

Palo Alto Firewall Ürünlerinde HA Yapısı ve Versiyon Upgrade

Konuya başlamadan önce bilmeyen arkadaşlar ya da bilenler için de ufak bir hatırlatma yapmak adına HA yapıdan bahsetmek istiyorum. HA nedir? HA; yani uzun haliyle bildiğimiz High Availability dediğimiz teknoloji ya da yapı, IT/Network sistemleri içerisinde yer alan sistem/servis/cihazların biri ya da birkaçı arızalansa dahi sistemin kesintisiz ve sorunsuz ya da kesinti olsa bile minimum kayıp ile çalışabilmesidir. HA yapısının temelinde redundancy(yedeklilik), failover(aktarım) ve monitoring(izleme) bileşenleri mevcuttur. Yedeklilik diyince güç yedekliliği, ağ ortamında link yada stacking/vpc yapıdaki cihaz yedekliliği, sunucu/sanallaştırma ortamında ise cluster yapılar örnek verilebilir.

HA dediğimiz yapı 2 ayrı modda çalışmasını sürdürür. Bunlar Aktif-Aktif ya da Aktif-Pasif çalışma şeklindedir.

1. *Aktif-Aktif Yapı: Her iki cihaz da üzerinde yer alan yükü ya da üzerinden geçen data trafiğini load balance özelliği ile paylaşır. Cihazlardan bir tanesinin arızalanması durumunda yük tamamen diğer cihaza geçer. Performans açısından verimli bir yapı olsa da olumsuz yönleri de söz konusudur.*
2. *Aktif-Pasif Yapı: Tüm yük ya da geçen trafik tek bir cihaz üzerinden sağlanır. Diğer cihaz ise çalışır vaziyette yükü üzerine alabilecek şekilde hazırda bekler. Asıl cihaz down duruma geçerse yedekte yer alan cihaz devreye girer. Maliyet açısından diğer yapıya göre daha uygundur.*

Ağ mühendisi gözünden baktığımız zaman ağ yedekliliği diyince aklımıza HSRP, VRRP veya GLBP gibi protokoller gelebilir. Bunlarla paralel HA sağlanmış olur. Sanallaştırma ortamında ise fiziksel bir sunucu down duruma düştüğünde üzerinde yer alan tüm sanal makineler otomatik olarak başka bir sunucuda çalışmaya başlar.

Tüm trafik tek bir firewall üzerinden geçseydi Single Point of Failure durumu oluşup kesinti riski ortaya çıkabilirdi. HA yapısı sayesinde bu risk ortadan kaldırılarak sistem yedekliliği ile iş sürekliliği sağlanmış olur.

Firewall üzerinde yer alan HA yapı ile birlikte:

1. Donanımsal ya da yazılımsal herhangi bir sorun meydana gelse bile trafik kısa bir süre içerisinde yedek cihaza aktarılacağı için herhangi bir kesinti ya da kayıp söz konusu olmaz. Bu duruma failover denir.
2. Güncel teknolojiye aktif cihaz üzerinde yer alan tüm session bilgileri paralelde yedekte bekleyen cihazın database' i içerisinde de tutulur. Bu sayede cihaz değişikliği olduğunda kullanıcılar herhangi bir sorun hissetmez. (Stateful Failover)
3. HA yapı sayesinde kesinti yaşamadan bakım ve güncelleme çalışması gerçekleştirilebilir. Sırasıyla önce pasif sonra da aktif cihaz üzerinde çalışma gerçekleştirilecek kesinti ve kayıplar sıfıra indirgenebilir.
4. Aktif-Aktif durumda yük dengeleme durumu sayesinde çalışan her bir firewall'ın işlem yükü azaltılarak cihaz performanslarında artış sağlanabilir.

Firewall ürünlerinde HA yapı kurulabilmesi için gerekli ihtiyaçlar nelerdir?

1. Aynı marka ve modelde iki cihaz olması gerekir. (Port sayısı, tipi vs birebir aynı olmalı)
2. Her iki cihazda da aynı firmware versiyonu olmalıdır.
3. Her iki cihazda da aynı lisansların bulunması gerekmektedir.
4. Heartbeat: Cihazların birbirlerini sürekli up/down mu diye kontrol edebilmeleri için ve veri senkronizasyonu yapabilmesi için özel fiziksel bağlantı kurulması (Keep alive gibi de düşünebiliriz)

Palo Alto cihazlarda, aktif pasif yapıda versiyon upgrade'i nasıl yapılır?

