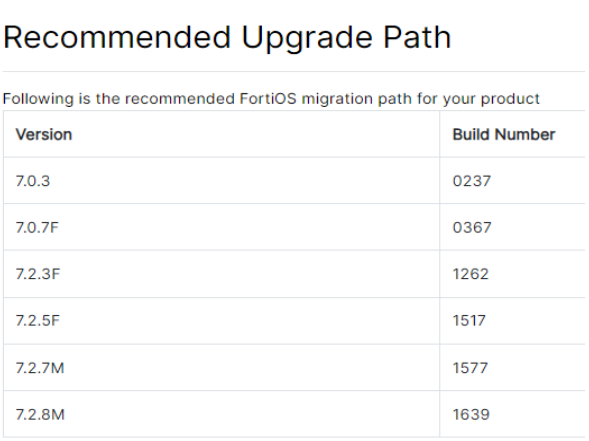
HA konfigürasyonuna başlamadan önce herhangi bir problemle karşılaşılma ihtimaline karşı cihazların yedekleri alınmalıdır. Yedekler alındıysa artık HA konfigürasyonuna başlanabilir.

- Cihazların yedekleri alındıktan sonra göz önünde bulundurulması gereken ilk koşul HA konfigürasyonu yapılacak cihazların model ve Firmware sürümlerinin aynı olmasıdır.
    - Modelleri aynı olmayan cihazlar arasında HA yapı oluşturulamaz.
    - Eğer ki HA yapılacak cihazların modelleri aynı ama üzerinde çalışan **Firmware sürümleri farklıysa** HA konfigürasyonu öncesinde cihazların Firmware sürümlerini ortak tek bir sürüme getirilmelidir (“**Dashboard -> Status –> System Information**” kısmında veya “**System -> Firmware –> Firmware Management**” yolunu izleyerek cihaz üzerinde hali hazırda çalışan Firmware sürümünü öğrenebilirsin).

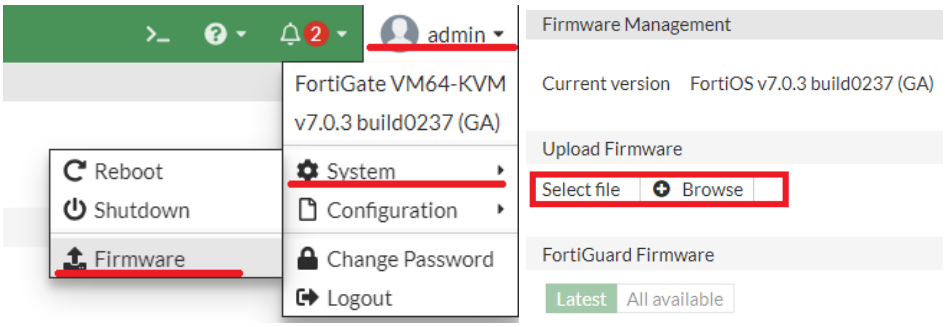


- Cihazlar üzerinde çalışan Firmware sürümlerini ortak tek bir sürüm getirebilmek için cihazlar üzerinde çalışan konfigürasyon olup olmadığına bakılır.
    - **Cihaz üzerinde hali hazırda tanımlı konfigürasyon bulunmuyorsa** yükseltilmek veya düşürülmek istenen Firmware sürümü doğrudan yüklenebilir.
    - **Cihaz üzerinde hali hazırda tanımlı konfigürasyon bulunuyorsa** bu durumda Firmware geçişlerinin sıralı bir şekilde yapılması gerekiyor. Aksi takdirde Firmware geçişinde cihaz üzerinde çalışan konfigürasyonlarda bozulmalar gözlemlenebiliyor. İstenilen Firmware sürümüne hangi adımlar üzerinden geçiş yapılabileceğini öğrenmek için Fort Support sayfasında “**Upgrade Path Tool**” kısmına güncellenmek istenen cihazın modeli, hali hazırda üzerinde çalışan Firmware sürümü ve yükseltilmek (veya düşürülmek) istenen Firmware sürümü tanımlanarak bu süreçte izlenmesi gereken yol haritası takip edilmelidir.

