

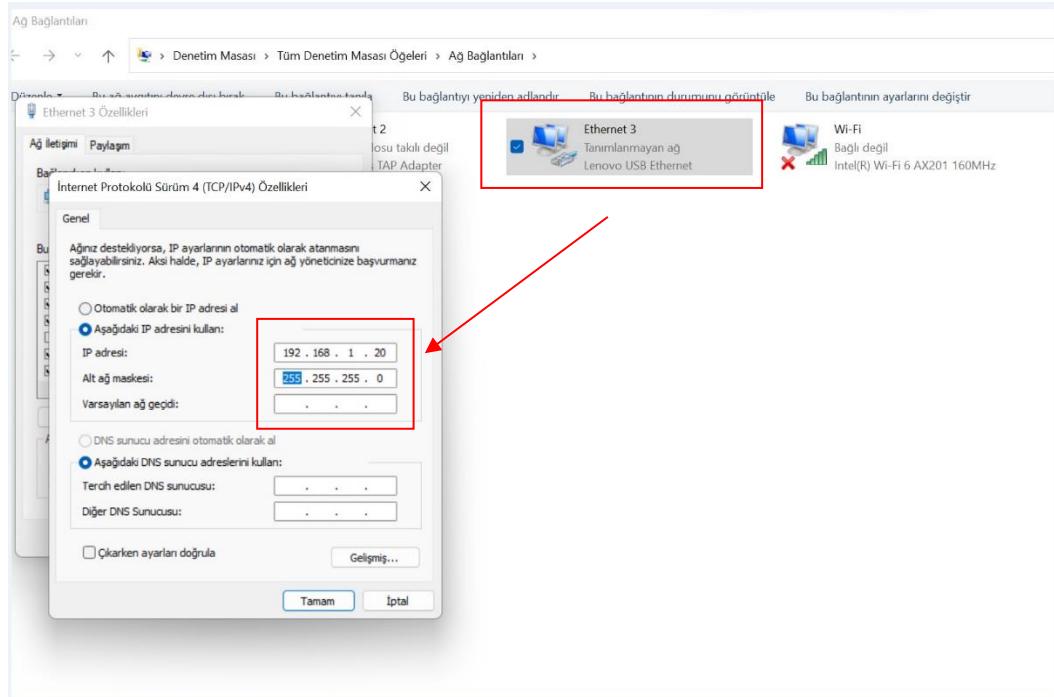
Palo Alto firewall cihazları üzerinde MANAGEMENT adında bir yönetim portu ile gelirler. Cihazınız MANAGEMENT port ip bilgisi standartta "192.168.1.1" dir.



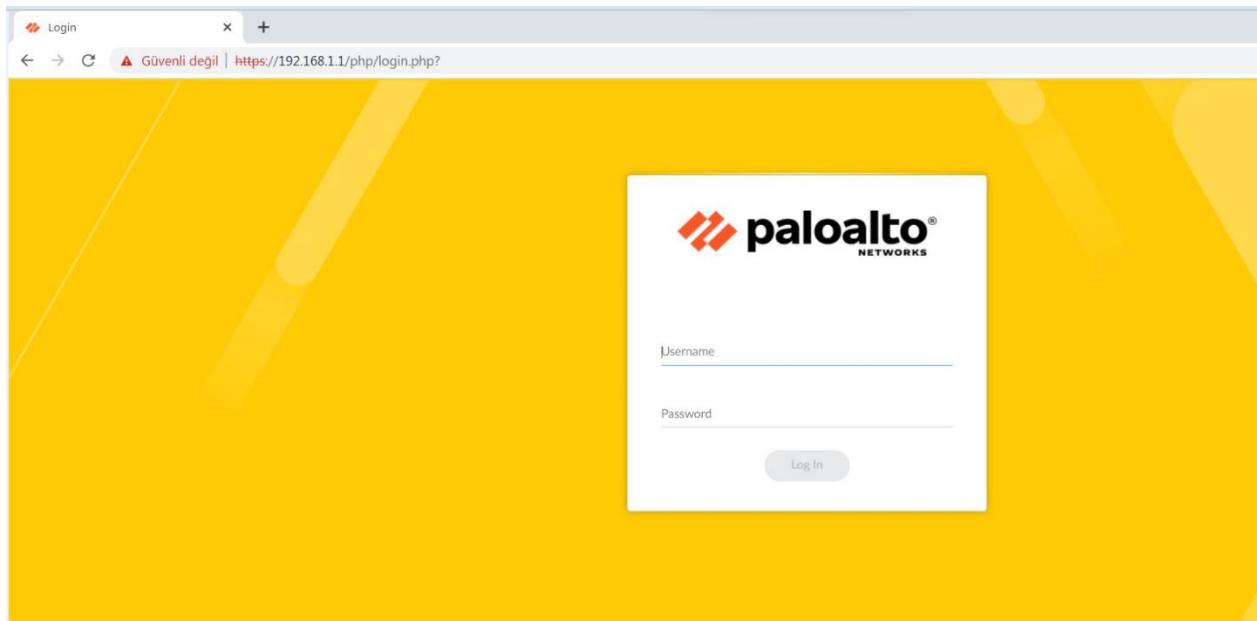
Bu nedenle bilgisayarımda ethernet girişi ve PALO ALTO management portuna fiziksel olarak birbirine bağlıyorum.



Bağlantı işlemini tamamladıktan sonra bilgisayarıma PALO ALTO management ip laboğundan manuel bir ip atamak için ağ bağlantılarına gidip Ethernet bağdaştırıcıma ip adresi vererek işlemimi gerçekleştirdiyorum.



Sonraki adımda internet tarayıcımı açıyorum ve adres çubuğuna <https://192.168.1.1> adresini girerek firewall arayüzüme ulaşıyorum.

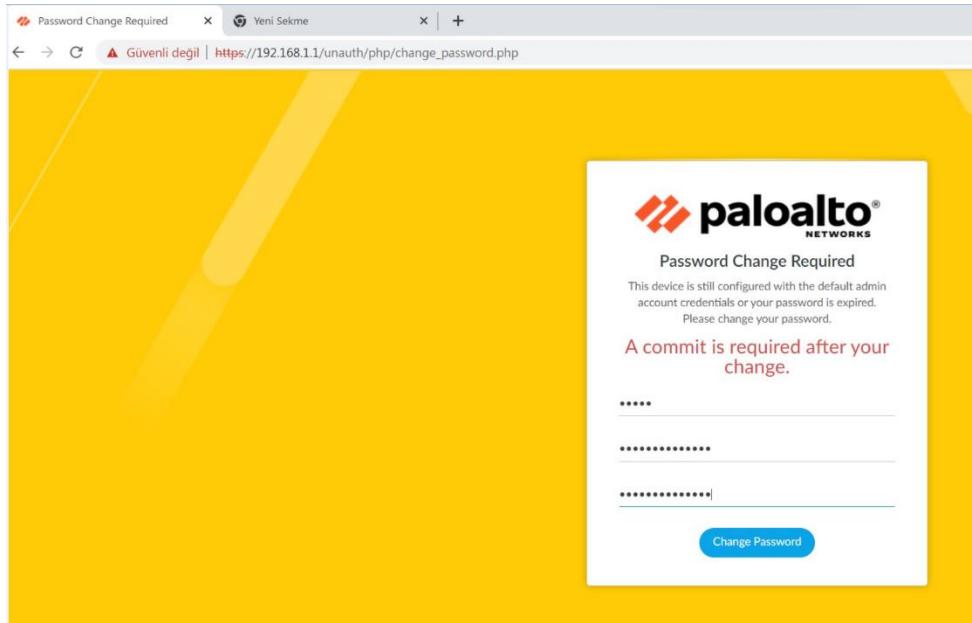


Cihazımızda oturum açmak için standartta gelen kullanıcı bilgileri aşağıdaki gibidir.

Username: admin

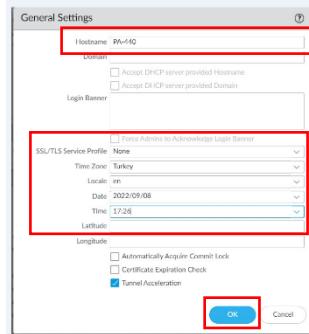
Password: admin

Gerekli bilgileri girdikten sonra bizden şifremizin değiştirilmesi gereği bildiriliyor. İlgili alanları doldurup **“Change Password”** diyerek işlemimi tamamlıyorum.



Sonraki adımda Firewall arayüzüne ulaşıyorum. Burada herkes kendi kurulum tarzını kullanabilir. Ben ilk olarak cihazımın genel ayarlarını yapacağım. Bu nedenle arayüzden **“DEVICE”** sekmesi altından **“SETUP”** kısmından **“MANAGEMENT”** ve yine oradan **“GENERAL SETTINGS”** kısmına geliyorum. İlgili alanı düzenlemek için **“EDIT”** butonuna basıyorum.

Sonraki adımda karşımıza çıkan menüden cihazımı isim veriyor, tarih ve saat ayarımı yapıp "OK" diyerek işlemimi tamamlıyorum.



Sonraki adımda işlemlerimi hızlıca tamamlamak için "ZONE" tanımlamaları yapacağım. Ben standartta gelen tanımlamı kullanmak istemiyorum. Bu nedenle arayüzden "NETWORK" sekmesi alındından "ZONES" seçeneğine tıklıyor ve ADD butonuna tıklayarak yeni "ZONE" tanımı yapacağım.

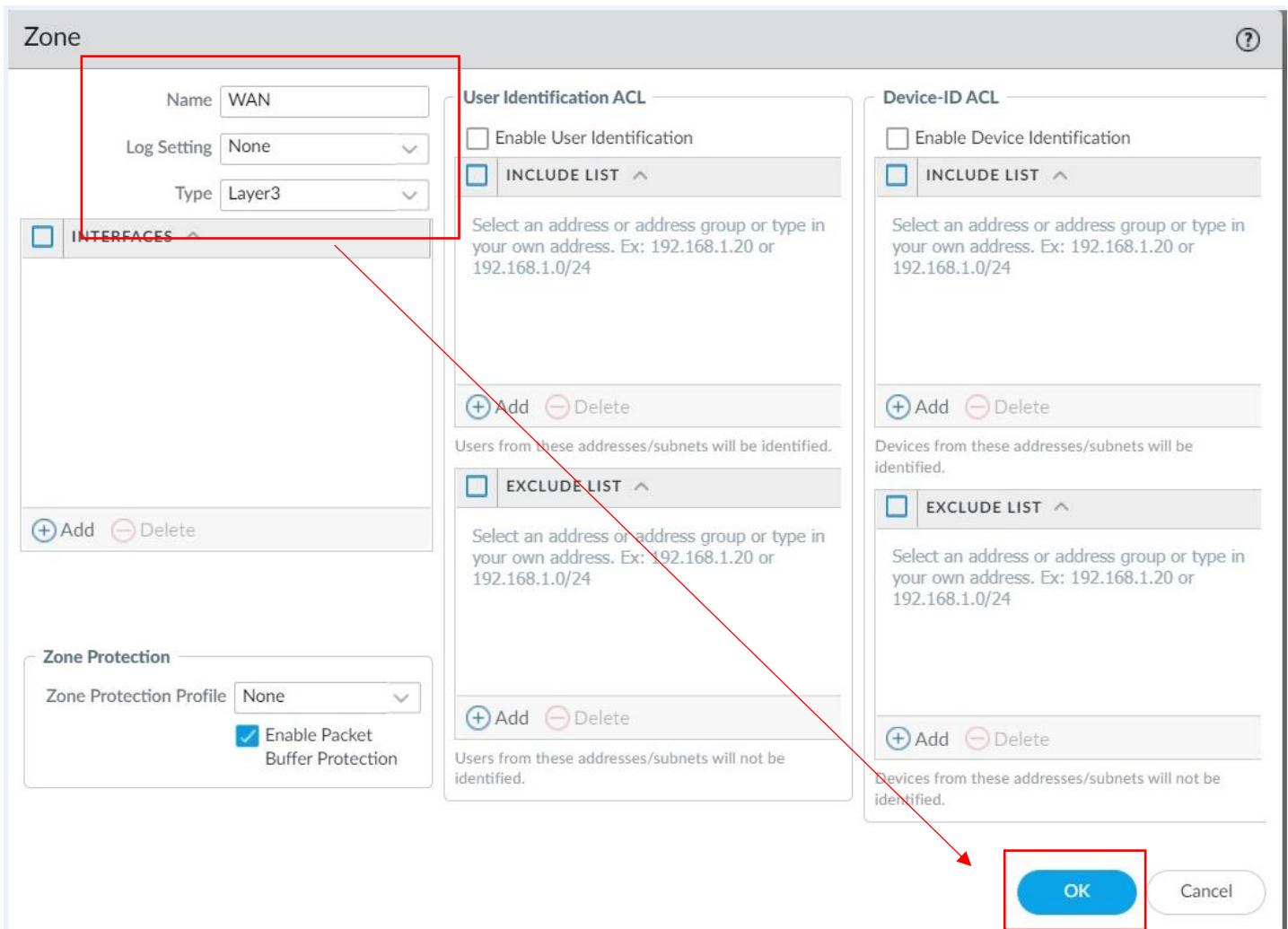
NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	User-ID		Device-ID		
						ENABLED	INCLUDED NETWORKS	EXCLUDED NETWORKS	ENABLED	INCLUDED NETWORKS
trust	virtual-wire			<input checked="" type="checkbox"/>	<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none
untrust	virtual-wire			<input checked="" type="checkbox"/>	<input type="checkbox"/>	any	none	<input type="checkbox"/>	any	none

Oluşturacağımız ZONE'ları tüm kurallarda kullanacağım. Bu nedenle aslında bir nevi gruplama yapmış olacağım yani oluşturduğumuz ZONE lara üye olan interfaceler, adresler, objeler için aynı kurallar geçerli olacak.