Palo Alto da bulunan High Availability (HA) yapısı sayesinde cihazların kesintisiz olarak çalışması sağlanır. Bu yapı sayesinde cihazlardan birisi arızalandığında diğer cihaz devreye girerek sistemlerin devam etmesini sağlar. HA yapısı içerisinde iki mod bulunmaktadır. Bunlar;

- *Aktif-Aktif*
- *Aktif-Pasif*

Bu dokümanda Aktif-Pasif ve modda çalışan Palo Alto cihazlarında versiyon upgrade'i nasıl yapıldığı anlatılmaktadır.

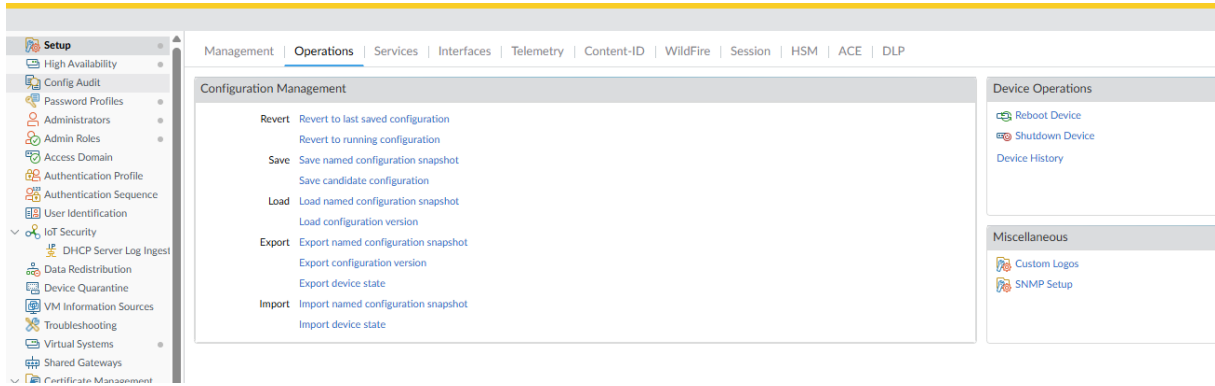
1.Adım

- *Versiyon yükseltmesine başlamadan önce olası bir durumda cihazları geri döndürebilmemiz için her iki cihazında yedeklerini almamız gerekmektedir.*
- *Yedek almak için ilk önce konfigürasyon dosyası oluşturmamız gerekmektedir.*
- *Eğer kayıtlı konfigürasyon dosyanız varsa ADIM 2'ye geçin.*

- “Device” sekmesine tıklayın.



- “Device” ekranı açıldıktan sonra sol taraftan “Setup” sekmesine tıklayın. “Setup” sekmesinin içerisinde “Operations” sekmesine geçin. Burada “Save named configuration snapshot” seçelim.

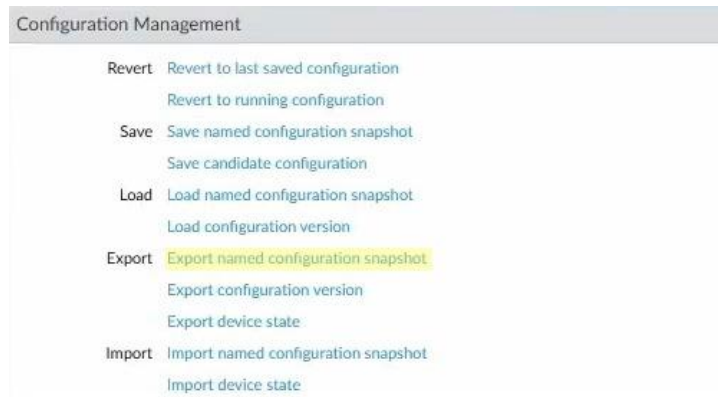


- Sonrasında açılan ekranda konfigürasyon dosyasına isim verip “OK” diyerek dosyayı oluşturalım.



2.Adım

- Device> Setup> Operations sekmesine tıklayın.
- Cihaz konfigürasyonunu indirmek için “Export named configuration snapshot” tıklayın.



- Cihaz konfigürasyonunu içeren XML dosyasını seçin ve OK tuşuna basarak indirin.

