

İlk olarak gelen talebimiz bu şekilde.

Bir telefon santralimiz var ve bu santrale sip hizmeti veren firmanın sunucuna ilgili portlara bağlantı izni isteniyor.

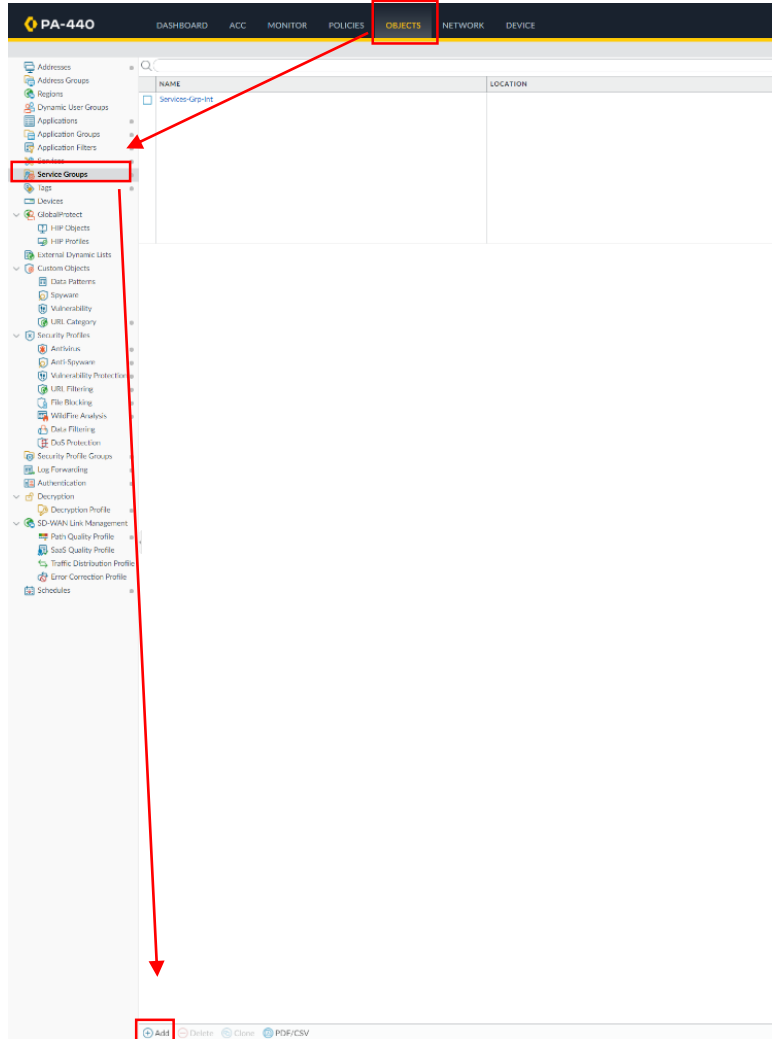
[@Fuma Bilgi Teknolojileri](#) Bey merhaba, trunk tanımlamaları için 212. [REDACTED] ip adresi 5089,5090 UDP/TCP, 10000-20000 UDP/TCP portlarına erişim izni sağlayabilir misiniz?

12:28

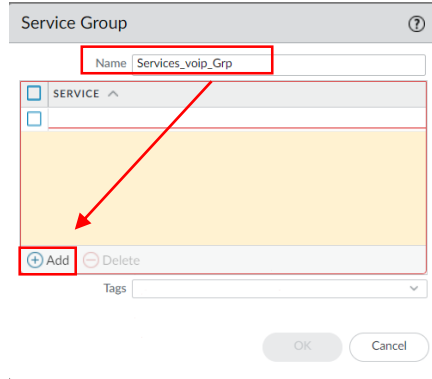
Hemen palo alto firewall a login oluyoruz. Yapmamız gerekenleri sıralayacak olursak;

- 1- Port tanımlamaları(servisler)
- 2- Kaynak ve hedef ip tanımlamaları
- 3- Son olarak security policy yazımı