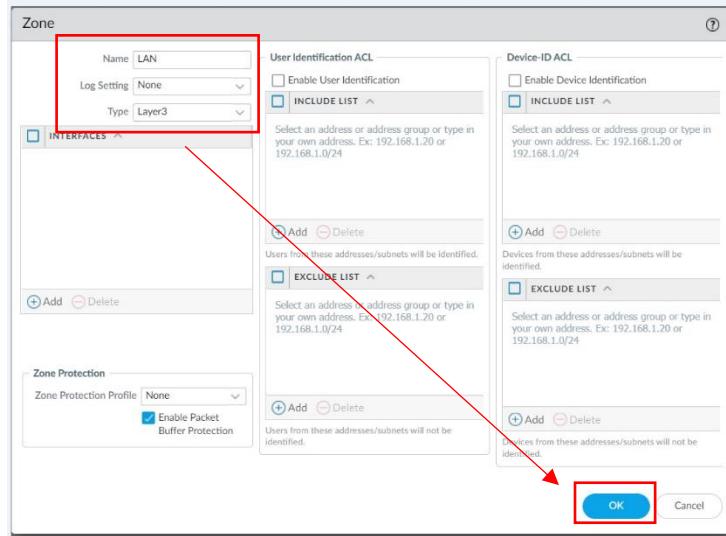
Add butonuna bastıktan sonra karşıma gelen menüden tanımlamaları gerçekleştiriyorum.

İlk olarak **“WAN”** adlı bir zone oluşturoyorum. Bu zone benim için internețe çıkıştı yöneteceğim zone olacak ve ileriki adımlarda oluşturduğumuz WAN zonuna interface atayarak internețe çıkışımızı sağlayacağız.

İlgili alanları dolduruyorum. Burada dikkat etmemiz gereken bir hususta static ve dinamik yönlendirme protokollerini kullanabilmek için **“TYPE”** kısmı **“Layer3”** seçmek ilgili alanları doldurup **“OK”** diyerek işlemimi gerçekleştiriyorum.



Sonraki adımda bir de LOCAL NETWOK ü yönetebilmek adına “ LAN” adında bir zone oluşturuyorum.



Zone tanımlama işlemimi tamamladım. Arayüzümde görünüyor. Sonraki adımda bu oluşturduğum zone lara interface, address, obje gibi tanımlar ekleyeceğim.

Bu nedenle yapımı daha tanımlanabilir ve anlaşılabilir olması için ip adreslerimi, subnetlerimi ve gateway lerimi tanımlayacağım.

NAME	TYPE	INTERFACES / VIRTUAL SYSTEMS	ZONE PROTECTION PROFILE	PACKET BUFFER PROTECTION	LOG SETTING	ENABLED	INCLUDED NE
trust	virtual-wire			<input checked="" type="checkbox"/>		<input type="checkbox"/>	any
untrust	virtual-wire			<input checked="" type="checkbox"/>		<input type="checkbox"/>	any
WAN	layer3			<input checked="" type="checkbox"/>		<input type="checkbox"/>	any
LAN	layer3			<input checked="" type="checkbox"/>		<input type="checkbox"/>	any

Şimdiki adımda yukarıda bahsettiğim gibi adresler ekleyeceğim. Bunlar kurallar yada tanımlamalar yaparken benim işimi inanılmaz şekilde kolaylaştıracak.

Şimdi arayüzden “OBJECTS” sekmesinin altından “ADRESSES” tabına gelip , yeni bir adres tanımlaması yapmak için “add” butonuna tıklıyorum.

The screenshot shows the PA-440 interface with the 'OBJECTS' tab selected. On the left, a sidebar lists various object types. The 'Addresses' item is highlighted with a red box and has a red arrow pointing to it from the top-left. At the bottom of the screen, a toolbar contains several buttons, with the '+ Add' button highlighted with a red box. A red arrow points from the bottom-left towards this button.

PA-440

DASHBOARD ACC MONITOR POLICIES **OBJECTS** NETWORK DEVICE

Addresses

- Address Groups
- Regions
- Dynamic User Groups
- Applications**
- Application Groups
- Application Filters
- Services
- Service Groups
- Tags
- Devices
- GlobalProtect
 - HIP Objects
 - HIP Profiles
- External Dynamic Lists
- Custom Objects
 - Data Patterns
 - Spyware
 - Vulnerability
 - URL Category
- Security Profiles
 - Antivirus
 - Anti-Spyware
 - Vulnerability Protection
 - URL Filtering
 - File Blocking
 - WildFire Analysis
 - Data Filtering
 - DoS Protection
- Security Profile Groups
- Log Forwarding
- Authentication
- Decryption
 - Decryption Profile
- SD-WAN Link Management
 - Path Quality Profile
 - SaaS Quality Profile
 - Traffic Distribution Profile
 - Error Correction Profile
- Schedules

NAME	LOCATION	TYPE

+ Add **Delete** **Clone** **PDF/CSV**

Karşıma gelen menüden personnel subnet için bir gateway tanımlaması yapacağım. İlgili alanları doldurup "Ok" diyerek işlemimi tamamlıyorum. Siz kendi network topoloji veya dizaynınıza göre şekillendirebilirsiniz.

Address

Name

Description

Type

Enter an IP address or a network using the slash notation (Ex. 192.168.80.150 or 192.168.80.0/24). You can also enter an IPv6 address or an IPv6 address with its prefix (Ex. 2001:db8:123:1::1 or 2001:db8:123:1::/64)

Tags

Ben bu adımları gerçek bir ortamda yaptığım için birden çok network tanımlaması yapıyorum. Tüm tanımlamalarımı aynı şekilde gerçekleştirdim ve tanımlama adımını tamamlamış oldum.

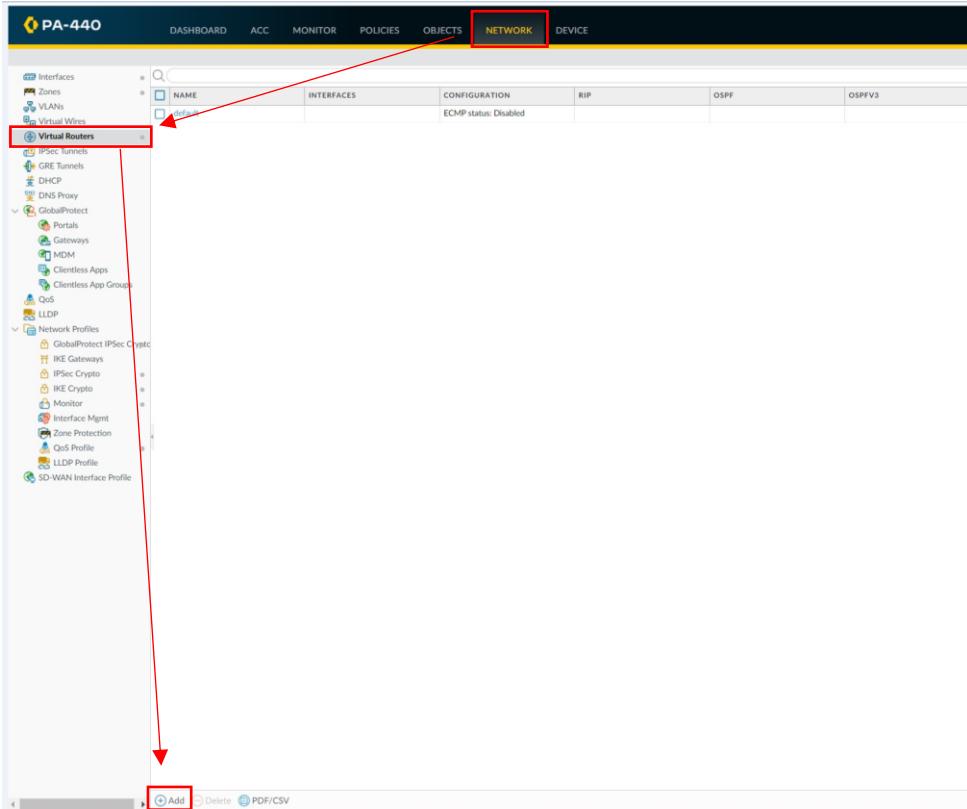
PA-440

DASHBOARD ACC MONITOR POLICIES OBJECTS NETWORK DEVICE

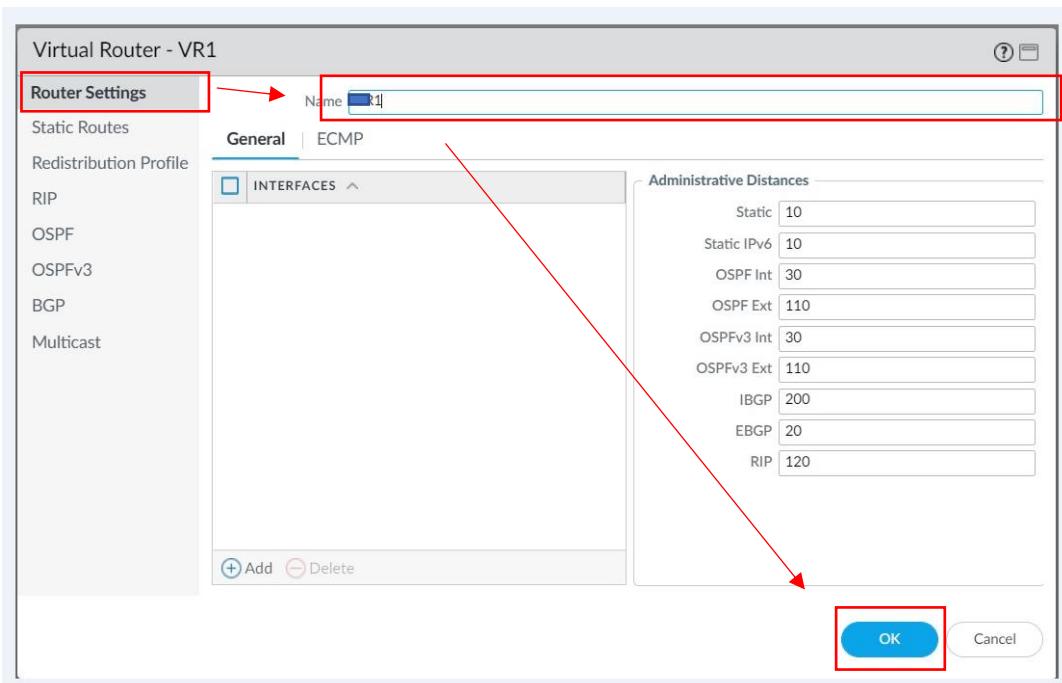
NAME	LOCATION	TYPE	ADDRESS
KAMERA_SUBNET		IP Netmask	10.0.0.0/24
LAB01_SUBNET		IP Netmask	10.0.0.0/24
LAB02_SUBNET		IP Netmask	10.0.0.0/24
LAB03_SUBNET		IP Netmask	10.0.0.0/24
MANAGEMENT_SUBNET		IP Netmask	10.0.0.0/24
PERSONEL_SUBNET		IP Netmask	10.0.0.0/24
SANTRAL_SUBNET		IP Netmask	10.0.0.0/24
SUNUCU_SUBNET		IP Netmask	10.0.0.0/24
TURNIKE_SUBNET		IP Netmask	10.0.0.0/24
WIFI_STAFF_SUBNET		IP Netmask	10.0.0.0/24
WIFI_STUDENT_SUBNET		IP Netmask	10.0.0.0/22
WIFI_SUBNET		IP Netmask	10.0.0.0/24

Sonraki adımda internețe çıkış işlemleri ve layer yönlendirme için static router tanımlamaları yapacağım.

Arayüzümden "NETWORK" menüsüne gidiyor "VIRTUAL ROUTER" sekmesi altında yeni bir router oluşturmak için "ADD" butonuna tıklıyorum.



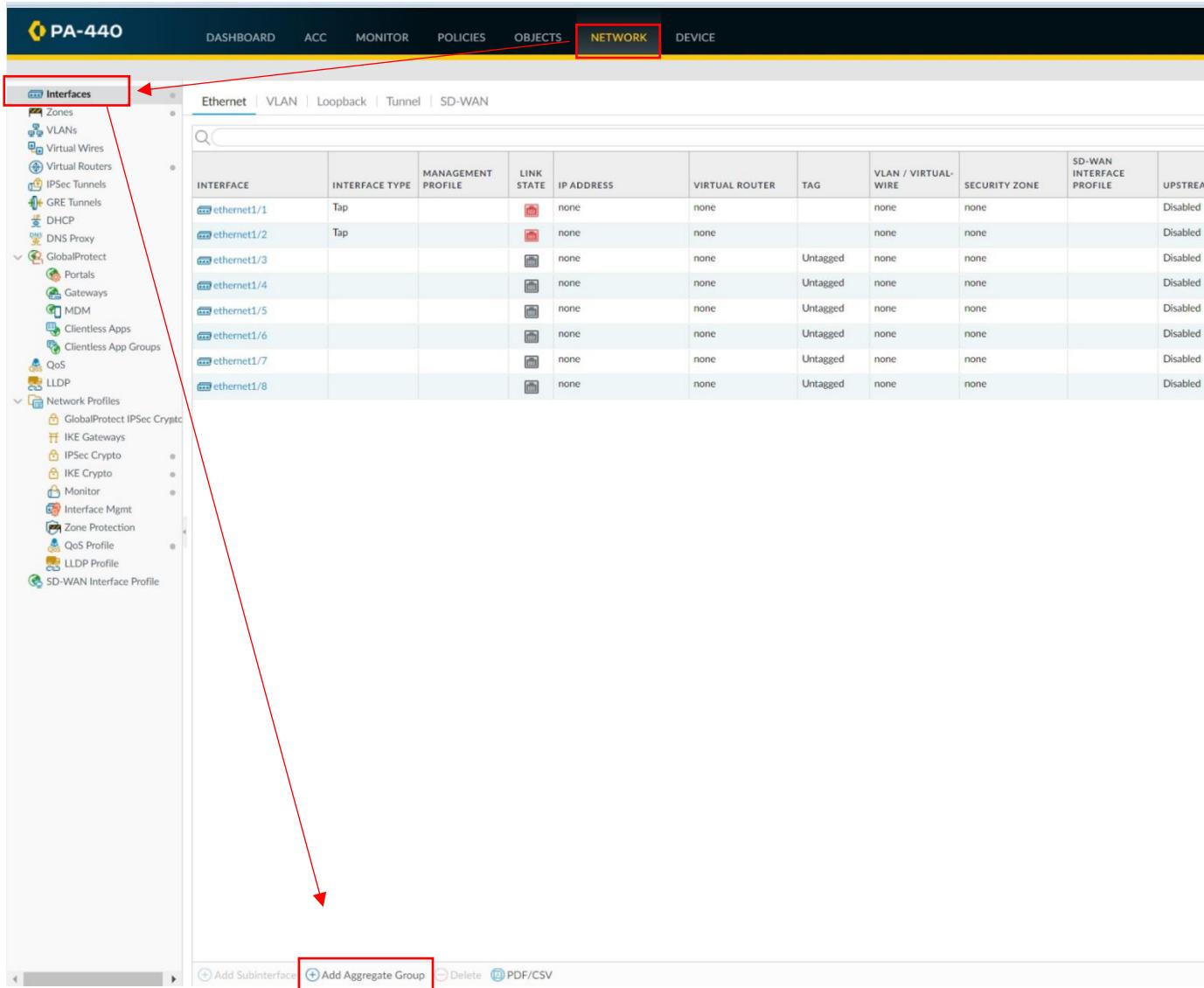
Karşımı gelen menüden ROUTER a bir isim veriyor ve "OK" diyerek işlemimi tamamlıyorum.



