



Bilgi Teknolojileri

IIS SERVER



MERKEZ



Site To Site  
VPN



CLOUD

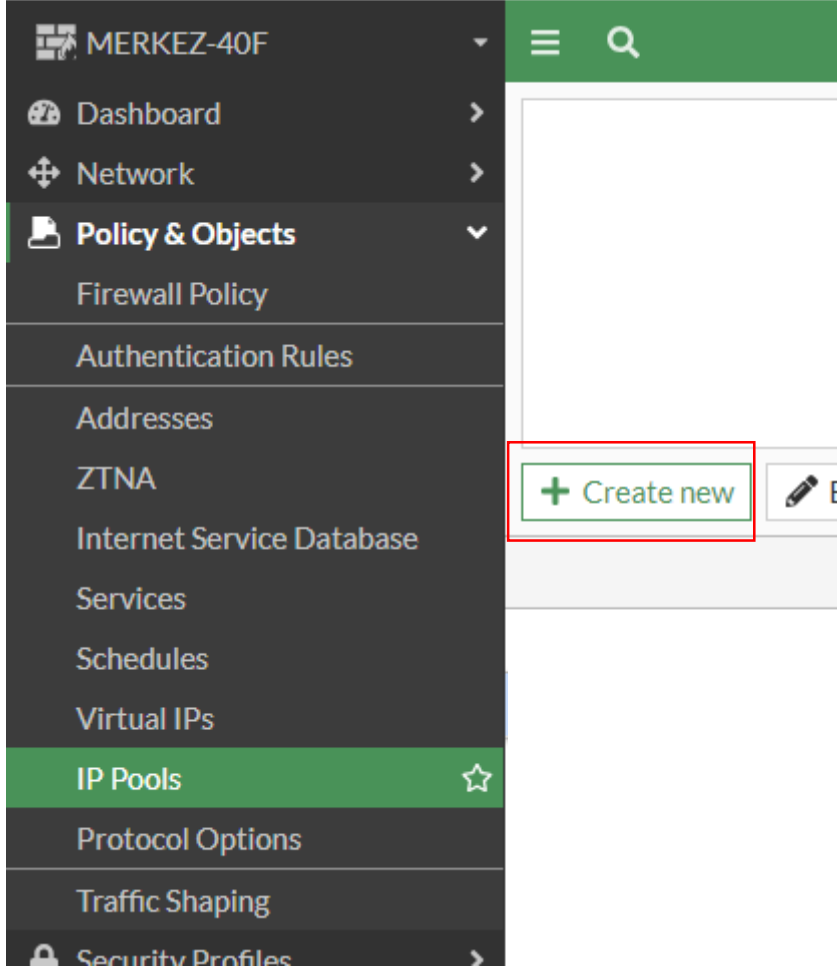


INTERNET

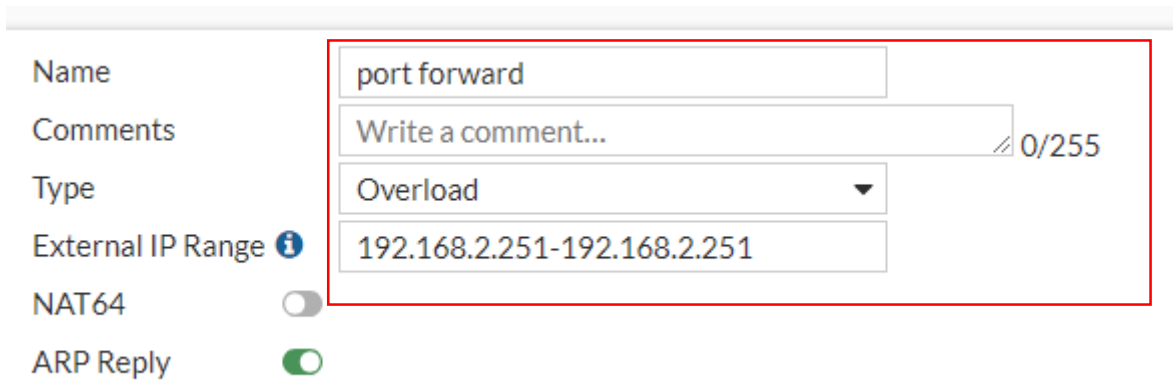


KULLANICI

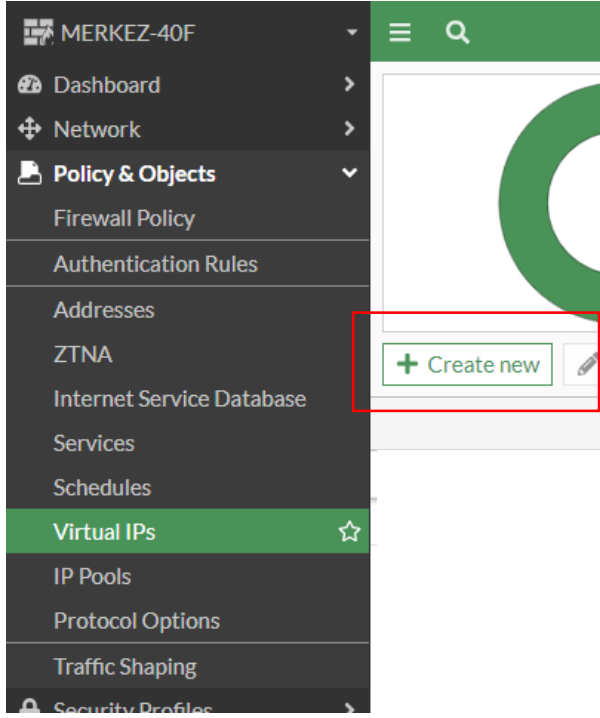
İlk olarak local subnetimden boşta bulunan bir ip içi ip pool oluşturacağım. Bu nedenle firewall arayüzden “policy & Objects” altından “IP Pools” a tıklıyorum ve “create new” diyorum.



