

NOTLAR

- Biri ADSL diğeri METRO olmak üzere 2 adet internet hattımız bulunmaktadır.
- 2 hattımız da aktiftir.
- STATIC ROUTE oluştururken METRIC değerini düşük verdiğimiz route öncelikli olarak kullanılacaktır.
- Örneğimde ethernet 1/1 (ADSL) ve 1/3 (METRO) olarak kullandım.

YAPILACAKLAR

- Interfaces tanımları
- Static Route tanımlama
- Patch monitoring tanımlama

Daha önceki kurulum makalesinde PALO ALTO firewall ile internete nasıl çıkılır yayınlamıştım. Döküman içerisinde ZONE tanımlama, INTERFACE tanımla, STATIC ROUTE vb... gibi temelde lazım olan herşeyi bulabilirsiniz.

Ayrıca bu dökümanda kısaca interface tanımlamasını göstereceğim.

Bu döküman sayesinde basit bir şekilde PALO ALTO firewall cihazımız yedekli olarak internet nasıl kullanımı nasıl yapılandırır öğrenmiş olacaksınız.

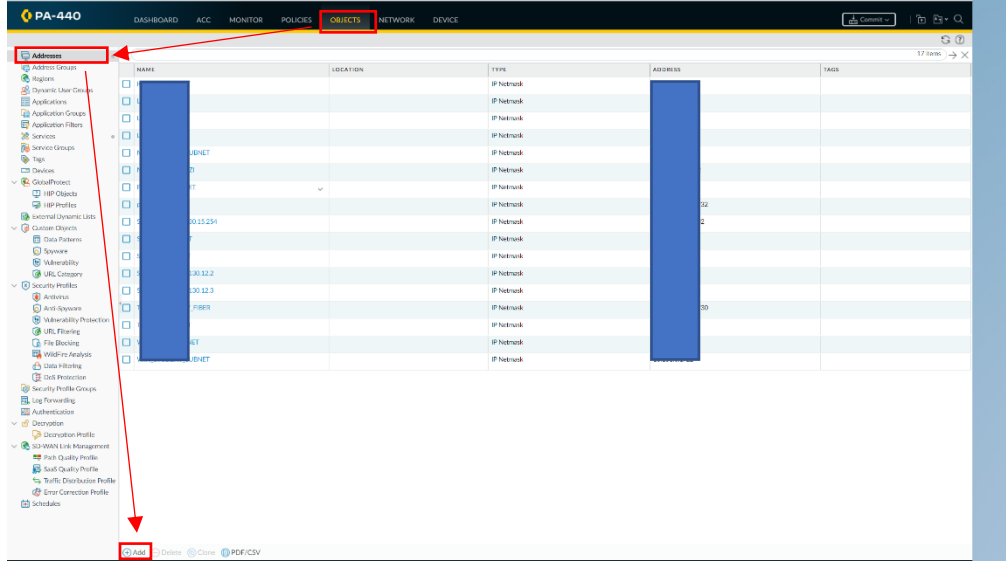
Benim örneğimde yukarıda dediğim gibi daha önce yayınlamış olduğum pdf dökümanında açıkça belirtmiş olduğum ayarlar ile devam edeceğim.

Yapıma sonradan eklediğim METRO internet altyapısını ekleyip, mevcut ADSL hattımızla birlikte yedekli kullanımı aktif edeceğiz.

Başlayalım.

PALO ALTO firewall cihazımın arayüzü açıyorum. İlk olarak elimdeki bilgiler ile ip adres tanımlamalarımı yapacağım.

Arayüzden “OBJECTS” menüsünden “ADRESSES” sekmesine geliyor ve yeni bir adres tanımlamak için “ADD” butonuna tıklıyorum.



Karşıma gelen menüden adresime bir isim tanımlıyorum. Ardından ip adresimi belirtip “OK” diyerek işlemimi tamamlıyorum.

Bu adımı yapmamın sebebi bir düzen kurma. Kurallar oluştururken firewall için etiketleme çok önemli siz veya sizden sonra kullanacak arkadaş için kafa karışıklığını ortadan giderir. Benim için olmazsa olmaz.