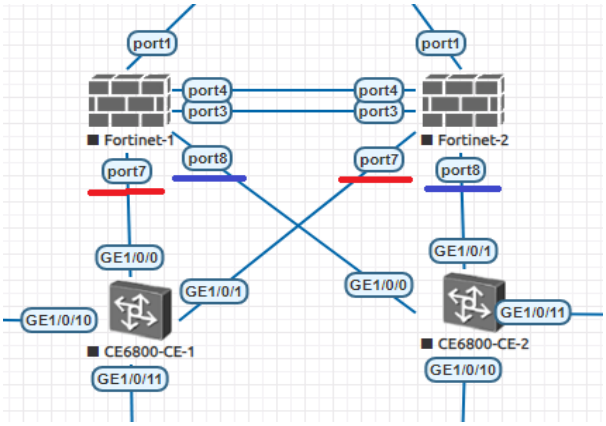




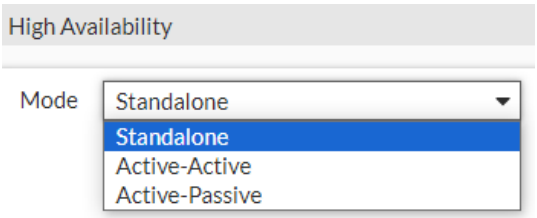
Cihazların Firmware sürümünü güncellemek için Fortinet Support hesabına giriş yapılmalıdır. Burada yüklenecek Firmware sürümlerine dair dosyaları bilgisayarınıza indirildikten sonra "**Admin -> System -> Firmware**" veya "**System -> Firmware –> Firmware**" yolu takip edilerek Firmware Management sayfasına geçilir. Firmware Management sayfasında "**Upload Firmware -> Select File –> Browse**" yolu takip edilerek bilgisayara indirilen Firmware dosyası seçilir ve güncelleme işlemine başlanır.



- HA yapılacak cihazar atnı Firmware sürümüne getirildikten sonra HA konfigürasyonuna başlanabilir. Cihazlar arasında HA yapılacak portlar arasında fizikesel bağlantı/kablolama yapılmalıdır. Cihazları birbirine bağlarken;
    - Cihazlar konum olarak birbirine yakınsa HA konfigürasyonu için Fortigate cihazların üzerinde bu iş için adanmış bakır HA portları kullanılabilmektedir.
    - Cihazlar konum olarak birbirine uzaksa bu durumunda HA konfigürasyonu için cihaz üzerindeki fiber portlar kullanılıyor.
- Burada **UNUTULMAMALIDIR Kİ** aralarında HA yapılacak cihazların portlarındaki bağlantılar da simetrik olacak şekilde aynı bağlanmalıdır (Örnek bağlantı şekli aşağıdaki görselde ifade edilmeye çalışılmıştır).