Karşıma gelen menüden ip pool a bir isim belirliyorum ve boşta bulunan bir local ip adresimi set edip ok ile işlemimi sonlandırıyorum.



Sonraki adımda cloud tarafındaki sunucu ip bilgisini kullanarak bir Virtuals Ip oluşturacağım. Bu nedenle yine arayüzden “policy & Objects” altından virtual IPs tıklıyorum ve karşıma gelen menüden Create new butonuna tıklıyorum.



Karşıma gelen menüden sanal ip me bir isim belirliyorum. External ip adresine merkez dış ip bilgimi yazıyorum. IPv4 bölümüne ise cloud arkasındaki sunucu local ip adresini yazıyorum. Sonrasında içerideki 80 nolu portla çakışma olmaması açısından portları da map liyor ve ok diyerek işlemimi sonlandırıyorum.

Name: cloud paperwork  
Comments: Write a comment... 0/255  
Color: Change

Network

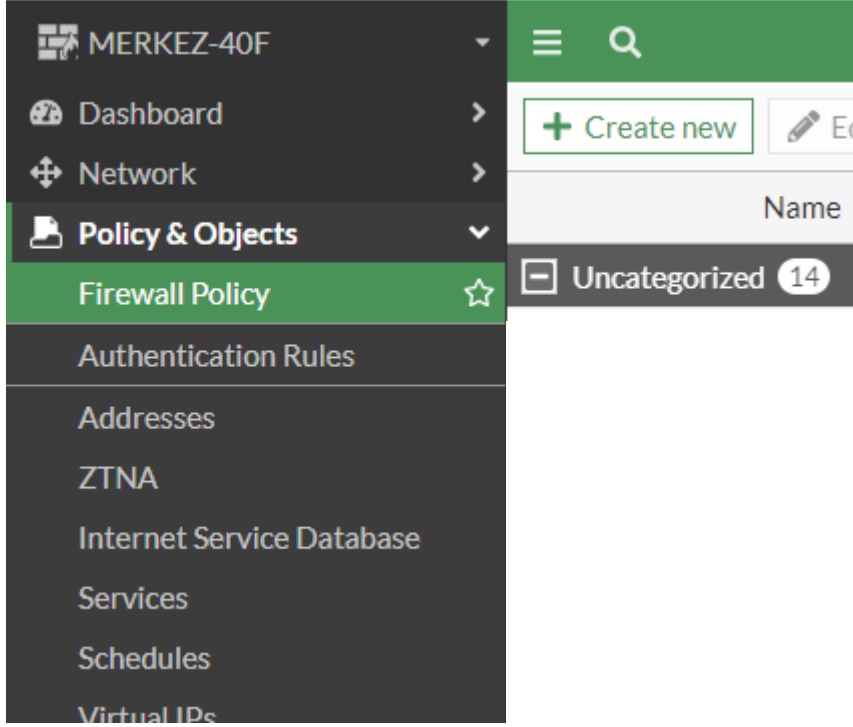
Interface: INTERNET (wan)  
Type: Static NAT  
External IP address/range:   
Map to:  
IPv4 address/range: 10.80.90.202

☐ Optional Filters

☒ Port Forwarding

Protocol: ☒ TCP ☐ UDP ☐ SCTP ☐ ICMP  
Port Mapping Type: ☒ One to one ☐ Many to many  
External service port: 8085  
Map to IPv4 port: 80

Sonraki adımda ana menüden Firewall Policy ye geliyor ve Create new diyerek yeni bir policy oluştuyorum.



Karşıma gelen menüden kuralıma isim veriyorum. Incoming olarak wan bacağımı outgoing olarak merkez ve cloud bağlantı interface i seçiyorum. Destination olarak ise üst adımlarda oluşturduğum Virtual IPs i seçiyorum.

The screenshot shows the configuration form for a Firewall Policy. The form has a left-hand sidebar with labels for each field, and a main area with the corresponding input fields. The fields are: Name (Paperwork- port Forwarding), Type (Standard, ZTNA), Incoming Interface (INTERNET (wan)), Outgoing Interface (MERKEZ To CLOUD), Source (all), IP/MAC Based Access Control (Disabled), Logical And With Secondary Tags (Specify), Destination (cloud paperwork), Schedule (always), Service (ALL), Action (ACCEPT, DENY), and Inspection Mode (Flow-based, Proxy-based). The 'Destination' field is highlighted with a red box. The 'Action' field has a green checkmark next to 'ACCEPT' and a red 'X' next to 'DENY'. The 'Inspection Mode' field has a green checkmark next to 'Flow-based' and a grey 'X' next to 'Proxy-based'.

işlemlerime devam ederken NAT açıyorum ve Ip pool Confuguration dan Use Dynamic IP Pool seçiyorum ve yine üst adımlarda oluşturduğım ip pool u seçiyorum ve OK diyerek işlemlerimi tamamlıyorum.

Firewall/Network Options

NAT

IP Pool Configuration

Preserve Source Port

Protocol Options

Use Outgoing Interface Address

Use Dynamic IP Pool

port forward

+

PROT default

Security Profiles

AntiVirus

Web Filter

DNS Filter

Application Control

IPS

SSL Inspection

no-inspection

Logging Options

Log Allowed Traffic

Security Events

All Sessions

Comments

Write a comment...

0/1023

Enable this policy

OK

Cancel

Sonrasında kontrolümü gerçekleştirdiğimde port yönlendirme işlemlerimin başarılı bir şekilde çalıştığını teyit ediyorum.