Address

Name

TTNET_METRO_PUBLIC_IP

Description

Type

IP Netmask

Resolve

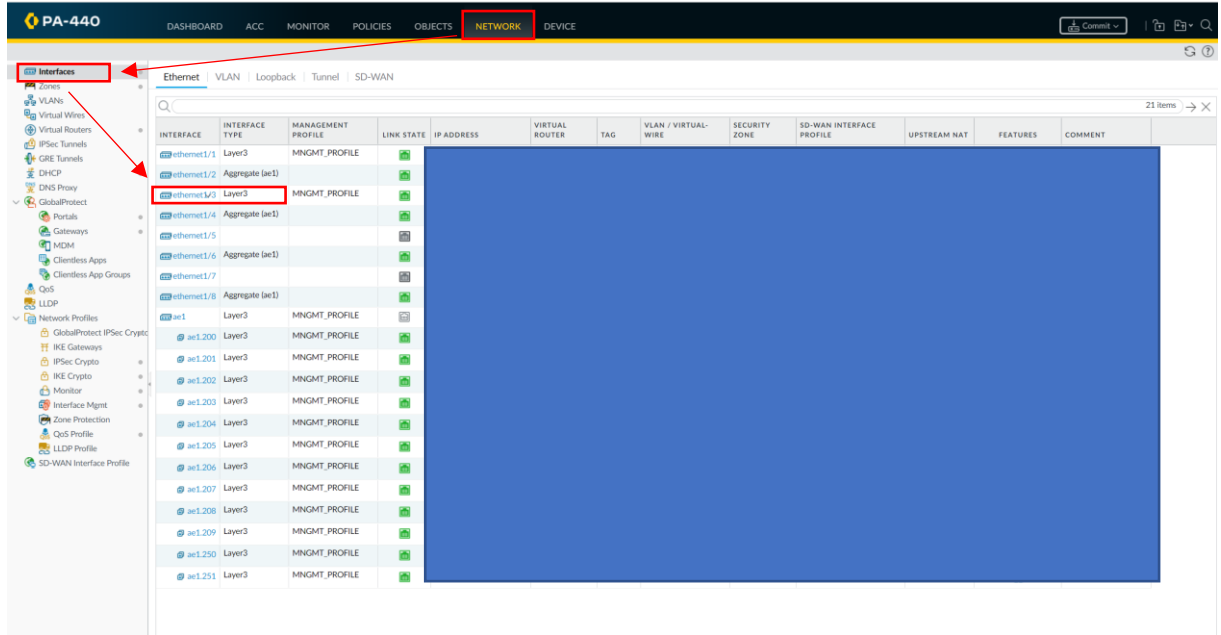
Tags

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)

OK

Cancel

Sonraki adımda interface tanımı yapmak için arayüzden “NETWORK” menüsünden “INTERFACES” sekmesine gelip “ETHERNET 1/3” e düzenlemek için tıklıyorum.



Karşıma gelen menüden “CONFIG” sekmesi altından virtual router ve security zone seçiyorum.

Ben router ve zone ayarlarımı diğer dökümanımda göstermiştim. Inceleyebilirsiniz.

Ethernet Interface

Interface Name

ethernet1/3

Comment

Interface Type

Layer3

Netflow Profile

None

Config

IPv4

IPv6

SD-WAN

Advanced

Assign Interface To

Virtual Router

VR1

Security Zone

WAN

OK

Cancel

Yine aynı menüden “IPv4” sekmesine gelip “ADD” diyorum. Karşıma gelen seçeneklerden üst adımlarda adres olarak eklediğim Internet Servis Sağlayıcı tarafından verilen bilgilerimi tanımlıyorum.

The screenshot shows the 'Ethernet Interface' configuration window with the 'IPv4' tab selected. The 'Interface Name' is 'ethernet1/3'. The 'Interface Type' is 'Layer3'. The 'Netflow Profile' is 'None'. The 'Type' is set to 'Static'. The 'IP' section shows a list with one entry: 'TTNET_METRO_PUBLIC_IP'. Below the list, there is an 'Add' button (a blue circle with a plus sign) and a 'Delete' button (a red circle with a minus sign). The 'Add' button is highlighted with a red box. The 'OK' button is at the bottom right.

Yine aynı menüden son olarak interface management profili eklemek için “ADVANCED” sekmesine geliyorum. Profilimi seçip “OK” diyerek işlemimi tamamlıyorum.

The screenshot shows the 'Ethernet Interface' configuration window with the 'Advanced' tab selected. The 'Link Settings' section shows 'Link Speed' as 'auto', 'Link Duplex' as 'auto', and 'Link State' as 'auto'. The 'Other Info' section shows 'Management Profile' as 'MNGMT_PROFILE' and 'MTU' as '[576 - 1500]'. The 'Adjust TCP MSS' section is expanded, showing 'IPv4 MSS Adjustment' as 40 and 'IPv6 MSS Adjustment' as 60. The 'Untagged Subinterface' checkbox is unchecked. The 'OK' button is highlighted with a red box and an arrow pointing to it from the 'Adjust TCP MSS' section.