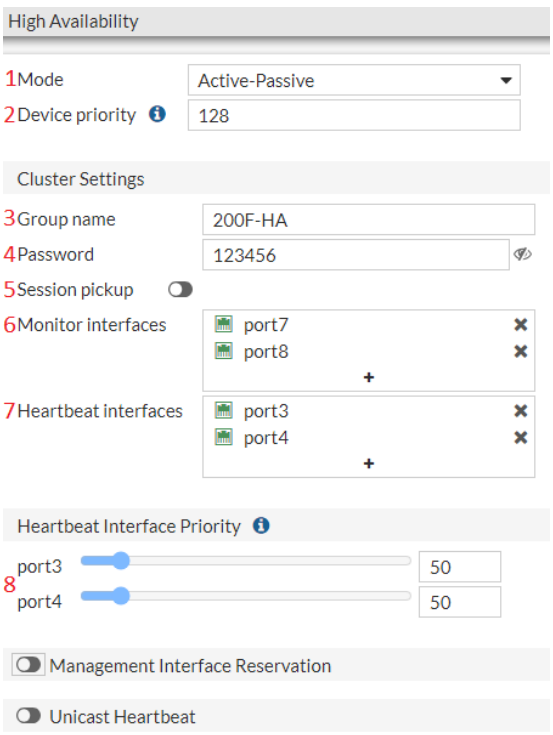


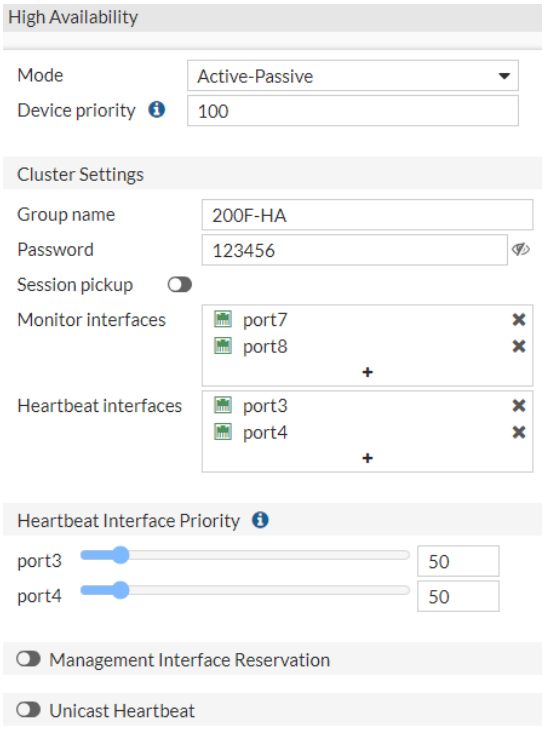
- Cihazlar arasındaki fiziksel bağlantı sağlandıktan sonra web arayüzünde "**System –> HA**" yolu takip edilmelidir. Burada ilk olarak cihazlar arasında kurulacak HA modu belirlenmelidir (Bu yazıda Active-Passive modunda konfigüre edilecektir).
    - **Standalone**, varsayılanda gelen moddur. Cihazın yedeksiz çalışması istendiğinde seçilir.
    - **Active-Passive**, cihazlardan birinin aktifliği alarak hizmet verdiği, diğerinin ise pasif duruma geçerek aktif seçilen cihazın durumunu izler. Bu süreçte aktif durumdaki cihaz üzerindeki değişimleri/güncellemeleri anlık olarak almaya devam eder. Aktif cihaz üzerinde bir hizmet kesintisi olduğunda pasif durumdaki cihaz aktifliği alarak hizmet vermeye devam eder.
    - **Active-Active**, HA yapı ile yedeklenen her cihazın aktif şekilde hizmet verdiği ve trafiğin yedeklenen cihazlar arasında paylaştırıldığı moddur.



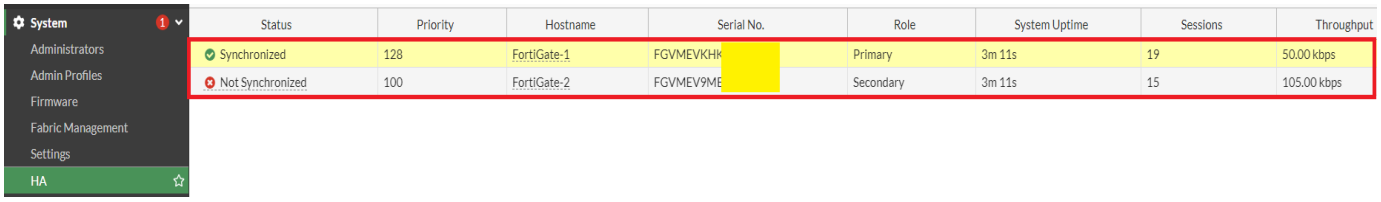
Kullanılacak HA modu seçildikten sonra;