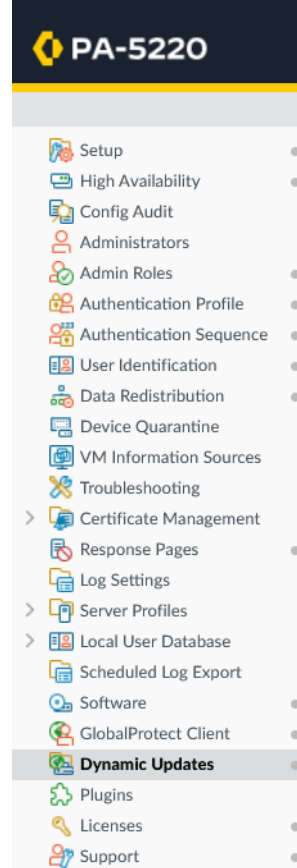


The image shows a dialog box titled "Export Named Configuration". It has a text input field labeled "Name" with a dropdown arrow on the right. Below the input field are two buttons: "OK" (blue) and "Cancel" (grey). A help icon (?) is in the top right corner.

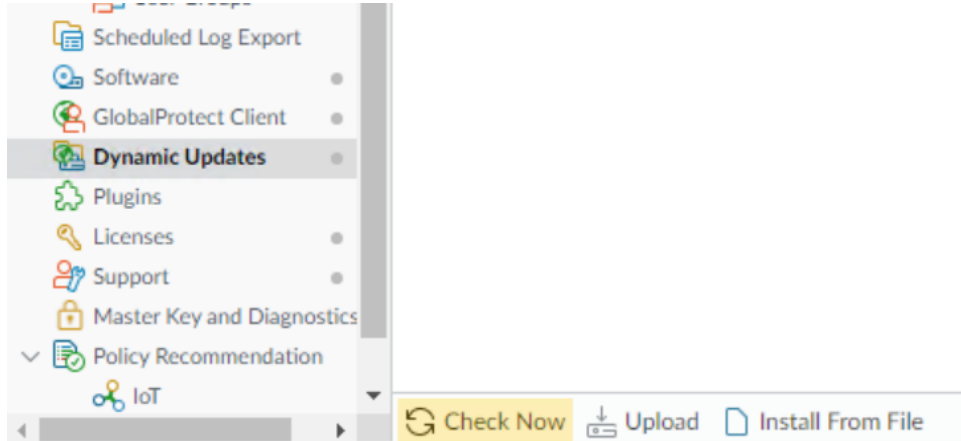
- Bu işlemleri her iki cihaz içinde uygulayın.

3.Adım

- İlk olarak dinamik bileşenlerin güncel olduğundan emin olmamız gerekmektedir. Dinamik bileşenlerin güncel olmaması durumunda, paketler yeni yazılım versiyonu ile uyumlu çalışmayabilir.
- Dinamik bileşenleri güncellemek için;
- Device>Dynamic Updates sekmesine tıklayın.



- Sol alt köşede bulunan Check Now butonuna tıklayarak son gelen güncellemeleri kontrol edin.

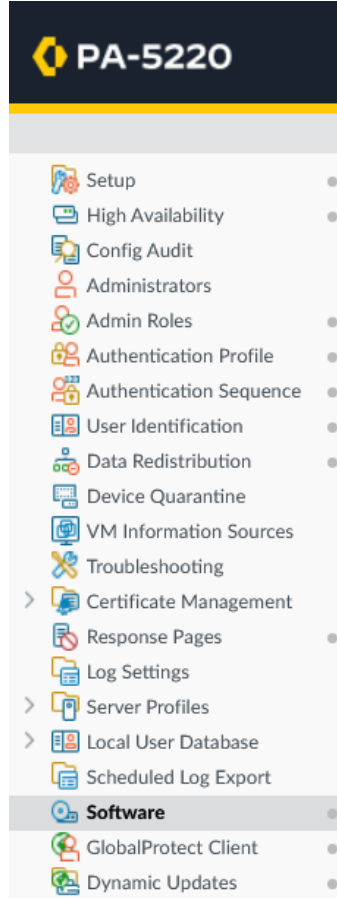


- Güncellenmesi gereken dinamik paketlerin gelmesi halinde Action > Download sonrasında Install butonlarına tıklayın ve paketlerin kurulumlarını tamamlayın.

