

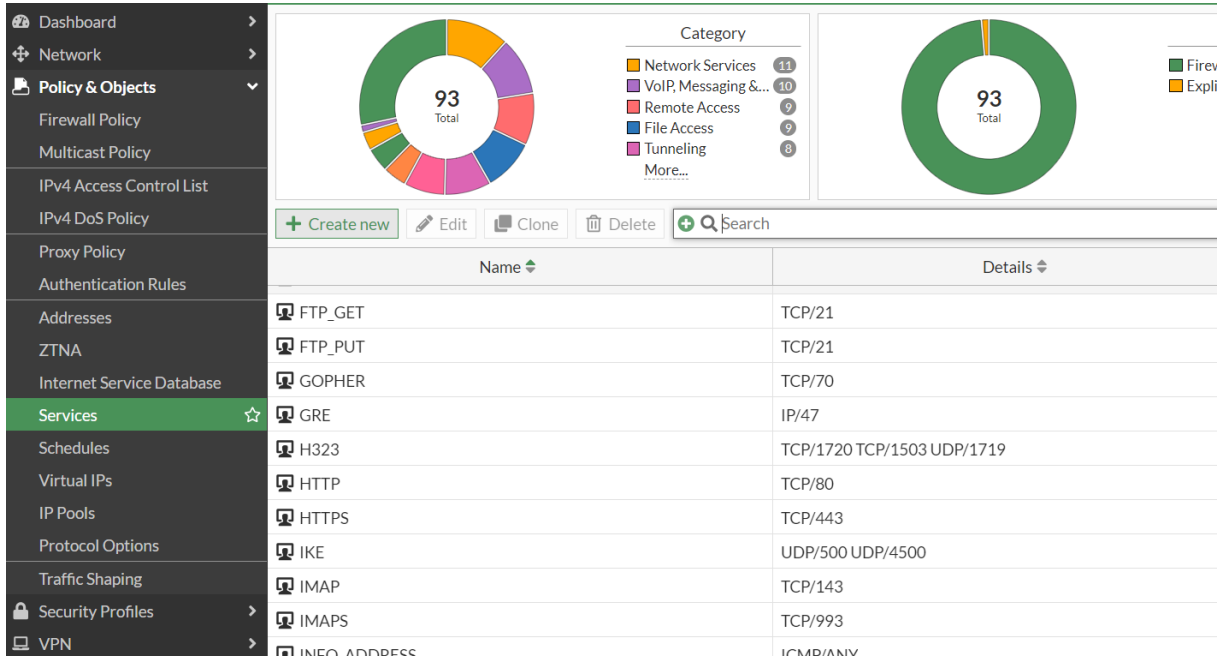


ZOOM MEETING UDP_FLOOD

ALLOW DDOS POLICY



Firewall menüden **"Policy & Objects"** altından **"Services"** sekmesine tıklıyorum ve karşıma gelen ekrandan yeni bir hizmet tanımı yapmak için **"Create new"** butonuna tıklıyorum.



Karşıma gelen ekrandan hizmetime isim veriyorum ve dinamik aralığa sahip portlarımı zoom UDP portlarına MAP ediyorum. Ok diyerek işlemimi tamamliyorum.

Zoom UDP Portları Aşağıdaki gibidir.

3478 , 3479 , 8801 , 8810

New Service

Name: ZOOM UDP PORTS

Comments: 0/255

Service Type: Firewall Explicit Proxy

Color: Change

Category: Uncategorized

Protocol Options

Protocol Type: UDP

Address: 0.0.0.0

Destination Port: 49152 - 65535

Source Port: 3478 - 3479, 8801 - 8810

Specify Source Ports: ☒

OK Cancel

Görüldüğü üzere hizmetimi oluşturuldu.

Name	Details	IP/FQDN	Category
ZOOM UDP PORTS	UDP/49152-65535:3478-3479 UDP/49152-65535:8801-8810	0.0.0.0	Uncategorized

Sonraki adımda firewall menüden yine **“Policy & Objects”** altından **“IPv4 DoS Policy”** tıklıyorum ve karşıma gelen ekrandan **“Create New”** butonuna tıklıyorum.

Dashboard

Network

Policy & Objects

Firewall Policy

Multicast Policy

IPv4 Access Control List

IPv4 DoS Policy

Proxy Policy

Authentication Rules

Addresses

ZTNA

Internet Service Database

Create New

Edit

Edit in CLI

Delete

Search

ID	Name	Interface	
1	WAN	INTERNET (wan1)	all

Karşıma gelen ekrandan incoming olarak wan bacağını seçiyorum ve service olarak tanımladım hizmeti seçiyor ve anomali listesinden udp_flood açıp Monitor seçip okey diyerek işlemimi tamamlıyorum.

Name

Zoom Udp Allow

Incoming Interface

INTERNET (wan1)

Source Address

all

Destination Address

all

Service

ZOOM UDP PORTS

L3 Anomalies

Name	Logging	Action	Disable	Block	Monitor	Threshold
ip_src_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
ip_dst_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000

L4 Anomalies

Name	Logging	Action	Disable	Block	Monitor	Threshold
tcp_syn_flood	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2000
tcp_port_scan	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1000
tcp_src_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
tcp_dst_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
udp_flood	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	2000
udp_scan	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2000
udp_src_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
udp_dst_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
icmp_flood	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	250
icmp_sweep	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100
icmp_src_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	300
icmp_dst_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1000
sctp_flood	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	2000
sctp_scan	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1000
sctp_src_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000
sctp_dst_session	<input checked="" type="checkbox"/>	Disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	5000

Comments

Write a comment...

0/1023

Enable this policy

☒

OK

Cancel

Oluşturmuş olduğum Ddos policy i mevcut policiyelerin en üstüne taşıyorum işlemimi tamamlıyorum.

ID	Name	Interface	Source Address	Destination Address	Service
2	Zoom.Udp.Allow	INTERNET (wan1)	all	all	ZOOM UDP PORTS
1	WAN	INTERNET (wan1)	all	all	ALL



Bilgi Teknolojileri