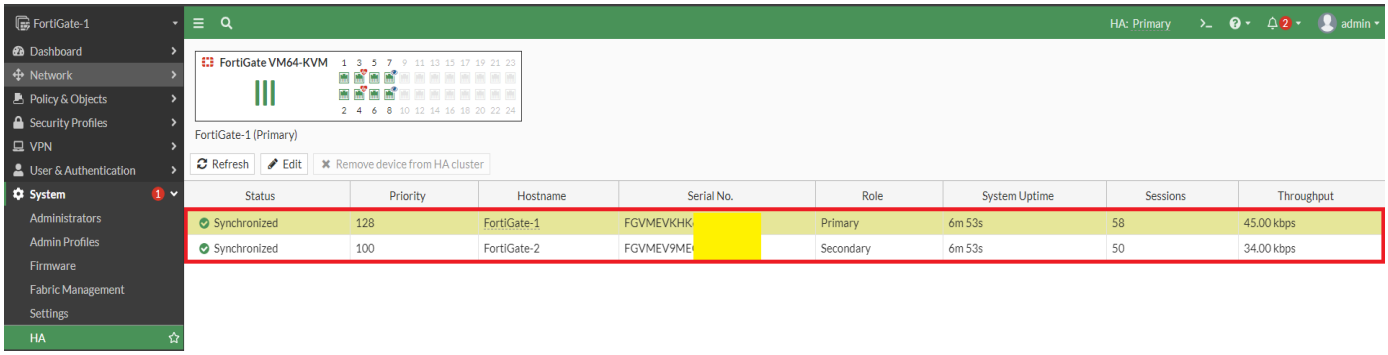
1- Seçilen HA modu görünmektedir.
2- HA yapıda cihazlar arasında aktifliği hangi cihazın alması isteniyorsa onun Priority değeri diğer cihaza kıyasla daha yüksek verilir (Bu değer varsayılanda 128 geliyor). Eğer ki bu değer varsayılan ayarında bırakılırsa Seri numarası yüksek olan cihaz aktif olarak seçilecektir (https[:]//community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-HA-Primary-unit-selection-process-when/ta-p/249745).
3- Bir grup adı tanımlanmalıdır. Buradaki grup adı HA yapılacak bütün cihazlarda aynı girilmelidir.
4- HA yapılan cihazlar arasında kullanılmak üzere bir parola tanımı yapılmalıdır. Burada tanımlanan parola bilgisi de HA yapılacak bütün cihazlarda aynı girilmelidir.
5- Aktif seçilen cihazda bir kesinti olması durumunda pasif durumdaki cihazın devreye alınması sürecinde mevcut oturumlarda kesinti olmadan veya en az kesintiyle aktifliği devralacak cihaza aktarılmasını sağlayan özelliktir.
6- HA yapılan cihazların üzerinde yedeklenmesi istenen arayüzler seçilmelidir. Eğer seçilen interface'lerden biri aktif cihaz üzerinde Down olursa Pasif cihaz ilgili arayüzün trafik yükünü devralır ve böylece ilgili arayüzün trafik akışı kesintisiz şekilde devam eder.
7- HA yapılan cihazların aralarında haberleşmesi için kullanılacak (HA Portları) portlar seçilmelidir.
8- HA portları da yedekli olacak şekilde ayarlanır. HA sürecinde bu bağlantıların ikisi de aktif kullanılmamaktadır. Dolayısıyla bu bağlantılar arasında da öncelik tanımı yapılabiliyor.





Konfigürasyon sonrasında Priority değeri yüksek verilen cihaz üzerinde “System -> HA” sekmesi altında her iki cihaz da gözlemlenebilir. Burada HA uygulanan cihazlar arasında senkronize olabilmesi biraz zaman alabiliyor. Cihazlar senkronize olduktan sonra Slave/Passive seçilen cihaza Console portu dışında erişim sağlanamayacağı bilinmelidir.





HA konfigürasyonu komut satırı üzerinden yapılmak istendiğinde temelde aşağıdaki komutları kullanmak yeteri olacaktır. Konfigürasyon sonrasında Slave/Passive moduna geçecek cihazın konsolunda aşağıdaki gibi çıktılar görülecektir.