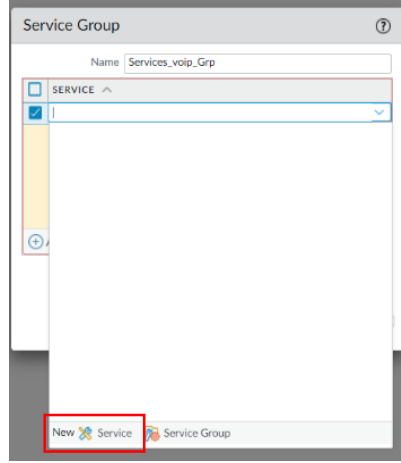
Palo Alto arayüzden **"OBJECTS"** sekmesinden birden fazla port ekleyeceğim için **"service Groups"** seçeneğine geliyor ve yeni ir grup tanımlamak için **"Add"** butonuna tıklıyorum.



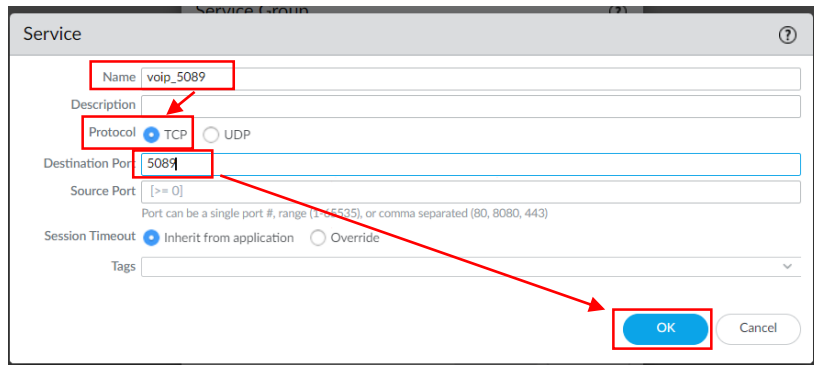
Karşıma gelen menüden servis grubuma isim tanımlıyorum ve “Add” diyerek yeni servis portlarımı tanımlamaya başlıyorum.



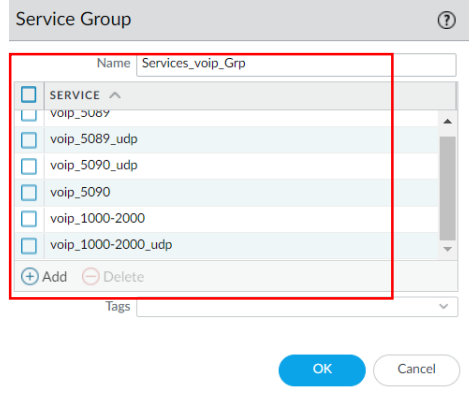
Karşıma gelen ekrandan “New Service” diyorum.



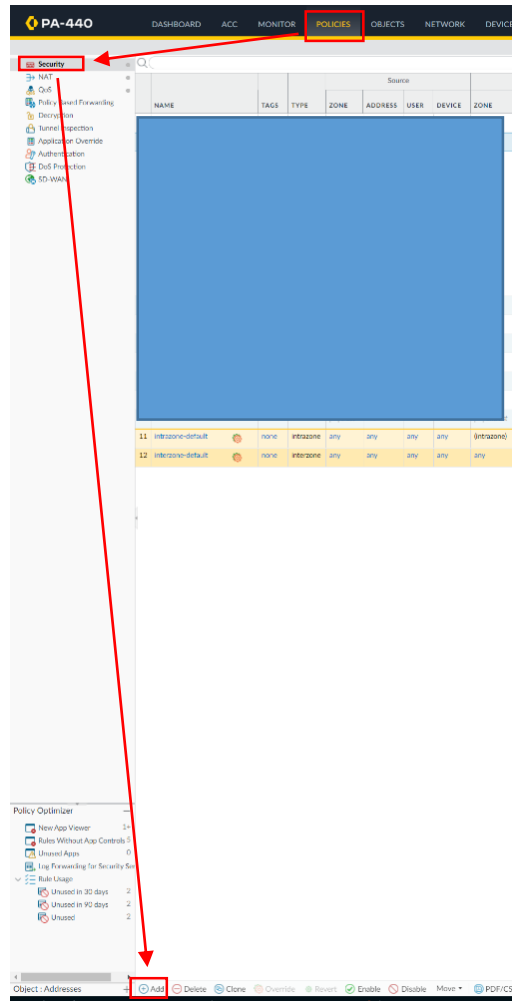
Yine karşıma gelen ekrandan servis portlarımı TCP ve UDP olarak tanımlamaya başlıyorum. Tanımlamayı yapıp “OK” ile işlemimi tamamlıyorum. Kaç tane servis tanımlayacaksam hepsi için aynı işlemi tekrarlıyorum.