Sonraki adımda interface ayarlarını yapmak için “NETWORK” menüsünden “INTERFACES” sekmesine geliyorum. Benim cihazımda 8 adet interface var.

Ben oluşturacağım yapıda 4 adet interfacemi gruplayıp LACP protokolü ile yedekli ve bant genişliğini artıracak şelilde yapılandırıp local networküm hizmet vereceğim , 1 adet interface ise internete çıkış için yapılandırıp WAN zonuna üye yapacağım.

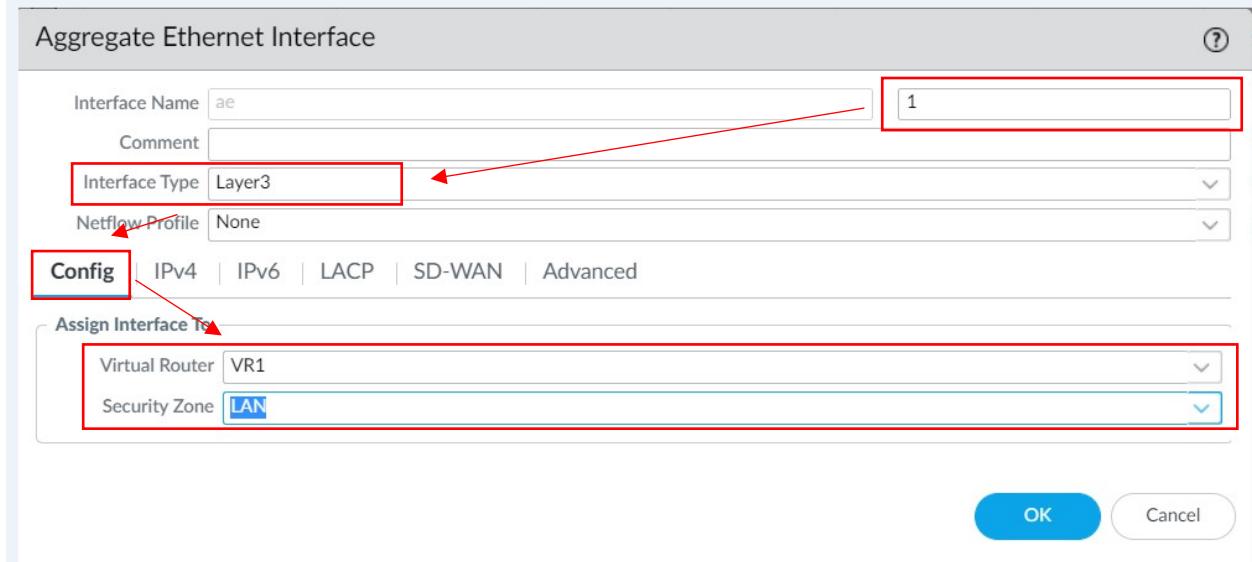
Ben LACP yapılandıracağım için “ADD AGGREGATE GROUP” butonuna tıklıyorum.



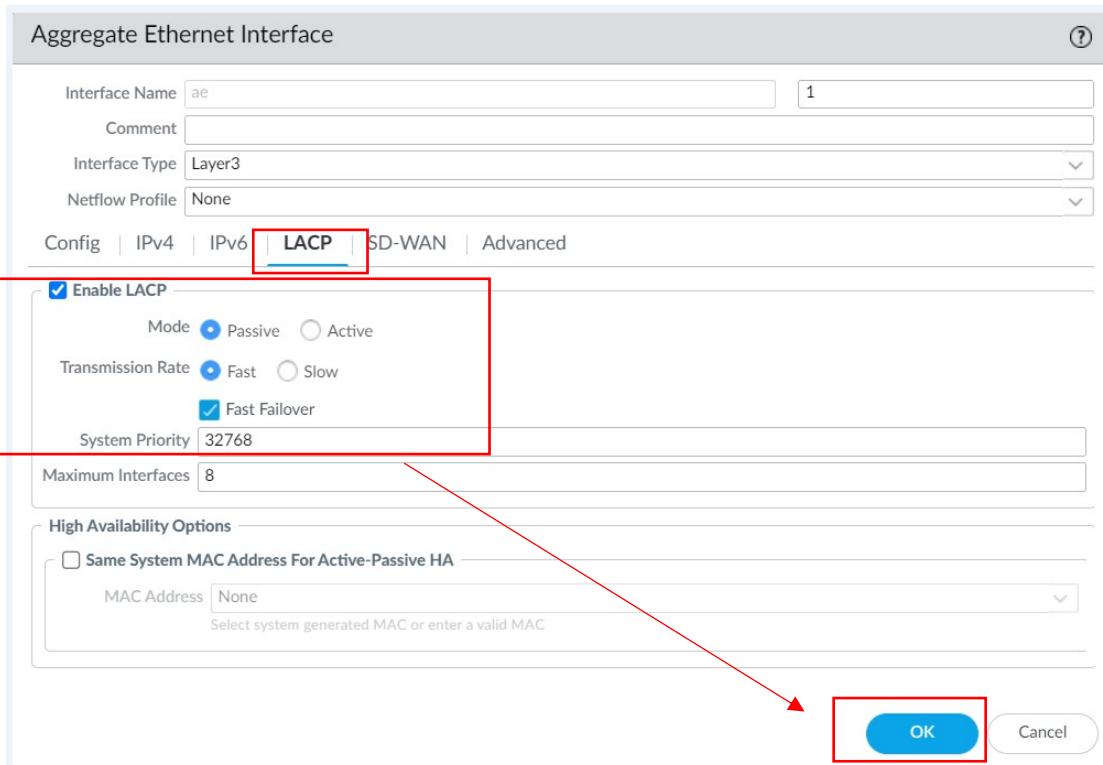
The screenshot shows the PA-440 interface configuration interface. The top navigation bar includes DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, NETWORK (which is highlighted with a red box), and DEVICE. The left sidebar contains sections for Zones, VLANs, Virtual Wires, Virtual Routers, GRE Tunnels, DHCP, DNS Proxy, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, and SD-WAN Interface Profile. The main content area shows a table of interfaces with columns: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, IP ADDRESS, VIRTUAL ROUTER, TAG, VLAN / VIRTUAL-WIRE, SECURITY ZONE, SD-WAN INTERFACE PROFILE, and UPSTREAM. The table lists 8 interfaces (ethernet1/1 to ethernet1/8) all set to Tap type and none for management profile. The bottom of the interface shows buttons for Add Subinterface, Add Aggregate Group (which is highlighted with a red box), Delete, and PDF/CSV.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM
ethernet1/1	Tap		none	none			none	none		Disabled
ethernet1/2	Tap		none	none			none	none		Disabled
ethernet1/3			none	none	Untagged	none	none			Disabled
ethernet1/4			none	none	Untagged	none	none			Disabled
ethernet1/5			none	none	Untagged	none	none			Disabled
ethernet1/6			none	none	Untagged	none	none			Disabled
ethernet1/7			none	none	Untagged	none	none			Disabled
ethernet1/8			none	none	Untagged	none	none			Disabled

Karşıma gelen menüden **LACP** interface için bir Numara verip gerekli interface type, route ve security zone u seçiyorum.



Sonraki adımda yine aynı menüden **“LACP”** sekmesine geliyorum ve ilgili alanları düzenliyorum ve **“OK”** dierek işlemimi tamamlıyorum.



Sonraki adımda oluşturduğum LACP protokolüne interface lerimi üye yapacağım. TAG'leyeceğim diyeyim. "NETWORK" menüsü "INTERFACES" sekmesi altından yapılandırmak istediğim interfacemi seçiyorum. Yukarıdaki adımlarda bahsettiğim gibi ben 4 adet interface yapılandıracağım. Interfacelerim Ethernet 1/2 , Ethernet 1/4 , Ethernet 1/6 ve Ethernet 1/8 ilk interfacemin üzerine tıklıyorum.

The screenshot shows the PA-440 interface configuration page. The left sidebar contains various network and security settings. The main area is titled 'Interfaces' and shows a table of interfaces. The interface 'ethernet1/2' is selected and highlighted with a red box. The table columns include: INTERFACE, INTERFACE TYPE, MANAGEMENT PROFILE, LINK STATE, IP ADDRESS, VIRTUAL ROUTER, TAG, VLAN / VIRTUAL-WIRE, SECURITY ZONE, SD-WAN INTERFACE PROFILE, and UPSTREAM. The interface 'ethernet1/2' is listed as a 'Tap' type interface.

Karşıma gelen menüden interface tipini seçiyor ve LACP grubumu seçip "OK" ile işlemimi tamamlıyorum. Bunu 4,6,8 nolu interfacelerim içinde yapacağım.

The screenshot shows the 'Ethernet Interface' configuration dialog box. The 'Interface Name' is set to 'ethernet1/2'. The 'Interface Type' dropdown is set to 'Aggregate Ethernet' and the 'Aggregate Group' dropdown is set to 'ae1'. The 'OK' button at the bottom right is highlighted with a red box. A red arrow points from the 'OK' button at the bottom right to the 'OK' button at the bottom center of the dialog.

Ben network topolojime göre interfacelerimi yapılandırdım. Aşağıda görüldüğü üzere LACP protokolüne üye interfaceler ve ana LACP Grubum gözükmekte.

INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1	Tap		Up	none	none	none	none	none		Disabled		
ethernet1/2	Aggregate (xc1)		Up	none	none	Untagged	none	none		Disabled		
ethernet1/3			Up	none	none	Untagged	none	none		Disabled		
ethernet1/4	Aggregate (xc1)		Up	none	none	Untagged	none	none		Disabled		
ethernet1/5			Up	none	none	Untagged	none	none		Disabled		
ethernet1/6	Aggregate (xc1)		Up	none	none	Untagged	none	none		Disabled		
ethernet1/7			Up	none	none	Untagged	none	none		Disabled		
ethernet1/8	Aggregate (xc1)		Up	none	none	Untagged	none	none		Disabled		
air1	Layer3		Up	none	VR1	Untagged	none	LAN		Disabled		

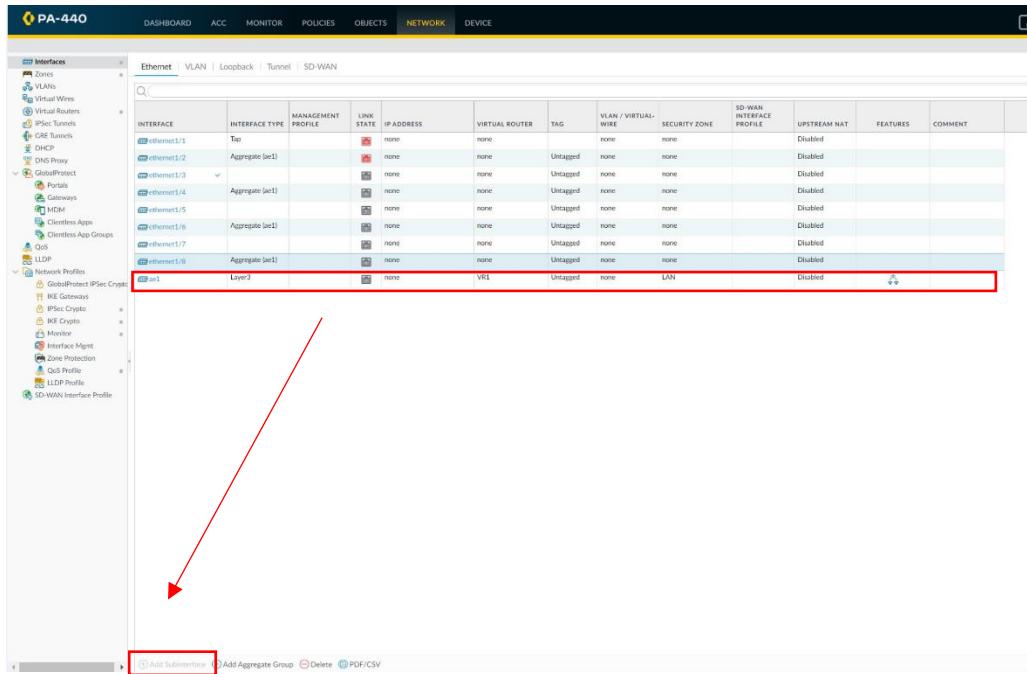
Şimdiye kadar zone tanımları, adres tanımları, genel interface tanımlamaları ve router tanımlaması yaptım.