VERSION	FILE NAME	FEATURES	TYPE	SIZE	SHA256	RELEASE DATE	DOWNLOADED	CURRENTLY INSTALLED	ACTION	DOCUMENTATION
Applications and Threats Last checked: 2022/09/23 07:52:19 MDT Schedule: Every 30 minutes at minutes past half hour (Download and Install)										
B611-7538	panosp2-uf-apps-B611-7538	Apps	Full	51 MB	2a1554a3c433a0f...	2022/08/23 21:13:49 MDT			Download	Release Notes
B612-7539	panosp2-uf-apps-B612-7539	Apps	Full	51 MB	4f8b199b5f315a1...	2022/08/24 09:28:51 MDT			Download	Release Notes
B613-7545	panosp2-uf-apps-B613-7545	Apps	Full	51 MB	5a190a94319a1...	2022/08/29 19:56:37 MDT			Download	Release Notes
B614-7547	panosp2-uf-apps-B614-7547	Apps	Full	51 MB	3a8a0d7434231...	2022/08/30 22:39:40 MDT			Download	Release Notes
B615-7549	panosp2-uf-apps-B615-7549	Apps	Full	51 MB	1d29d279c2a057...	2022/09/01 16:48:50 MDT			Download	Release Notes
B616-7550	panosp2-uf-apps-B616-7550	Apps	Full	51 MB	11a0c101702098...	2022/09/06 15:28:32 MDT			Download	Release Notes
B617-7553	panosp2-uf-apps-B617-7553	Apps	Full	51 MB	384c49a73c7a0a...	2022/09/07 19:24:48 MDT			Download	Release Notes
B618-7565	panosp2-uf-apps-B618-7565	Apps	Full	51 MB	9a8f7a5b09a0a...	2022/09/13 22:42:48 MDT			Download	Release Notes
B619-7569	panosp2-uf-apps-B619-7569	Apps	Full	51 MB	d7c5d515a5a0a2...	2022/09/15 20:59:18 MDT			Download	Release Notes
B620-7574	panosp2-uf-apps-B620-7574	Apps	Full	51 MB	21a046f1380a47...	2022/09/20 08:33:00 MDT	✓ previously		Revert	Release Notes
B621-7584	panosp2-uf-apps-B621-7584	Apps	Full	51 MB	064545a4a0809...	2022/09/21 00:53:44 MDT	✓	✓	Review Policies Revert Apps	Release Notes
Device Dictionary Last checked: 2022/09/23 07:52:24 MDT										
S7-348	panosp-all-devicelb-S7-348	lib	Full	165 KB	6c784482b6a2c...	2022/09/01 23:22:54 MDT				Release Notes
S8-351	panosp-all-devicelb-S8-351	lib	Full	165 KB	b584b103346c7a...	2022/09/15 19:59:56 MDT	✓	✓		Release Notes

4.Adım

- *Aktif-Pasif yapılandırmasındaki firewall için, ilk olarak pasif HA eşini yükseltin.*
- *Device > Software seçin.*



- *Sol alt köşede bulunan Check Now butonu ile son gelen güncellemeleri kontrol edin.*
- *İndirilmesi gereken sürümü bulun ve Download seçeneği ile sürümü indirin.*
- *Sürüm indirildikten sonra Install seçeneği ile kurulumu başlatın.*

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	
10.2.2-h2	339 MB	2022/08/18 09:06:40			Download	Release Notes
10.2.2	339 MB	2022/06/07 10:21:55			Download	Release Notes
10.2.1	334 MB	2022/04/18 13:10:45			Download	Release Notes
10.2.0-h1	556 MB	2022/03/30 17:26:51			Download	Release Notes
10.2.0	556 MB	2022/02/27 19:31:56			Download	Release Notes
10.1.7	359 MB	2022/09/12 14:40:56			Download	Release Notes
10.1.6	357 MB	2022/05/24 12:46:17			Download	Release Notes
10.1.6-h6	357 MB	2022/08/09 15:48:40	Downloaded	✓	Reinstall	Release Notes

Kurulum başarıyla tamamlandıktan sonra aşağıdaki yöntemleri takip edin:

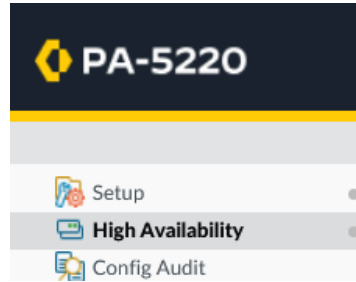
- *Yeniden başlatmanız istenirse Yes'e tıklayın.*
- *Yeniden başlatmanız istenmezse Device > Setup > Operations ve Reboot Device tıklayın.*

5.Adım

- Pasif cihaz yeniden başlatıldıktan sonra Dashboard > High Availability penceresini kontrol edin ve aktif cihaz ile senkronize olmasını bekleyin.
- Senkronize tamamlandıktan sonra aktif cihaz için yükseltme işlemine geçin.