Tanımlamalarımı tamamladım. Aşağıda görüldüğü üzere istenilen portları gruptladım. **"OK"** diyerek işlemimi tamamliyorum.



Sonraki adımda ilgili işlemler için security kuralı yazacağım. Bu nedenle ara yüzden **"POLICIES"** sekmesinden **"Security"** seçeneğine gelip **"Add"** diyerek yeni bir kural oluşturun.



Karşıma gelen ekrandan kuralıma isim veriyorum.

Security Policy Rule

General | Source | Destination | Application | Service/URL Category | Actions | Usage

Name: **SANTRAL_TO_voip_grp.allow**

Rule Type: universal (default)

Description:

Tags:

Group Rules By Tag: None

Audit Comment:

[Audit Comment Archive](#)

OK Cancel

"Source" sekmesinden kaynak zonu mu ve hostumu seçiyorum. Benim kuralımda sadece satral cihazının ilgili portlara ulaşması için **"Source Address"** kısmında ip tanımını yaptığım santal cihazımı seçiyorum.

Security Policy Rule

General | **Source** | Destination | Application | Service/URL Category | Actions | Usage

☐ Any

☒ SOURCE ZONE ^

☐ LAN

☐ Any

☒ SOURCE ADDRESS ^

☐ SANTAL

☐ any

☒ SOURCE USER ^

☐ any

☒ SOURCE DEVICE ^

+ Add - Delete

+ Add - Delete

+ Add - Delete

+ Add - Delete

☐ Negate

OK Cancel

"Destination" sekmesine geliyorum ve hedef zonumu ve hostumu seçiyorum. Yani local network den gelen satral cihazım wan zone u üstünden ilgili adrese gidecek.

Security Policy Rule

General | Source | **Destination** | Application | Service/URL Category | Actions | Usage

select

☒ DESTINATION ZONE ^

☐ WAN

☐ Any

☒ DESTINATION ADDRESS ^

☐ al

☐ any

☒ DESTINATION DEVICE ^

+ Add - Delete

+ Add - Delete

+ Add - Delete

☐ Negate

OK Cancel

“Service/URL Category” sekmesine gelerek yukarıdaki adımlarda oluşturduğumuz. “Service Group” seçimini yapıyorum.

Unutmadan seçimleri “add” butonuna basarak yapıyoruz. :D

The screenshot shows the 'Security Policy Rule' configuration window with the 'Service/URL Category' tab selected. The 'Service' list on the left contains 'SERVICE' and 'Services_voip_Grp'. The 'URL CATEGORY' list on the right is empty. The 'Add' button is highlighted in red. The 'OK' button is also highlighted in red.

Son olarak “Actions” sekmesine geliyorum. Action kısmına kuralımın aktif olması için Allow aynı zamanda kuralda log kaydı için ilgili seçimi yapıp “OK” diyerek işlemimi tamamliyorum.

The screenshot shows the 'Security Policy Rule' configuration window with the 'Actions' tab selected. The 'Action Setting' section has 'Action' set to 'Allow'. The 'Log Setting' section has 'Log at Session Start' checked. The 'Other Settings' section has 'Schedule' and 'QoS Marking' set to 'None'. The 'OK' button is highlighted in red.

Unutmadan oluşturduğum kuralı en üste taşıyorum ki hiyerarşik sorun çıkmasın herhangi bir engele takılmasın.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS	Rule Usage				DAYS WITH NO NEW APPS
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE						HIT COUNT	LAST HIT	FIRST HIT	APPS SEEN	
1	SANTRAL_TO_voip_grp_allow	none	universal	LAN	SAN...	any	any	WAN		any	any	Services_voip...	Allow	none		0	-	-	-	-