Netwokumuzu ayağa kaldırıp interne e ulaşmak için gerekli ayarlarımı devam ediyorum. Yukarıdaki adımda adres tanımlamalarında birden fazla gateway adres tanımı yaptım.

Bu nedenle birden fazla netwoküm olduğu için one a stick uygulaması yapacağım. Benim 12 adet netwoküm var. bu networklerin her birine vlan atayıp aynı zamanda gateway tanımlayarak LACP grubu altında sub interfaceler oluşturacağım.

Bu nedenle Yine “NETWORK” menüsü “INTERFACES” sekmesine giderek subinterfaceler oluşturmaya başlayalım.

Karşıma gelen menüden **AE1** interface seçili iken **“ADD SUBINTERFACE”** butonuna tıklıyorum.

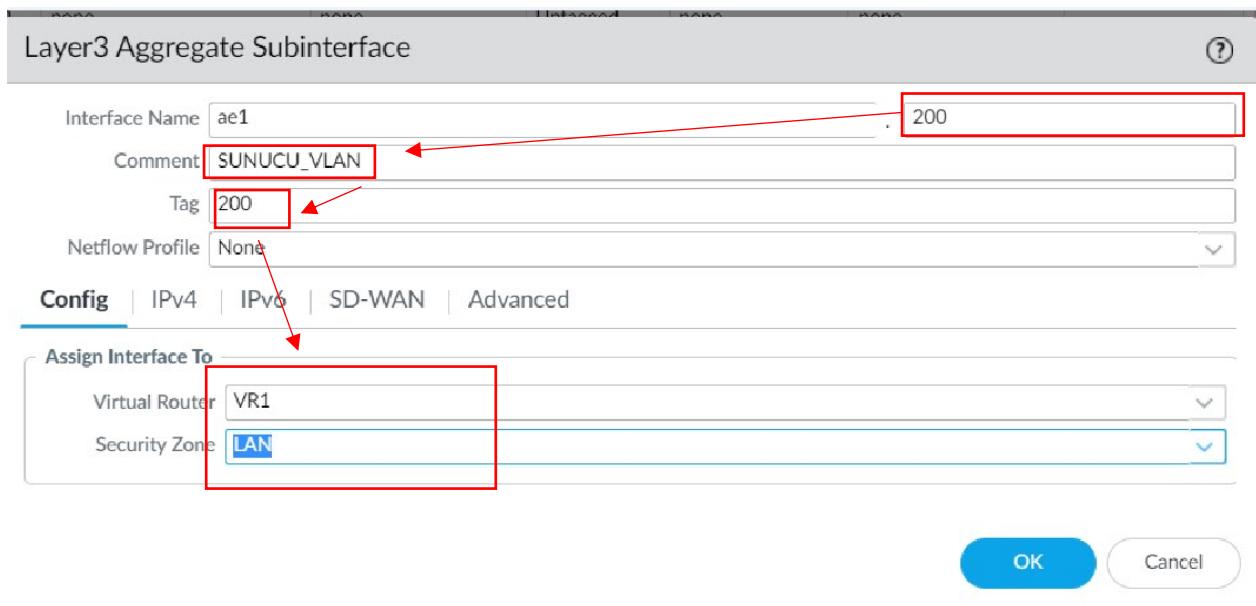


The screenshot shows the PA-440 interface list. The interface **ae1** is selected and highlighted with a red box. A red arrow points from the text above to this red box. At the bottom of the interface list, there is a toolbar with several buttons. The **“Add Subinterface”** button is highlighted with a red box, and a red arrow points from the text above to this button.

Karşıma gelen menüdün ilk sub interfacemı oluşturmak için gerekli alanları dolduruyorum.

Interface 'e bir **vlan id** atıyorum, açıklama giriyorum. **Tag** kısmına da aynı şekilde vlan id bilgimi giriyorum. Burası mutlaka vlan id ile aynı olmak zorunda.

Interface için router ve zone seçimini yapıyorum. Oluşturacağım sub interfaceler local network olacağı için **LAN** zonu seçiyorum.

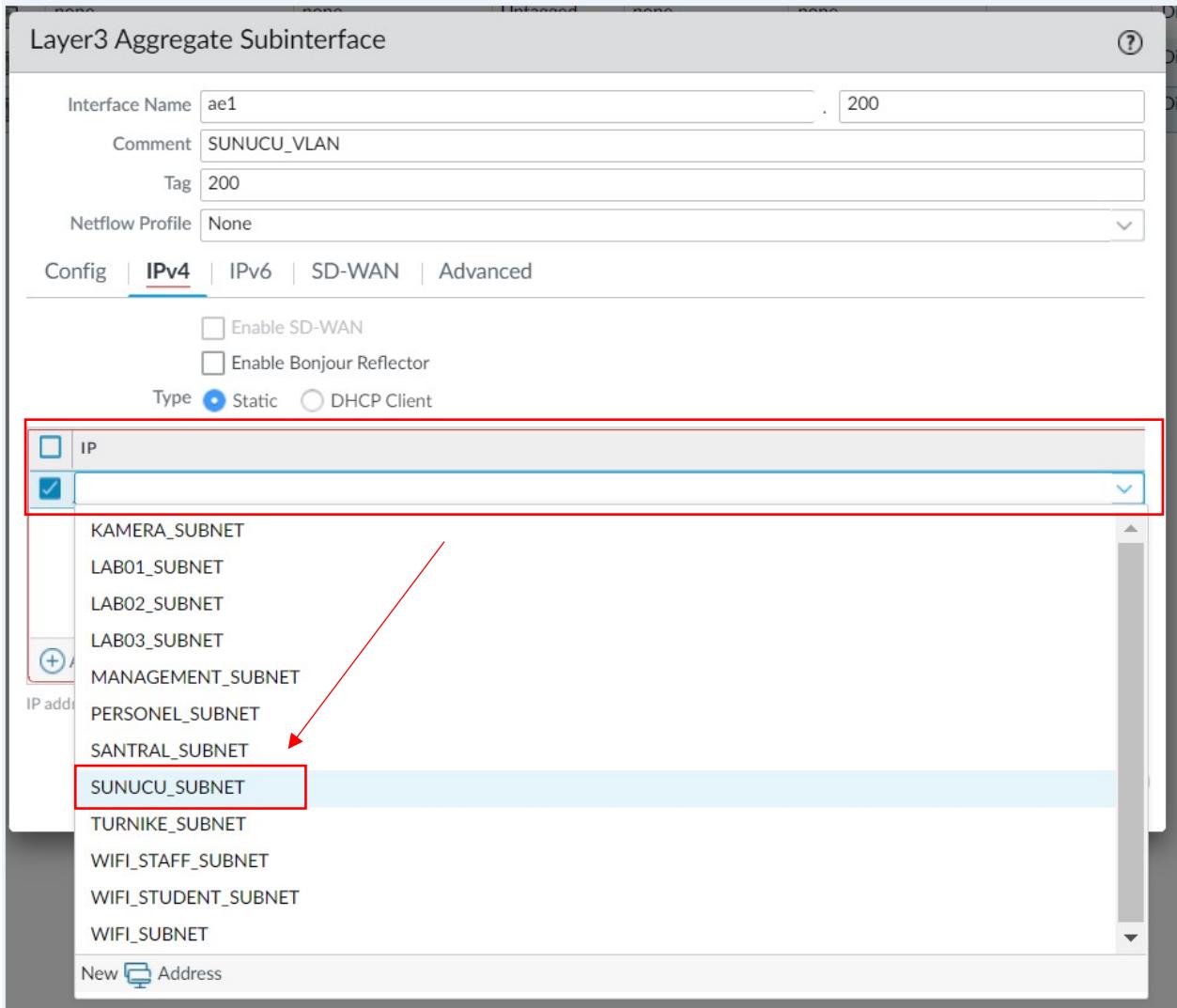


The screenshot shows the **Layer3 Aggregate Subinterface** configuration dialog. Several fields are highlighted with red boxes and arrows pointing to them from the text above:

- Interface Name:** **ae1** (highlighted with a red box)
- Comment:** **SUNUCU_VLAN** (highlighted with a red box)
- Tag:** **200** (highlighted with a red box)
- Virtual Router:** **VR1** (highlighted with a red box)
- Security Zone:** **LAN** (highlighted with a red box)

At the bottom right of the dialog are the **OK** and **Cancel** buttons.

Sonraki adımda interfacemi ip atayarak gateway tanımlaması yapacağım. "IPV4" sekmesine gelerek üst adımlarda tanımladığım adresimi seçiyorum ve "OK" dierek işlemimi tamamlıyorum.

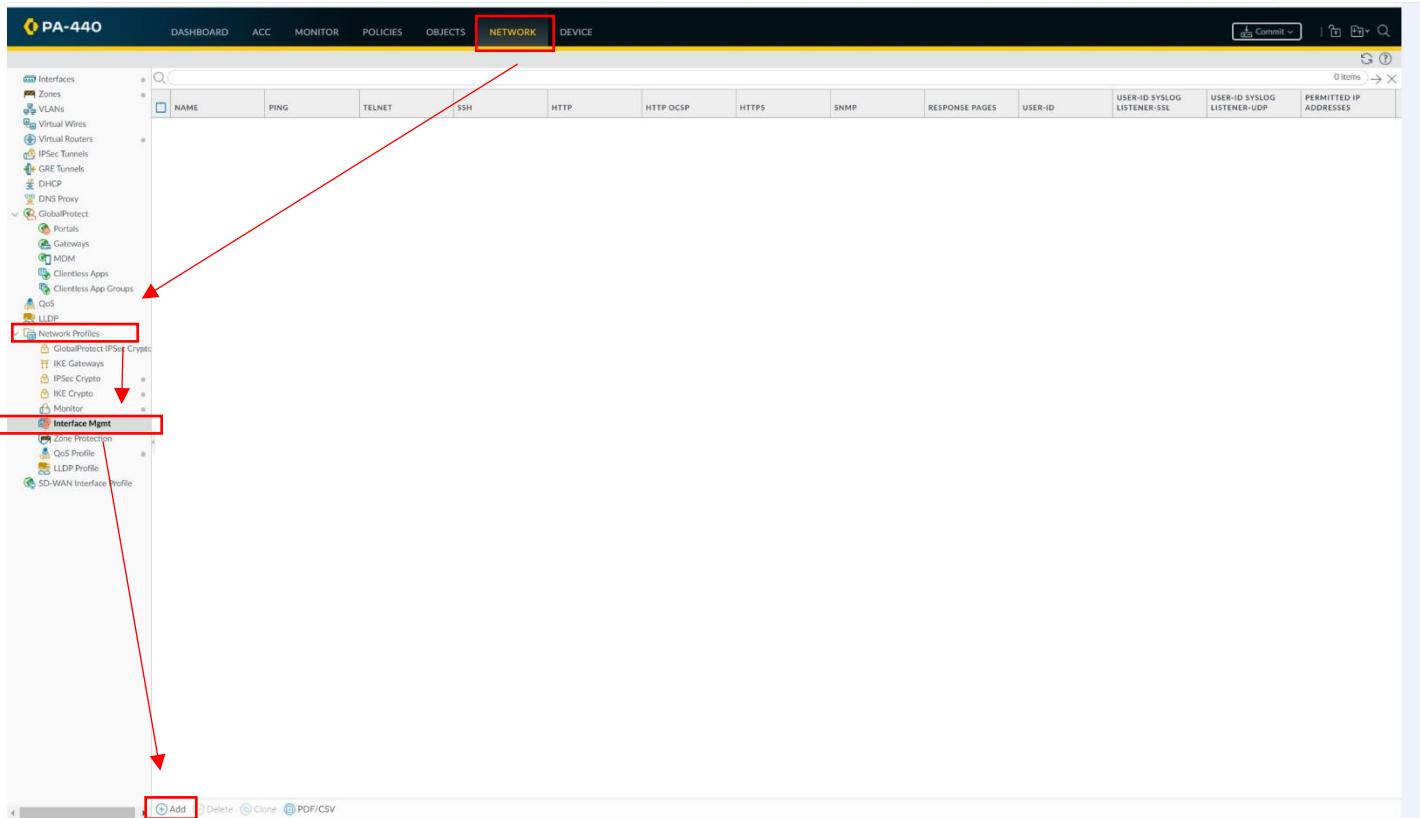


Sonraki adımda yine aynı yöntemi kullanarak diğer sub interfface'leri oluşturacağım.

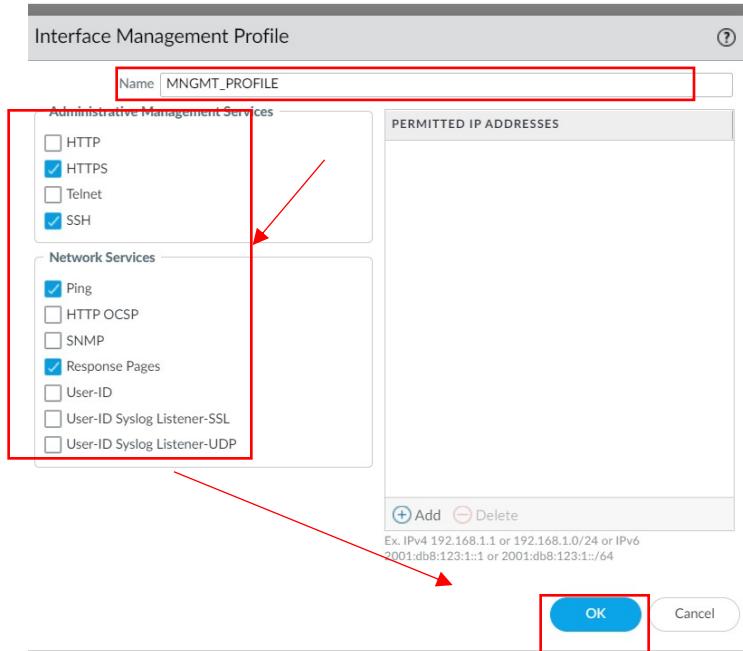
Ama öncesinde bu interfacelerden PALO ALTO cihazıma web, ssh üzerinden ulaşmak için bir management profili oluşturacağım.