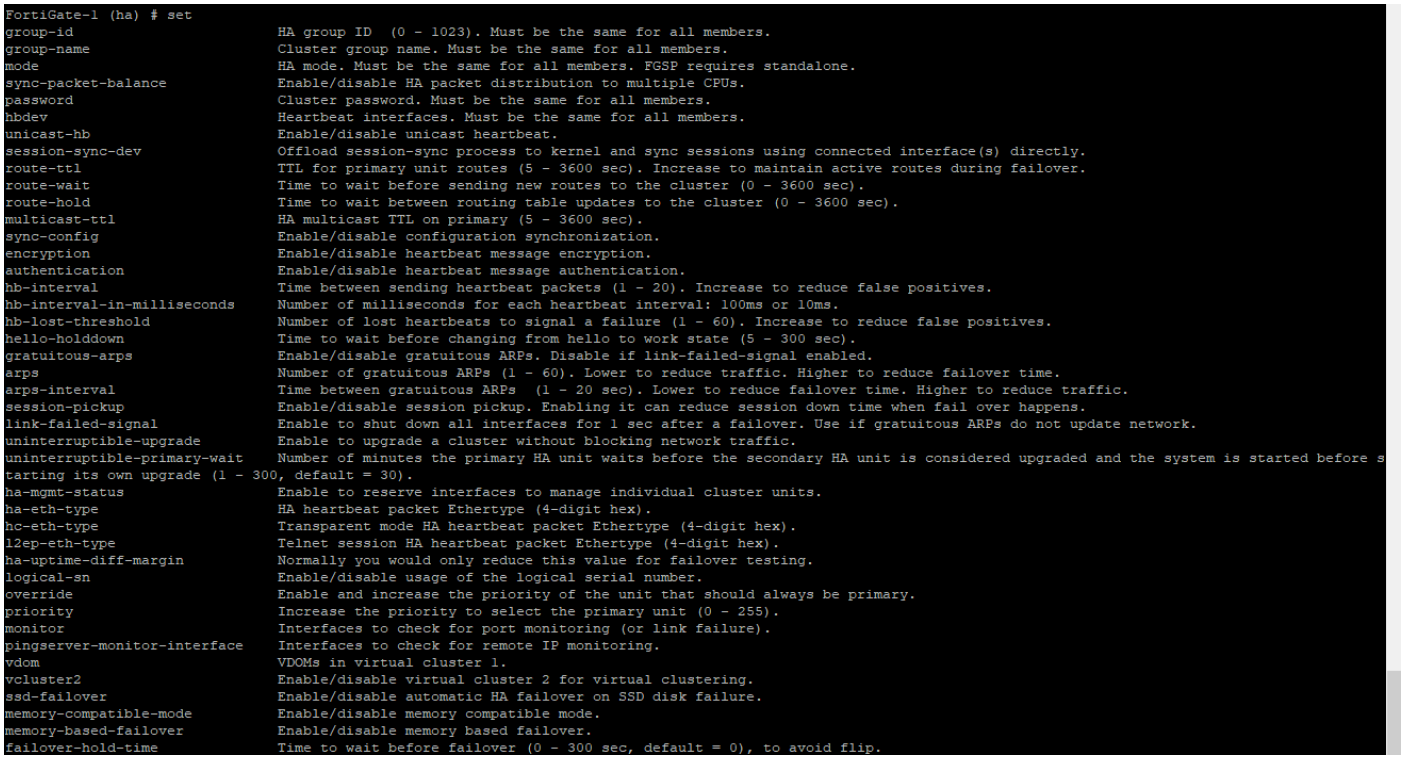
```
FortiGate-1 # config system ha
FortiGate-1 (ha) # set mode a-p
FortiGate-1 (ha) # set priority 128
FortiGate-1 (ha) # set group-id 1
FortiGate-1 (ha) # set group-name 200F-HA
FortiGate-1 (ha) # set password 123456
FortiGate-1 (ha) # set monitor port7 port8
FortiGate-1 (ha) # set hbdev port3 50 port4 50
FortiGate-1 (ha) # end
```

```
FortiGate-2 # config system ha
FortiGate-2 (ha) # set mode a-p
FortiGate-2 (ha) # set priority 100
FortiGate-2 (ha) # set group-id 1
FortiGate-2 (ha) # set group-name 200F-HA
FortiGate-2 (ha) # set password 123456
FortiGate-2 (ha) # set monitor port7 port8
FortiGate-2 (ha) # set hbdev port3 50 port4 50
FortiGate-2 (ha) # end
```

```
FortiGate-2 # secondary's external files are not in sync with the primary's, seq
uence:0. (type CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:1. (type
 CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:2. (type
 CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:3. (type
 CERT_LOCAL)
secondary's external files are not in sync with the primary's, sequence:4. (type
 CERT_LOCAL)
secondary succeeded to sync external files with primary
secondary's configuration is not in sync with the primary's, sequence:0
secondary's configuration is not in sync with the primary's, sequence:1
secondary's configuration is not in sync with the primary's, sequence:2
secondary's configuration is not in sync with the primary's, sequence:3
secondary's configuration is not in sync with the primary's, sequence:4
secondary starts to sync with primary
logout all admin users
```

Cihazlar arasında HA konfigürasyonu yapıldıktan sonra artık Firmware güncelleme işlemleri Aktif rolündeki (cihaz-1) cihaz üzerinde gerçekleştirilir. Aktif rolünü üstlenen cihaz üzerine güncel Firmware dosyası yüklendikten sonra önce aktif cihaz (cihaz-1) aktifliği pasif rolündeki (cihaz-2)cihaza devrederek kendi üzerinde güncelleme işlemini gerçekleştirir (Bu süreçte pasif rolündeki (cihaz-2) cihaz hizmet verir). Güncelleme yapılan (cihaz-1) cihaz üzerinde işlem tamamlandıktan sonra aktif rolünü geri alır ve pasif rolündeki (cihaz-2) cihaz üzerinde güncelleme işlemine başlanır.