6.Adım

- Aktif cihazın versiyonunu yükseltmeden önce pasif duruma getirmeniz gerekmektedir.
- Device > High Availability sekmesine tıklayın.



- Operational Commands sekmesine gidin.

General | HA Communications | Link and Path Monitoring | **Operational Commands**

- Suspend local device for high availability seçeneğine tıklayarak Aktif cihazı askıya alın.

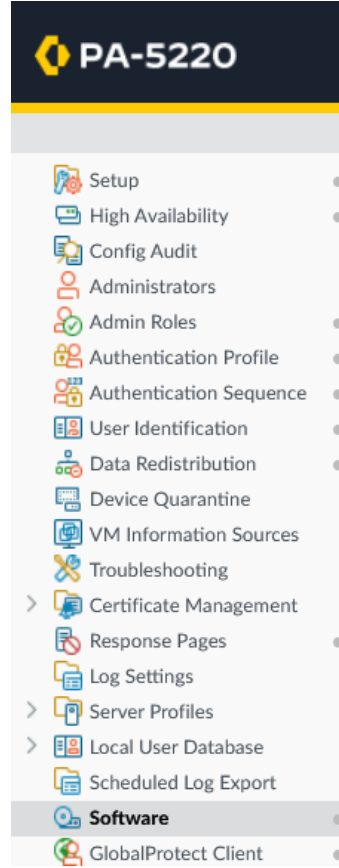
General | HA Communications | Link and Path Monitoring | **Operational Commands**

Suspend local device for high availability

- Bu adım aktif cihazı askıya alarak pasif duruma getirir ve pasif cihazı da otomatik olarak aktif duruma getirir.

7.Adım

- Aktif cihaz pasif duruma geldikten sonra yükseltme işlemine başlayın.
- Device > Software seçin.



- Sol alt köşede bulunan Check Now ile son gelen güncellemeleri kontrol edin.
- İndirilmesi gereken sürümü bulun ve Download seçeneği ile sürümü indirin.
- Sürüm indirildikten sonra Install seçeneği ile kurulumu başlatın.

VERSION	SIZE	RELEASE DATE	AVAILABLE	CURRENTLY INSTALLED	ACTION	
10.2.2-h2	339 MB	2022/08/18 09:06:40			Download	Release Notes
10.2.2	339 MB	2022/06/07 10:21:55			Download	Release Notes
10.2.1	334 MB	2022/04/18 13:10:45			Download	Release Notes
10.2.0-h1	556 MB	2022/03/30 17:26:51			Download	Release Notes
10.2.0	556 MB	2022/02/27 19:31:56			Download	Release Notes
10.1.7	359 MB	2022/09/12 14:40:56			Download	Release Notes
10.1.6	357 MB	2022/05/24 12:46:17			Download	Release Notes
10.1.6-h6	357 MB	2022/08/09 15:48:40	Downloaded	✓	Reinstall	Release Notes

Kurulum başarıyla tamamlandıktan sonra aşağıdaki yöntemleri takip edin:

- Yeniden başlatmanız istenirse Yes'e tıklayın
- Yeniden başlatmanız istenmezse Device > Setup > Operations ve Reboot Device tıklayın.

8.Adım

- *Pasif cihaz (ilk aktif) yeniden başlatıldıktan sonra Dashboard > High Availability penceresini kontrol edin ve aktif (ilk pasif) cihaz ile senkronize olmasını bekleyin.*
- *Senkronizasyon tamamlandıktan sonra sonraki adıma geçin.*

9.Adım

- *Pasif cihazın (ilk aktif) güncelleme işlemi tamamlandıktan sonra tekrardan aktif duruma getirin.*
- *Device > High Availability > Operational Commands sekmesine gidin.*

General | HA Communications | Link and Path Monitoring | Operational Commands

- *Make local device functional for high Availability seçeneğine tıklayın.*

General | HA Communications | Link and Path Monitoring | Operational Commands

Make local device functional for high availability

- *Pasif cihaz (ilk aktif) tekrardan aktif duruma gelir.*

10.Adım

- *Pasif cihaz (ilk aktif) yeniden aktif duruma geldikten sonra Dashboard > High Availability penceresini kontrol edin ve pasif cihaz ile senkronize olmasını bekleyin.*