NETWORK menüsü altından Network Profiles altından Interface Mgmt seçeneğine geliyorum.

ADD butonuna tıklıyorum.



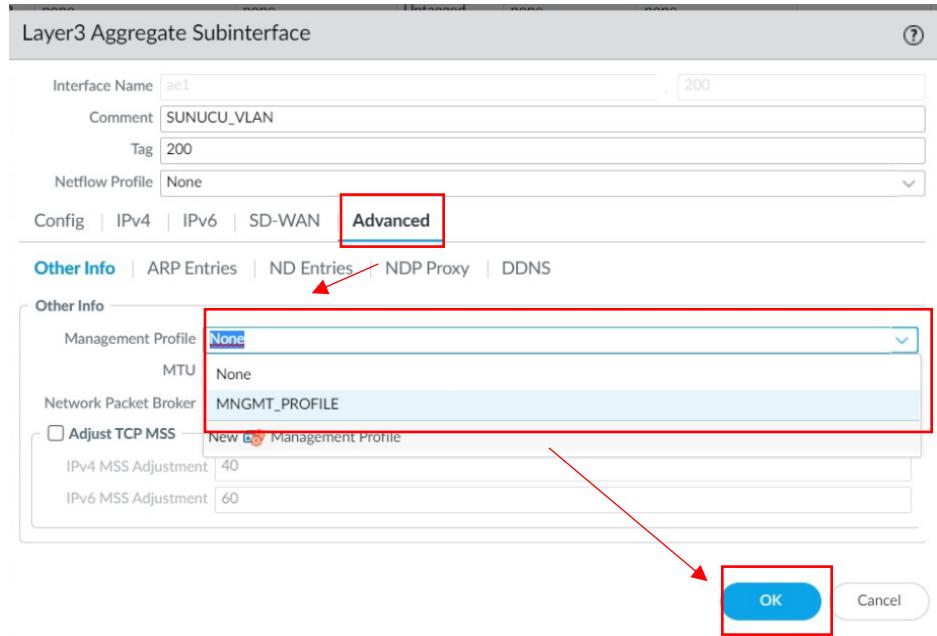
Karşıma gelen menüden profilime isim verip ilgili protokollerimi seçip "OK" ile işlemimi tamamlıyorum.



Sonraki adımda tanımlamış olduğum profilimi yine bir önceki adımda oluşturmuş olduğum interfacemi tanımlıyorum.

İlgili interfacemi seçip **Advanced** sekmesinden profilimi seçerek **OK** dierek işlemimi tamamlıyorum.

Eğer bu tanımlamayı yapmazsanız ilgili interfaceden PALO ALTO arayüzüze ulaşamazsınız.



Sonraki adımda kalan 11 adet sub interfacemi tanımlayıp aynı ayarları adım adım yapıyorum.

Network Profiles	Interface	Type	Actions
GlobalProtect IPSec Crypto	ae1	Layer3	
IKE Gateways	ae1.200	Layer3	
IPSec Crypto	ae1.201	Layer3	
IKE Crypto	ae1.202	Layer3	
Monitor	ae1.203	Layer3	
Interface Mgmt	ae1.204	Layer3	
Zone Protection	ae1.205	Layer3	
QoS Profile	ae1.206	Layer3	
LLDP Profile	ae1.207	Layer3	
SD-WAN Interface Profile	ae1.208	Layer3	
	ae1.209	Layer3	
	ae1.250	Layer3	
	ae1.251	Layer3	

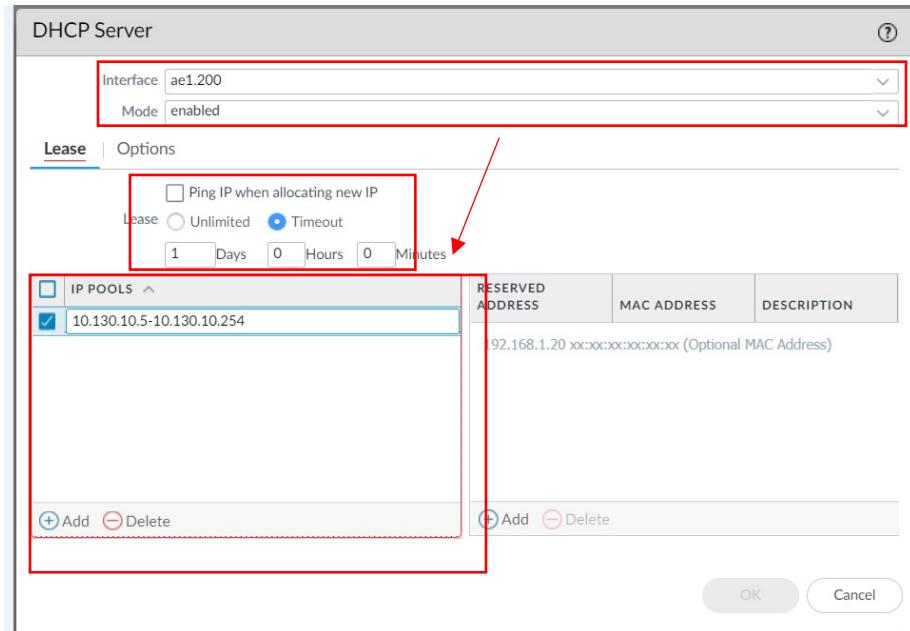
Şimdi oluşturmuş olduğum bu sub interfacelere DHCP den ip dağıtıcağım. NETWORK menüsünden DHCP sekmesine gelip ADD diyorum.

The screenshot shows the PA-440 interface with the following highlights:

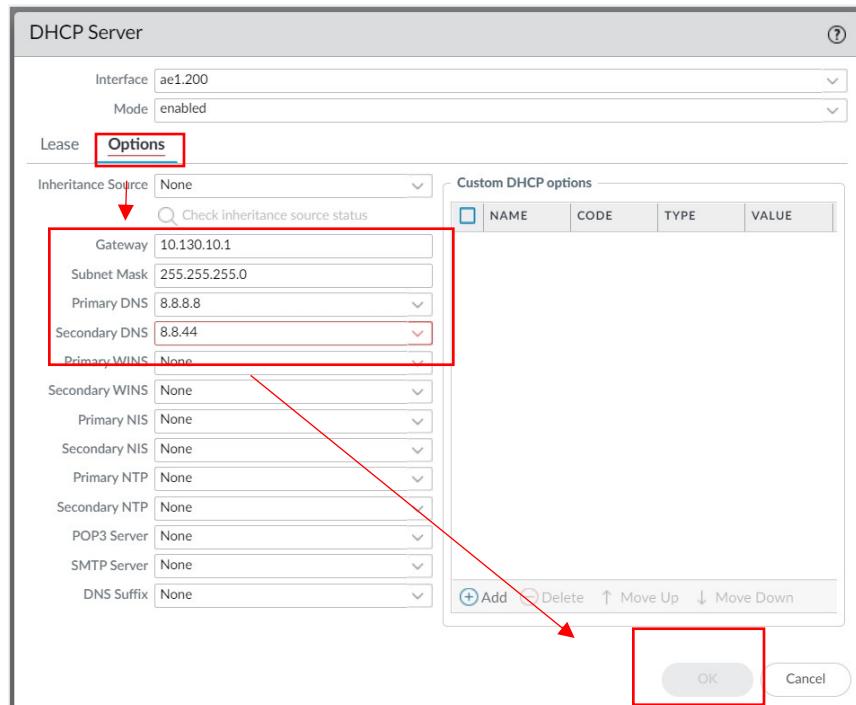
- Top Navigation Bar:** DASHBOARD, ACC, MONITOR, POLICIES, OBJECTS, **NETWORK** (highlighted with a red box), DEVICE.
- Left Sidebar:** A tree view of configuration objects. The **DHCP** node is expanded, with **DHCP Server** highlighted with a red box. Other nodes include Interfaces, Zones, VLANs, Virtual Wires, Virtual Routers, IPSec Tunnels, GRE Tunnels, GlobalProtect, Portals, Gateways, MDM, Clientless Apps, Clientless App Groups, QoS, LLDP, Network Profiles, and SD-WAN Interface Profile.
- Center Content Area:** A table header for "DHCP Server" with columns: INTERFACE, MODE, PROBE IP, and OPTIONS. The table body is currently empty.
- Bottom Action Bar:** Buttons for **+ Add**, **Delete**, and **PDF/CSV**.

A red arrow points from the **+ Add** button at the bottom to the **+ Add** button in the table header, indicating the path to add a new DHCP server entry.

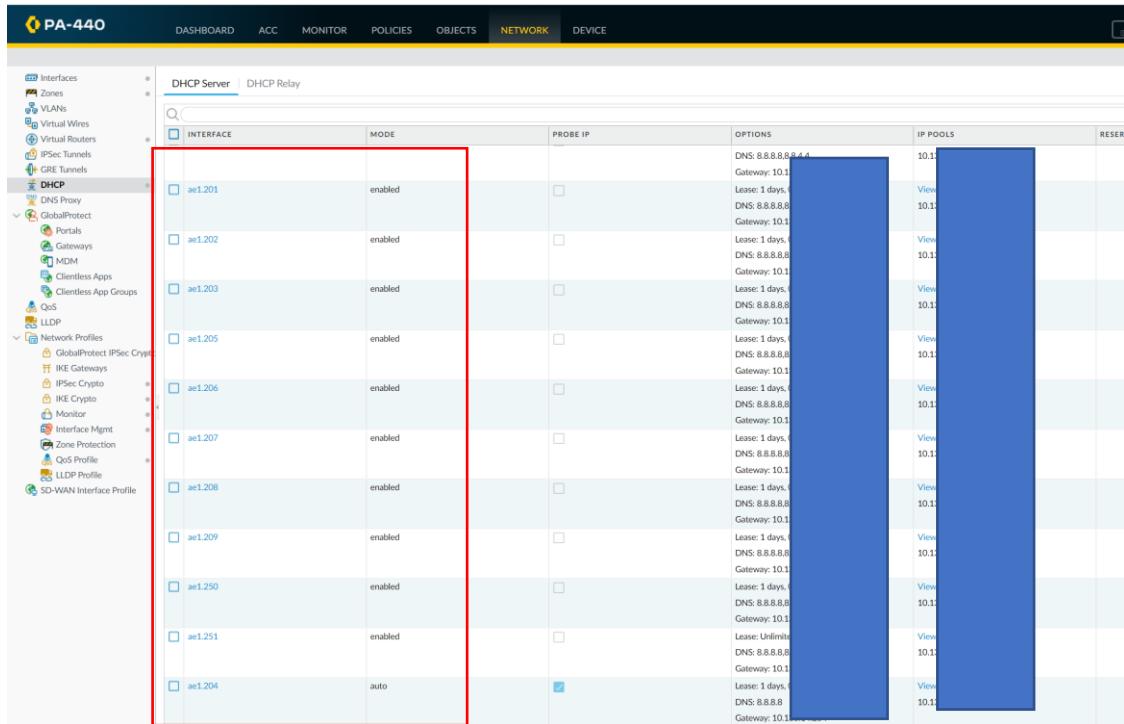
Karşıma gelen ekranın ip dağıtmak istediği interface'ı seçiyorum. Mode kısmından hemen devreye girmesi için enable seçeneğini seçiyorum. IP pool kısmından add diyerek dağıtilacak ip aralığını tanımlıyorum ayrıca dağıtilacak ip ne kadar kiralanacak süresini seçiyorum.



Sonraki adımda Options sekmesine gelerek DHCP serverim için gateway, subnet ve dns tanımı yapıyor ve ok ile işlemimi tamamlıyorum.



DHCP tanımlama olayını diğer 11 interfacem içinde yapıyorum. Mantık aynı. Aşağıda görüldüğü üzere tüm sub interfaceler için dhcp hizmeti devreye girdi.



INTERFACE	MODE	PROBE IP	OPTIONS	IP POOLS	RESERV
ae1.201	enabled		DNS: 8.8.8.8, 8.8.8.4, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.202	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.203	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.205	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.206	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.207	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.208	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.209	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.250	enabled		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	
ae1.251	enabled		DNS: 8.8.8.8, Lease: Unlimite, 8.8.8.8, Gateway: 10.1	10.1	
ae1.204	auto		DNS: 8.8.8.8, Lease: 1 days, 8.8.8.8, Gateway: 10.1	10.1	

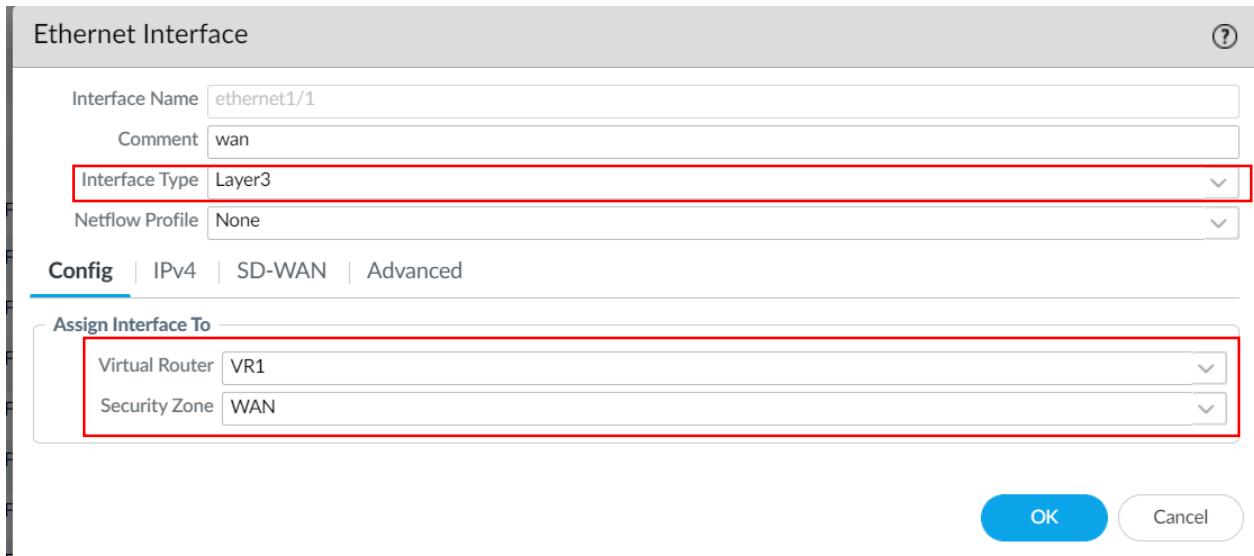
Sıradaki adımda internette çıkışta kullanacağım interfacemı yapılandıracağım. Bu nedenle ilgili interfacemı seçiyorum.