Komut satırı üzerinde daha pek çok özelleştirme uygulanabildiği de unutulmamalıdır.



```
FortiGate-1 (ha) # set
group-id                        HA group ID  (0 - 1023). Must be the same for all members.
group-name                      Cluster group name. Must be the same for all members.
mode                            HA mode. Must be the same for all members. FGSP requires standalone.
sync-packet-balance             Enable/disable HA packet distribution to multiple CPUs.
password                        Cluster password. Must be the same for all members.
hbdev                           Heartbeat interfaces. Must be the same for all members.
unicast-hb                      Enable/disable unicast heartbeat.
session-sync-dev                Offload session-sync process to kernel and sync sessions using connected interface(s) directly.
route-ttl                       TTL for primary unit routes (5 - 3600 sec). Increase to maintain active routes during failover.
route-wait                      Time to wait before sending new routes to the cluster (0 - 3600 sec).
route-hold                      Time to wait between routing table updates to the cluster (0 - 3600 sec).
multicast-ttl                   HA multicast TTL on primary (5 - 3600 sec).
sync-config                     Enable/disable configuration synchronization.
encryption                      Enable/disable heartbeat message encryption.
authentication                  Enable/disable heartbeat message authentication.
hb-interval                     Time between sending heartbeat packets (1 - 20). Increase to reduce false positives.
hb-interval-in-milliseconds     Number of milliseconds for each heartbeat interval: 100ms or 10ms.
hb-lost-threshold               Number of lost heartbeats to signal a failure (1 - 60). Increase to reduce false positives.
hello-holddown                  Time to wait before changing from hello to work state (5 - 300 sec).
gratuitous-arps                 Enable/disable gratuitous ARPs. Disable if link-failed-signal enabled.
arps                            Number of gratuitous ARPs (1 - 60). Lower to reduce traffic. Higher to reduce failover time.
arps-interval                   Time between gratuitous ARPs  (1 - 20 sec). Lower to reduce failover time. Higher to reduce traffic.
session-pickup                  Enable/disable session pickup. Enabling it can reduce session down time when fail over happens.
link-failed-signal              Enable to shut down all interfaces for 1 sec after a failover. Use if gratuitous ARPs do not update network.
uninterruptible-upgrade         Enable to upgrade a cluster without blocking network traffic.
uninterruptible-primary-wait    Number of minutes the primary HA unit waits before the secondary HA unit is considered upgraded and the system is started before s
tarting its own upgrade (1 - 300, default = 30).
ha-mgmt-status                  Enable to reserve interfaces to manage individual cluster units.
ha-eth-type                     HA heartbeat packet Ethertype (4-digit hex).
hc-eth-type                     Transparent mode HA heartbeat packet Ethertype (4-digit hex).
l2ep-eth-type                   Telnet session HA heartbeat packet Ethertype (4-digit hex).
ha-uptime-diff-margin           Normally you would only reduce this value for failover testing.
logical-sn                      Enable/disable usage of the logical serial number.
override                        Enable and increase the priority of the unit that should always be primary.
priority                        Increase the priority to select the primary unit (0 - 255).
monitor                         Interfaces to check for port monitoring (or link failure).
pingserver-monitor-interface    Interfaces to check for remote IP monitoring.
vdom                            VDOMs in virtual cluster 1.
vcluster2                       Enable/disable virtual cluster 2 for virtual clustering.
ssd-failover                    Enable/disable automatic HA failover on SSD disk failure.
memory-compatible-mode          Enable/disable memory compatible mode.
memory-based-failover           Enable/disable memory based failover.
failover-hold-time              Time to wait before failover (0 - 300 sec, default = 0), to avoid flip.
```

Kaynaklar

- https[:]//docs.fortinet.com/document/fortigate/7.4.4/administration-guide/900885/ha-active-passive-cluster-setup
- https[:]//www.beyaz.net/tr/guvenlik/makaleler/fortigate_ha_yedekli_cihaz_kurulumu.html
- https[:]//docs.selectel.ru/en/servers-and-infrastructure/firewalls/fortigate/high-availability/
- https[:]//docs.fortinet.com/document/fortigate/7.4.0/best-practices/114990/high-availability-and-redundancy
- https[:]//community.fortinet.com/t5/FortiGate/Technical-Tip-FortiGate-HA-Primary-unit-selection-process-when/ta-p/249745