Yukarıdaki işlemlerin aynısını 2. Internet hattım olan ADSL içinde uygulayacağım. Bu nedenle "NETWORK" menüsü "INTERFACES" sekmesinden "ETHERNET 1/1" e tıklıyorum.

Route ve zone tanımlamamı yapıyorum.

Önemli NOT: yedekli internetin çalışması için 2 interface zonunun aynı olması gerkelidir.

Ethernet Interface

Interface Name: ethernet1/1

Comment: wan

Interface Type: Layer3

Netflow Profile: None

Config | IPv4 | SD-WAN | Advanced

Assign Interface To

Virtual Router: VR1

Security Zone: WAN

OK Cancel

Aynı arayüzden "IPv4" sekmesine geliyorum. Ben Modemimi köprü moduna aldım. Modem görevini PALO ALTO yapacak. Bu nedenle ISP tarafından bildirilen PPPOE bilgilerimi giriyorum.

Ethernet Interface

Interface Name: ethernet1/1

Comment: wan

Interface Type: Layer3

Netflow Profile: None

Config | **IPv4** | SD-WAN | Advanced

☐ Enable SD-WAN ☐ Enable Bonjour Reflector

Type: ☐ Static ☒ PPPoE ☐ DHCP Client

General | Advanced

☒ Enable

Username: go...@ttnet

Password:

Confirm Password:

Show PPPoE Client Runtime Info

OK Cancel

Bu arada PPPOE yapılandırmasında Static route kendiliğinden oluşturğu için herhangi bir route eklemeyeceğim. Fakat "ADVANCED" sekmesine gelip static route oluşması ve metric ayarını girmek için tanımlama yapıyorum.

Metric ayarı benim için çok önemli Metric ayarı düşük olan interface PALO ALTO tarafında öncelikli olarak kullanılacaktır.

Tanımlamalarımı yaptıktan sonra "OK" ile işlemimi tamamlıyorum.

Dediğim gibi PPPOE yapılandırmasında ekstra static route tanımlaması yapmadığımız için metric ayarını burada yapıyorum.

Ethernet Interface

Interface Name: ethernet1/1

Comment: wan

Interface Type: Layer3

Netflow Profile: None

Config: **IPv4** | SD-WAN | Advanced

☐ Enable SD-WAN ☐ Enable Bonjour Reflector

Type: ☐ Static ☒ PPPoE ☐ DHCP Client

General: **Advanced**

Authentication: None

Static Address: None

☒ automatically create default route pointing to peer

Default Route: 10

Metric: 10

Access Concentrator:

Service:

☐ Passive

OK Cancel

Şimdiki adımda static route oluşturmak için “NETWORK” menüsü “VIRTUAL ROUTERS” sekmesine geliyorum. Benim daha önce oluşturmuş olduğum routers a tıklıyorum.

NAME	INTERFACES	CONFIGURATION	RIP	OSPF	OSPFV3
VR1	ae1 ae1.200 ae1.201 ae1.202 ae1.203 ae1.204 ae1.205 more...	Static Routes: 1 ECMP status: Disabled			

Karşıma gelen menüden “STATIC ROUTERS” sekmesine gelip tanımlama yapmak için “ADD” butonuna tıklıyorum.

NAME	DESTINATION	INTERFACE	TYPE	VALUE	ADMIN DISTANCE	METRIC	ROUTE TABLE
------	-------------	-----------	------	-------	----------------	--------	-------------

+ Add - Delete Clone

OK Cancel

Karşıma gelen menüden bir isim belirliyorum. Tüm network bu interface üzerinden nete çıkması için ilgili tanımlamaları yapıyorum. Ben METRO internet üzerinden öncelikli olarak internete çıkılmasını istediğim için interface seçimimi ona göre yapıyorum. Next hop adres olarak size internet sağlayıcısı tarafından verilen gateway bilgisini girmelisiniz.

Önemli: METRIC tanımını Metro internetimin öncelikli olması açısından ADSL den daha düşük Verdi. ADSL metrik değeri 10 Metronun ki ise 5.

Virtual Router - Static Route - IPv4

Namevr1

Destination0.0.0.0/0

Interfaceethernet1/3

Next HopIP Address

169

Admin Distance10 - 240

Metric5

Route TableUnicast

☒ Path Monitoring

Failure Condition ☒ Any ☐ All

Preemptive Hold Time (min) 2

<input type="checkbox"/>	NAME	ENABLE	SOURCE IP	DESTINATION IP	PING INTERVAL(SEC)	PING COUNT
--------------------------	------	--------	-----------	----------------	--------------------	------------

+ Add

- Delete

OK

Cancel

Yine aynı menüden İnternetimin kesinti durumunda yedekli çalışması için "PATH MONITORING" seçeneğini seçiyorum. "ADD" diyerek yeni bir tanımlama oluştuyorum.,

Virtual Router - Static Route - IPv4

Name: vr1

Destination: 0.0.0.0/0

Interface: ethernet1/3

Next Hop: IP Address

Admin Distance: 10 - 240

Metric: 5

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
--	------	--------	-----------	----------------	--------------------	------------

Karşıma gelen menüden ilgili seçeneklerimi seçiyorum. Source ip kısmına public ip mi destination kısmına ise ping atacağımız herhangi bir adresi girip "OK" diyerek işlemi tamamlıyorum.