Ben cihazımın **Ethernet 1/1** portunu internețe çıkış için yapılandıracağım.



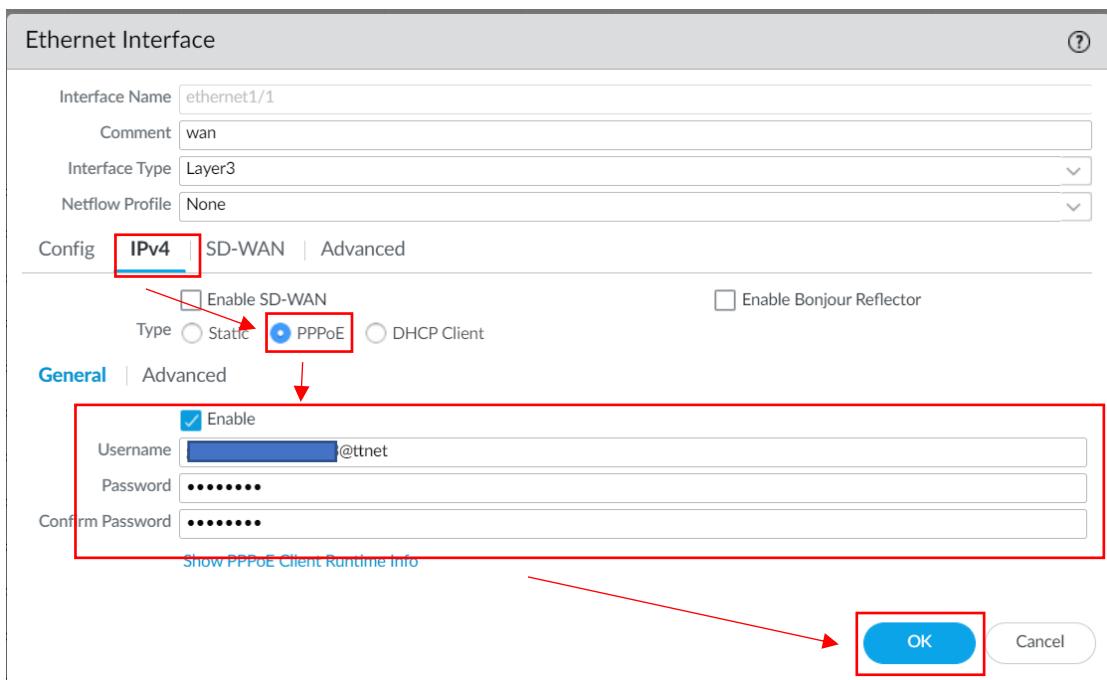
INTERFACE	INTERFACE TYPE	MANAGEMENT PROFILE	LINK STATE	IP ADDRESS	VIRTUAL ROUTER	TAG	VLAN / VIRTUAL-WIRE	SECURITY ZONE	SD-WAN INTERFACE PROFILE	UPSTREAM NAT	FEATURES	COMMENT
ethernet1/1						Untagged	none	WAN		Disabled	wan	

Karşıma gelen menüden interface type seçiyorum. Aynı zamanda yukarıdaki adımlarda oluşturduğumuz router ve zone tanımını yapıyorum. İnternete çıkışım ZONE u WAN olarak isimlendirdiğim için WAN zonu seçiyorum.



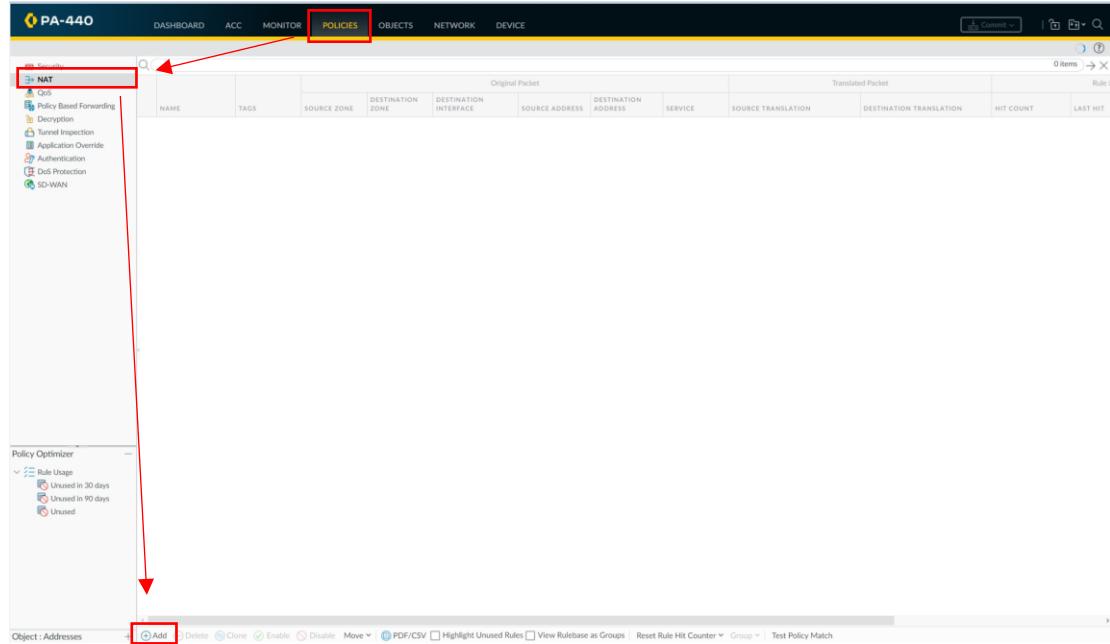
Sonraki internete çıkış bilgilerimi tanımlamak için **IPv4** sekmesine geliyorum. Ben örneğimde fiber gelene kadar DLS hat kullanacağım için PPPoE seçeneği ile ilerliyorum. Sizde genellikle fiber bağlantı olacağı için Static ile devam edebilirsiniz.

Gerekli bilgilerimi girdikten sonra **"OK"** diyerek işlemimi tamamlıyorum.



Sonraki adımda Oluşturduğum networklerin dış ip bilgisine çevrilerek internețe çıkabilmesi için bir NAT kuralı oluşturacağım.

Arayüzden “POLICIES” menüsü altından “NAT” sekmesine geliyorum. Yeni bir yönlendirme kuralı eklemek için “ADD” butonuna tıklıyorum.

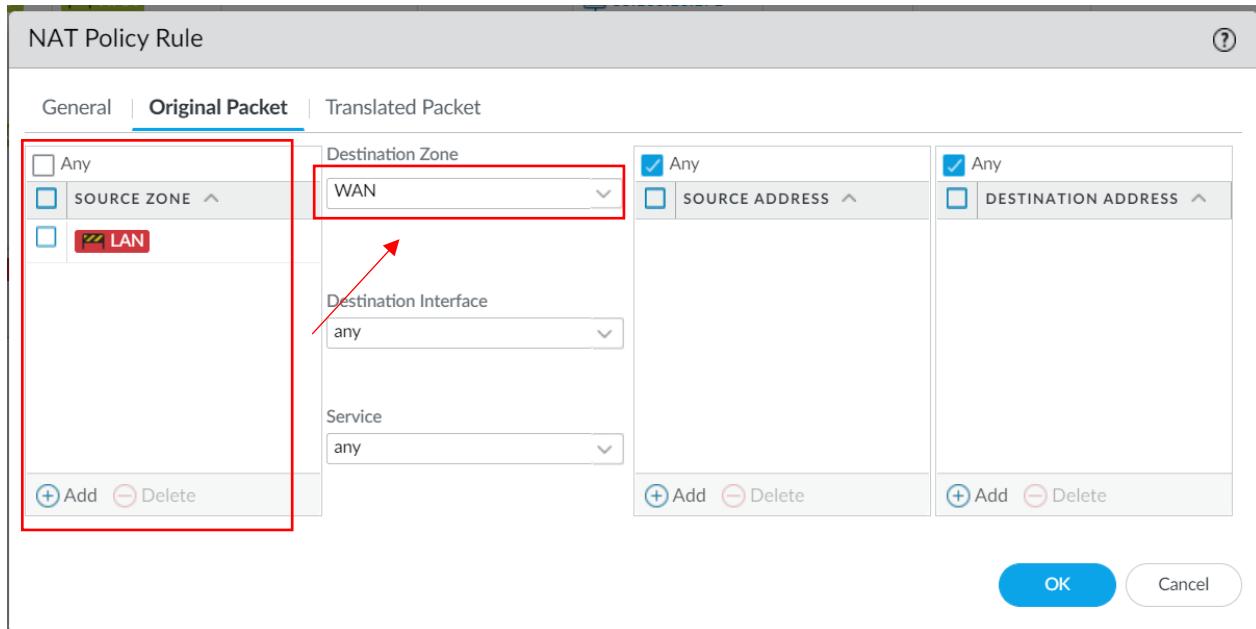


Karşımı gelen menüden NAT a isim veriyorum.

The screenshot shows the 'NAT Policy Rule' configuration dialog. The 'General' tab is selected. The 'Name' field is highlighted with a red box and contains the value 'static_nat_1'. Other fields in the General tab include 'Description' (empty), 'Tags' (empty), 'Group Rules By Tag' (set to 'None'), 'NAT Type' (set to 'ipv4'), and 'Audit Comment' (empty). Below the General tab is an 'Audit Comment Archive' section. At the bottom right are 'OK' and 'Cancel' buttons.

Sonraki adımda "ORIGINAL PACKET" sekmesine gelip ilgili alanları görseldeki gibi dolduruyorum.

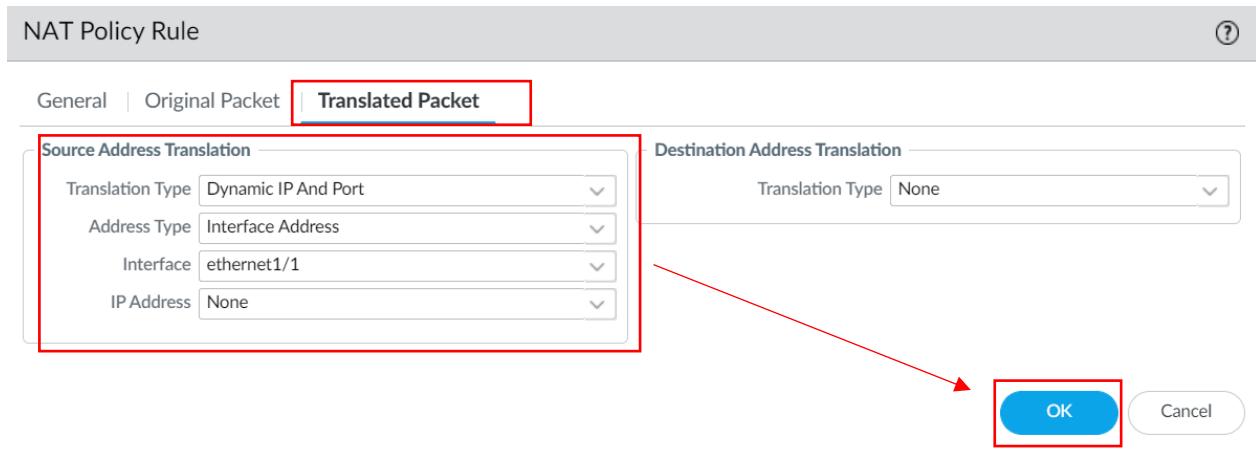
Lan zonumdaki networkler internețe çıkışta WAN zonumdaki interfacemi kullanacak.



Sonraki adımda "TRANSLATED PACKET" sekmesinden iç netwokümden ip ve port bilgilerimin değiştilmesini istediğim için ilgili alanları seçiyorum.

Interface kısmında internețe çıkış için belirlediğim ve **WAN** zonuna dahil ettiğim portumu seçiyorum.

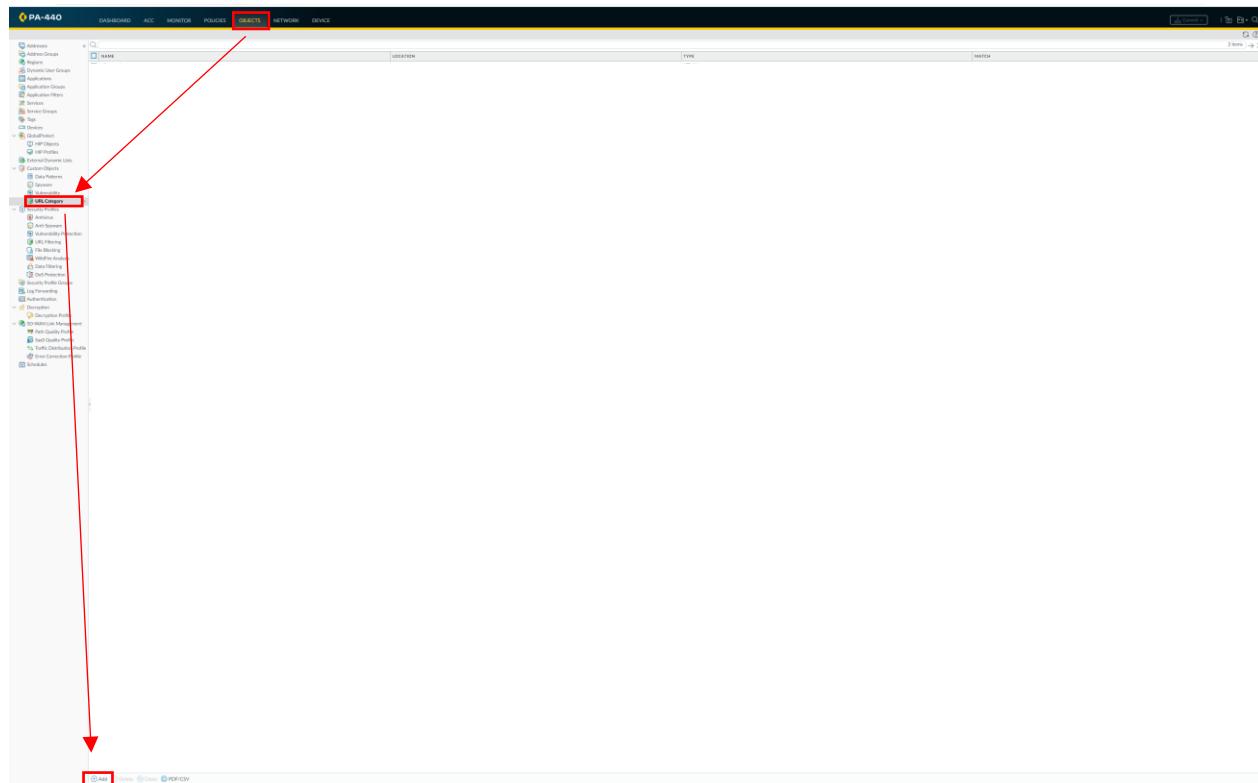
"OK" diyerek işlemimi tamamlıyorum.



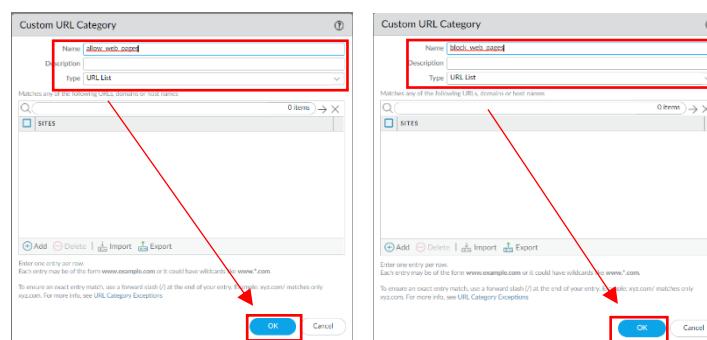
Şimdiki adımda "OBJECT" menüsü altından "URL CATEGORY" sekmesine gelerek ADD butonu ile "ALLOW" ve "BLOCK" adında 2 adet kişisel kategori ekleyeceğim.

Güvenlik politikası oluşturuken bu kategorileri kullanarak istek dahilinde erişim vermek istediğim web sitelerini "ALLOW" ayrıca yasaklamak istediklerimi "BLOCK" kategorisine ekleyeceğim.

ADD butonuna tıklıyorum.

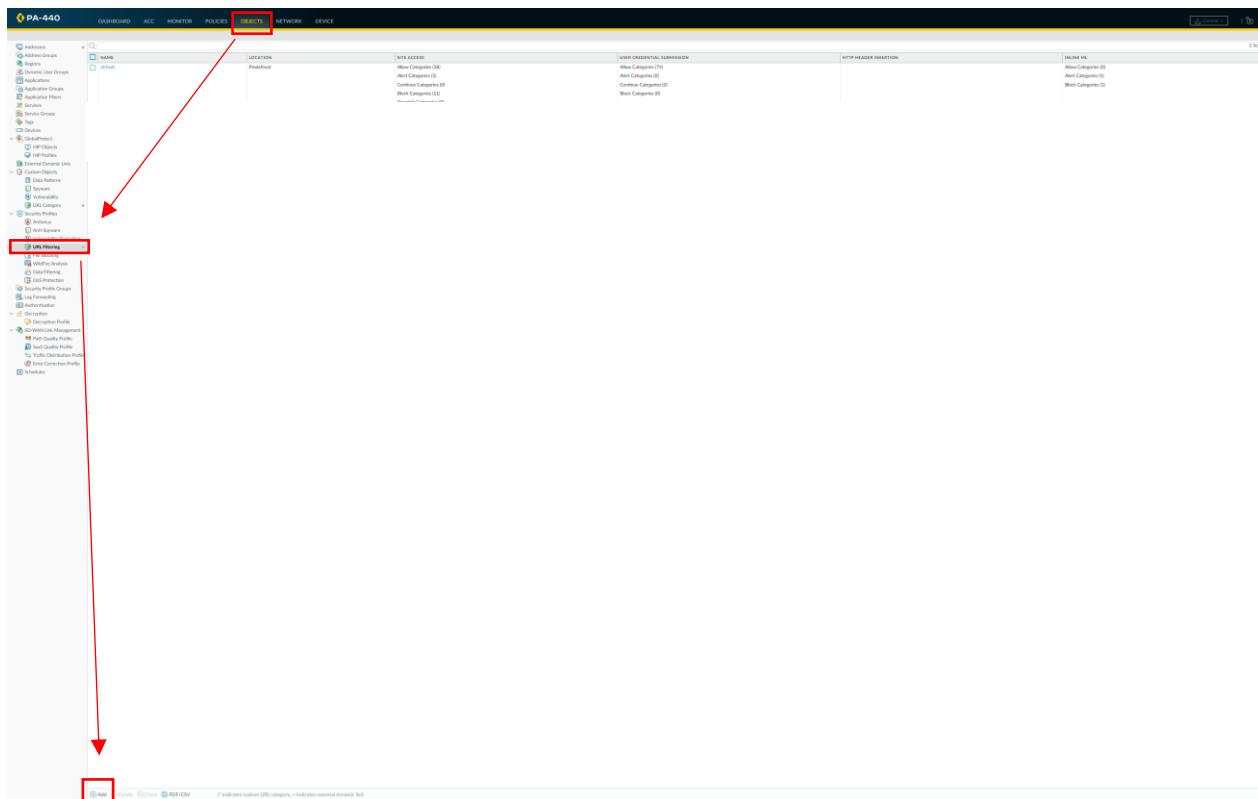


Karşıma gelen menüden bir isim belirliyorum. Type kısmını URL List seçip "OK" diyerek işlemimi tamamlıyorum. Aynı işlemi "BLOCK" kategorisi oluşturmak içinde tekrarlıyorum.

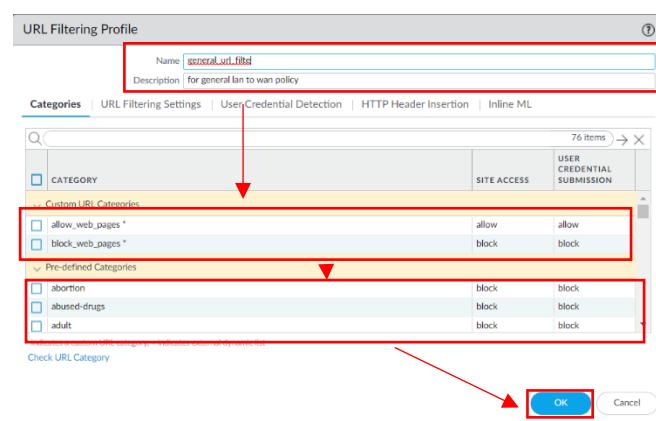


Sonraki adımda bir web politikası oluşturacağım. Yine “OBJECTS” menüsü altından “URL FILTERING” sekmesine geliyorum. ADD diyerek yeni bir URL filtresi oluşturacağım. Oluşturacağım bu filtme benim internete çıkışta kullanıcıları kategoriz bazlı denetime sokacak allow verdigim kategorilerde erişim sağlanırken block verdigim kategorilerde erişim kısıtlaması sağlanacaktır.

Default olarak gelen bir filtre var ben bunu kullanmayacağım. O nedenle kendim oluşturmak için ADD butonuna tıklıyorum.



Karşıma gelen menüden filtreme isim veriyorum. Bir üstte oluşturduğum kişisel kategorilerimde görünüyor. Yasaklamak istediğim kategorilere “BLOCK” izin vermek istediklerime “ALLOW” seçerek ve “OK” diyerek işlemimi tamamlıyorum.



Bu işlemide tamamladıktan sonra kullanıcıları internete çıkması için genel bir Kural oluşturacağım. Oluşturduğum bu kurala URL filtremizi de ekleyip denetim sağlayacağım.

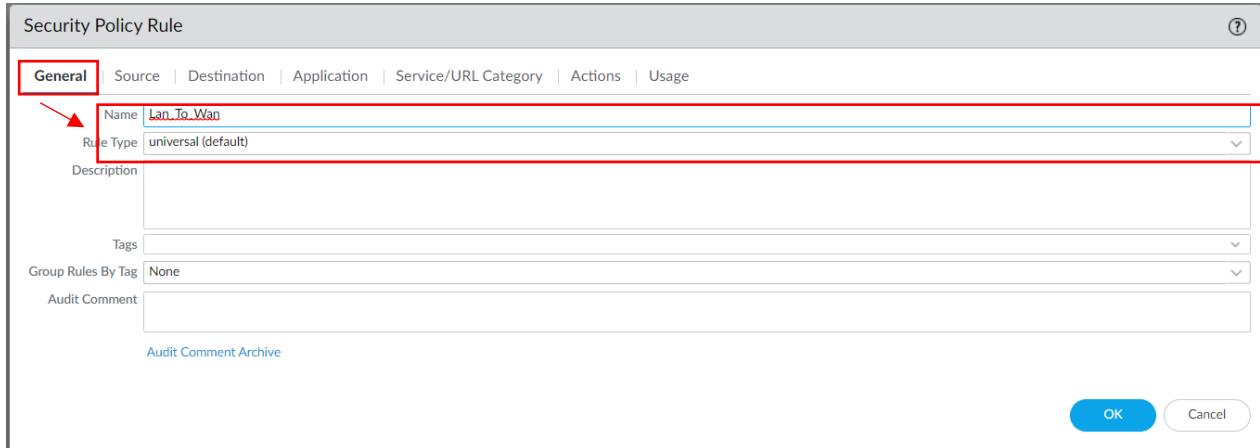
Arayüzden "POLICIES" menüsünden "SECURITY" sekmesine geliyorum. ADD diyerek yeni bir Kural oluşturuyorum.

The screenshot shows the PA-440 device management interface. The top navigation bar includes links for DASHBOARD, ACC, MONITOR, POLICIES (which is highlighted with a red box and has a red arrow pointing to it from the left sidebar), OBJECTS, NETWORK, and DEVICE. The left sidebar has a 'Security' section with various icons and a 'Policy Optimizer' section with a list of items like 'Unused Apps' and 'Unused'.

The main content area displays a table for creating a new policy. The table has columns for Source and Destination, and a 'Rule Usage' section at the bottom. The 'Source' section includes columns for NAME, TAGS, TYPE, ZONE, ADDRESS, USER, DEVICE, and ZONE. The 'Destination' section includes columns for ADDRESS, DEVICE, APPLICATION, SERVICE, ACTION, PROFILE, OPTIONS, HIT COUNT, LAST HIT, FIRST HIT, APPS SEEN, DAYS APPS, MODIFIED, and CREATED. The 'Rule Usage' section includes columns for HIT COUNT, LAST HIT, FIRST HIT, APPS SEEN, DAYS APPS, MODIFIED, and CREATED.

At the bottom of the interface, there are buttons for 'Add' (highlighted with a red box and a red arrow pointing to it), 'Delete', 'Clone', 'Override', 'Revert', 'Enable', 'Disable', 'Move', 'PDF/CSV', 'Highlight Unused Rules', 'View Rulebase as Groups', 'Reset Rule Hit Counter', 'Group', and 'Test Policy Match'. The status bar at the bottom shows 'Object: Addresses'.

Karşımıza gelen menüden kuralımı isim belirliyorum. Rule Type kısmından hem local e hemde wan a ulaşmak için universal seçiyorum.



Security Policy Rule

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

Name: Lan_To_Wan
Rule Type: universal (default)

Description:

Tags:

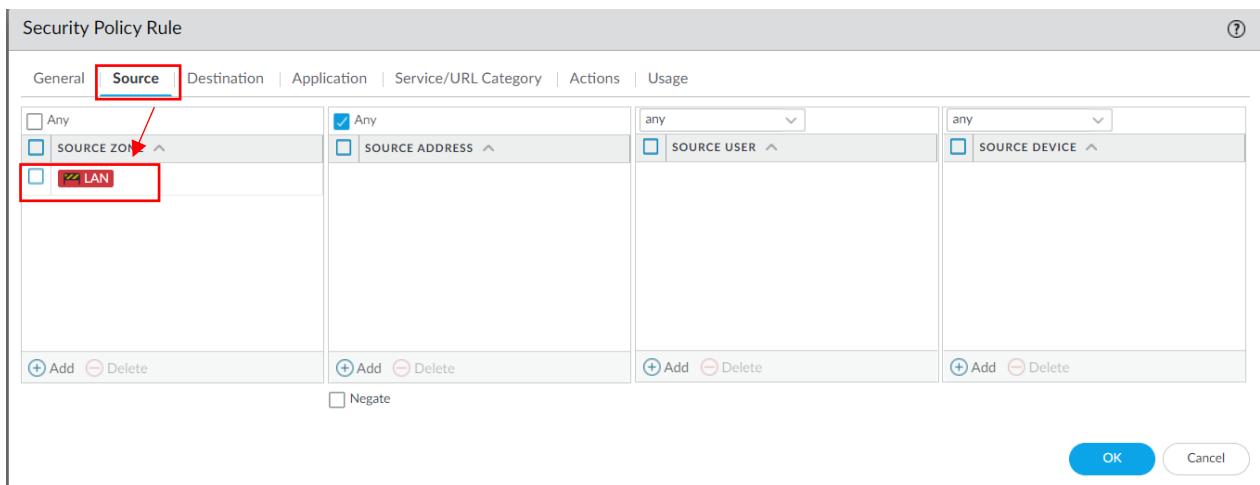
Group Rules By Tag: None

Audit Comment:

Audit Comment Archive

OK Cancel

Menüden "SOURCE" sekmesine geliyorum. Buradan kaynak zonu mu seçiyorum. Internete çıkarmak istediğim network leri. Diğer seçenekleri any olarak bırakıyorum.