Bu adım belirlediğimiz adrese ping atacak eğer cevap alamazsa sorun olduğunu anlayacak ve anında diğer internetimize geçiş olacaktır.

Path Monitoring Destination

Name: primary

☒ Enable

Source IP: TTNET_PUBLIC_IP

Destination IP: 1

Ping Interval(sec): 3

Ping Count: 5

Sıra geldi. Oluşturduğumuz interface ler için internete çıkışta kullanacağımız “NAT” ayarlarına. İlgili yapılandırma için “POLICIES” menüsünden “NAT” sekmesine gidiyorum ve yeni bir nat eklemek için “ADD” butonuna tıklıyorum.

Daha önce ADSL netim için nat oluşturmuştum. Ben size örnek olaması açısından METRO internetim için oluşturacağım.

Sizin yapınızda kaç adet internet bağlantısı varsa okadar aynı şekilde nat kuralı oluşturacaksınız

The screenshot shows the PA-440 web interface. The top navigation bar includes 'DASHBOARD', 'ACC', 'MONITOR', 'POLICIES', 'OBJECTS', 'NETWORK', and 'DEVICE'. The 'POLICIES' tab is selected. On the left sidebar, the 'Security' section is expanded, and the 'NAT' sub-tab is selected. A table displays existing NAT policies:

	NAME	TAGS	SOURCE ZONE	DESTINATION ZONE	DESTINATION INTERFACE	SOURCE ADDRESS	DESTINATION ADDRESS	SERVICE	SOURCE TRANSLATION	DESTINATION
5	static_nat_1	none	LAN	WAN	ethernet1/1	any	any	any	dynamic-ip-and-port	ethernet1/1

At the bottom of the interface, the 'Add' button is highlighted with a red box and an arrow.

Karşıma gelen menüden nat kuralıma isim veriyorum.

The screenshot shows the 'NAT Policy Rule' configuration dialog box. The 'General' tab is selected. The 'Name' field is highlighted with a red box and contains the text 'static_nat_4'. Other fields include 'Description', 'Tags', 'Group Rules By Tag' (set to 'None'), 'NAT Type' (set to 'ipv4'), and 'Audit Comment'. The 'OK' and 'Cancel' buttons are at the bottom right.

Aynı ekrandan "original packet" sekmesine geliyorum. Tanımlamalarımı aşağıdaki gibi yapıyorum.

NAT Policy Rule

General

Original Packet

Translated Packet

☐ Any

☒ SOURCE ZONE ^

☐ LAN

Destination Zone

WAN

Destination Interface

ethernet1/3

Service

any

+ Add

- Delete

☒ Any

☐ SOURCE ADDRESS ^

☒ Any

☐ DESTINATION ADDRESS ^

+ Add

- Delete

+ Add

- Delete

OK

Cancel

Aynı ekrandan "Translated Packet" sekmesine geliyorum. Tanımlamalarımı aşağıdaki gibi yapıyor ve "OK" diyerek işlemimi tamamlıyorum.

NAT Policy Rule

General

Original Packet

Translated Packet

Source Address Translation

Translation Type

Dynamic IP And Port

Address Type

Interface Address

Interface

ethernet1/3

IP Address

TTNET_METRO_PUBLIC_IP

None

Destination Address Translation

Translation Type

None

OK

Cancel

Bu işlemlerin ardından herşey tamamlandı. Ben dediğim gibi çalışan sistem üzerinden 2. Bir internet haattı ekleyip yedeklilik oluşturdum.

Eğer siz sıfırdan kurulum yapıyorsanız. Bu adımlara ek olarak birde security kuralı oluşturmalsınız. Benim security kuralım aşağıdaki gibidir.

	NAME	TAGS	TYPE	Source				Destination			APPLICATION	SERVICE	ACTION	PROFILE	OPTIONS
				ZONE	ADDRESS	USER	DEVICE	ZONE	ADDRESS	DEVICE					
1	Lan_To_Wan	none	universal	LAN	any	any	any	WAN	any	any	any	any	Allow		