Security Policy Rule

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

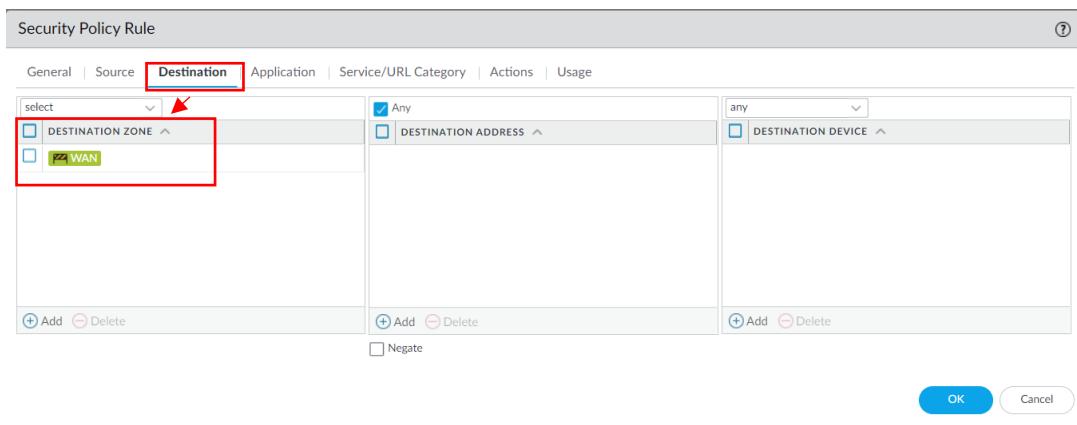
<input type="checkbox"/> Any	<input checked="" type="checkbox"/> SOURCE ZONE ^	<input type="checkbox"/> Any	<input type="checkbox"/> SOURCE ADDRESS ^	any	<input type="checkbox"/> SOURCE USER ^	any	<input type="checkbox"/> SOURCE DEVICE ^
<input type="checkbox"/> LAN			<input type="checkbox"/> SOURCE ADDRESS		<input type="checkbox"/> SOURCE USER		<input type="checkbox"/> SOURCE DEVICE

+ Add - Delete + Add - Delete + Add - Delete + Add - Delete

Negate

OK Cancel

Bu işlemide tamamladıktan sonra. Menüden "DESTINATION" sekmesine geliyorum. Hedef zone olarak WAN seçiyorum. Diğer seçenekleri any olarak bırakıyorum.



Security Policy Rule

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

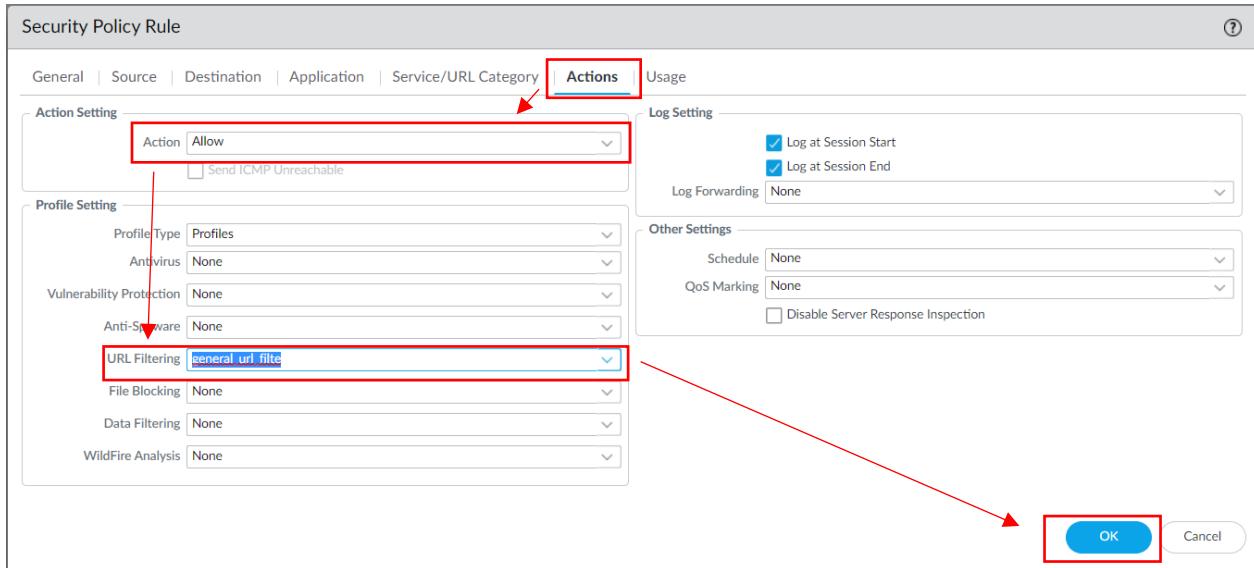
select	<input checked="" type="checkbox"/> DESTINATION ZONE ^	<input type="checkbox"/> Any	<input type="checkbox"/> DESTINATION ADDRESS ^	any	<input type="checkbox"/> DESTINATION DEVICE ^
	<input type="checkbox"/> WAN				

+ Add - Delete + Add - Delete + Add - Delete

Negate

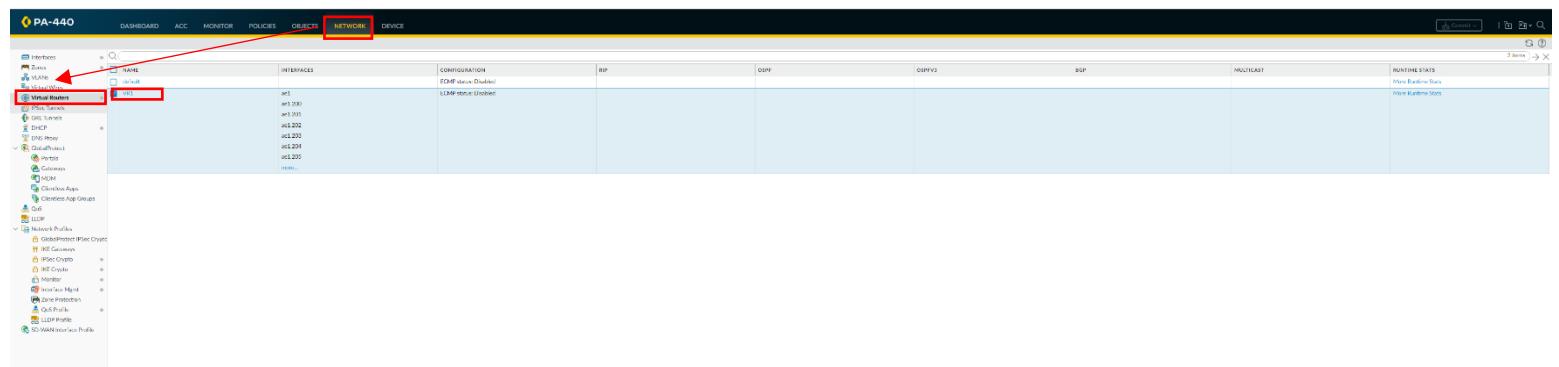
OK Cancel

Sonraki adımda yine menüden “ACTIONS” sekmesine gelerek kuralımı “ALLOW” ile izin veriyor, yukarıdaki adımlarda oluşturmuş olduğum URL Filtreyi seçiyorum. Aynı zamanda log için ilgili alanları seçip “OK” diyerek işlemimi tamamlıyorum.

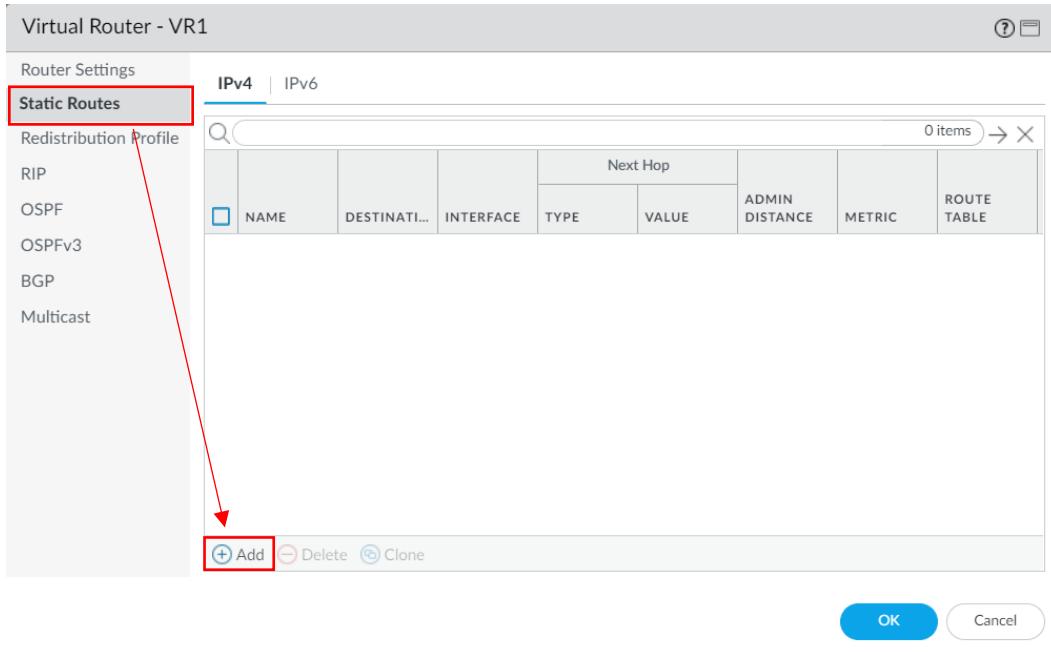


Son olarak tüm kaynaklarımızın interne çıkışması için **STATIC ROUTE** yazmamız gerekiyor. Ben PPPOE dsl kurulumu yaptığım için bana gerek yok. Fakat fiber kullananlarınız için şart.

Bu nedenle **“NETWORK”** menüsünden **“VIRTUAL ROUTER”** sekmesine gidiyorum. Üst adımlarda oluşturduğumuz **VR1** isimli routera tıklıyorum.



Karşımıza gelen menüden "static Routes" sekmesine geliyorum ve **add** diyorum.



Virtual Router - VR1

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

IPv4 | IPv6

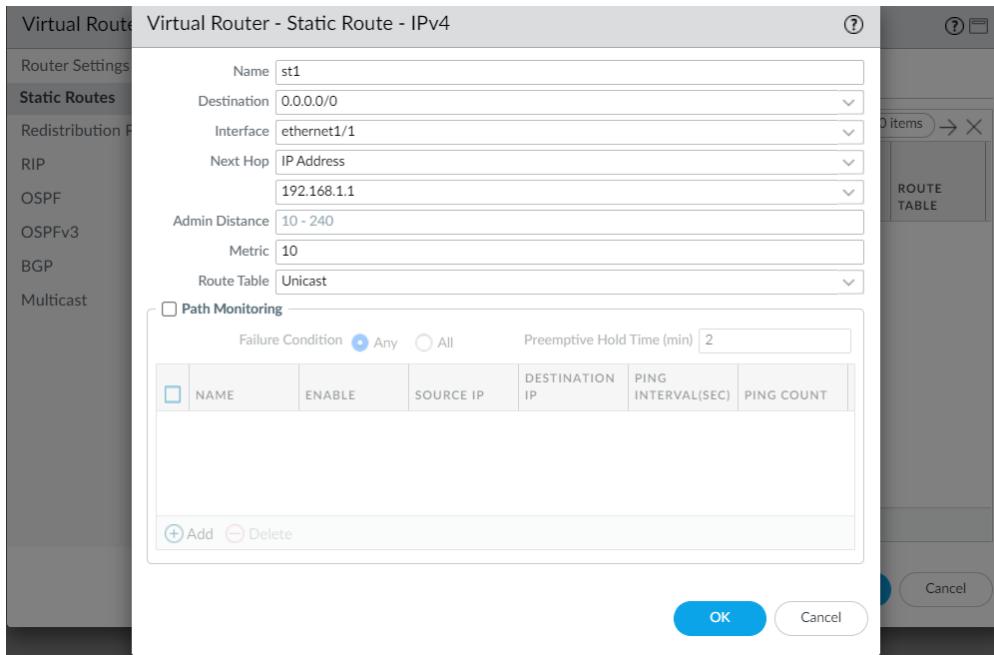
0 items → X

NAME	DESTINATI...	INTERFACE	Next Hop		ADMIN DISTANCE	METRIC	ROUTE TABLE
			TYPE	VALUE			

+ Add Delete Clone

OK Cancel

Karşımıza gelen menüden bir isim belirliyorum. Destination kısmında tüm local network ü yönlendirmek istediğim için 0.0.0.0/0 yazıyorum. Interface olarak WAN interfacemi seçiyorum. Next hop olarak ip adres seçerek public ip mi yazıyor ve "OK" diyerek işlemimi tamamlıyorum.



Virtual Router - Static Route - IPv4

Router Settings

Static Routes

Redistribution Profile

RIP

OSPF

OSPFv3

BGP

Multicast

Name st1

Destination 0.0.0.0/0

Interface ethernet1/1

Next Hop IP Address

192.168.1.1

Admin Distance 10 - 240

Metric 10

Route Table Unicast

Path Monitoring

Failure Condition Any All Preemptive Hold Time (min) 2

NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
------	--------	-----------	----------------	--------------------	------------

+ Add Delete

ROUTE TABLE

OK Cancel