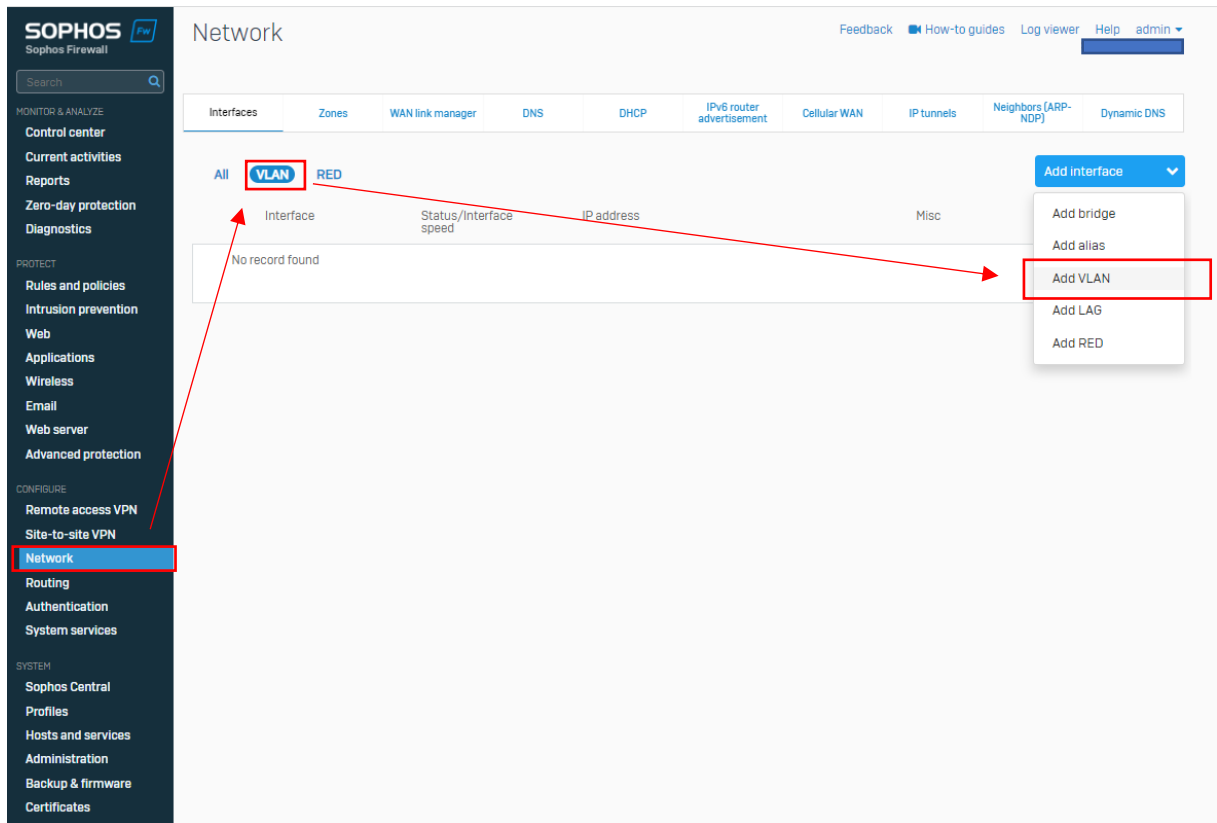


Öncelikle kimlik bilgilerimi girerek Sophos firewall cihazıma login oluyorum.



Karşıma gelen ekrandan Vlan oluşturmak için “Network” sekmesinden “VLAN” seçeneğine geliyorum ve “add interface” butonundan “Add VLAN” diyorum.



Karşıma gelen menüden oluşturmak istediğim Vlan bilgilerini giriyorum. Benim örneğim de vlan 150 oluşturacağım. Bu nedenle kafam karışmasın diye vlan isminide vlan 150 olarak belirliyorum.

Name kısmına vlan ismimizi

Interface kısmındaa lan portumuz kaç numara ise o portu

Zone kısmında LAN zonunu

Vlan Id kısmında Vlan numaramızı

Ipv4 kısmında network ve subnet bilgilerimizi girip "Save" butonu ile vlan oluşturma işlemini tamamlıyoruz.

SOPHOS Firewall

VLAN interface

Feedback How-to guides Log viewer Help admin

Interfaces Zones WAN link manager DNS DHCP IPv6 router advertisement Cellular WAN IP tunnels Neighbors (ARP-NDP) Dynamic DNS

Search

MONITOR & ANALYZE

Control center

Current activities

Reports

Zero-day protection

Diagnostics

PROTECT

Rules and policies

Intrusion prevention

Web

Applications

Wireless

Email

Web server

Advanced protection

CONFIGURE

Remote access VPN

Site-to-site VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Add VLAN

Name * Vlan150

Hardware Port1.150

Interface Port1

Zone LAN

VLAN ID * 150 [1-4094]

☒ IPv4 configuration

IP assignment Static PPPoE DHCP

IPv4/netmask * 192.168.150.1 /24 (255.255.255.0)

Gateway detail

Gateway name

Gateway IP

☐ IPv6 configuration

Save Cancel

Vlan oluřturma iřlemi ardından, Vlan network e ip dađıtacađım. Bu nedenle yine “Network” sekmesinden “DHCP” seeneđine geliyorum. “Add” diyerek vlan150 network iin ip dađıtacađım.

The screenshot shows the Sophos Firewall Network configuration page. The 'DHCP' tab is selected and highlighted with a red box. A red arrow points from the 'Add' button in the 'Server' section to the 'DHCP' tab. Another blue arrow points from the 'Add' button in the 'Relay' section to the 'DHCP' tab. The 'Server' section shows a table with columns: Name, Interface, Lease detail, IP version, Status, and Manage. The 'Relay' section shows a table with columns: Name, Interface, DHCP server IP, IP version, and Manage.

Karřıma gelen menüden bir isim belirliyorum. **Interface** kısmından ip dađıtmak istediđim arayüzümü seiyorum. Sonrasında otomatik olarak dađıtmak istediđim ip aralıđını belirterek “Save” ile iřlemimi tamamlıyorum.

The screenshot shows the Sophos Firewall Network configuration page, specifically the 'General settings' section. The 'Name' field is set to 'VLAN150' and the 'Interface' is set to 'Vlan150 - 192.168.150.1'. The 'Dynamic IP lease' section shows 'Start IP' as '192.168.150.10' and 'End IP' as '192.168.150.100'. The 'Static IP MAC mapping' section is empty. The 'DNS server' section has 'Primary DNS' set to '192.168.150.1'. The 'WINS server' section has 'Primary WINS server' and 'Secondary WINS server' fields. The 'Boot options' section has 'Next-server' and 'Boot file' fields. The 'DHCP options' section is empty. A red arrow points from the 'Save' button at the bottom to the 'DHCP options' section.

Böylece VLAN150 networkümüzü oluşturduk ve DHCP ile otomatik ip dağıttık. Son olarak VLAN150 networkünün nete çıkması için bir kural yazıyorum.

Arayüzünden “Rules and Policies” sekmesine geliyor ve “Add firewall Rule” altından “New Firewall Rule” seçeneğine tıklıyorum.

The screenshot shows the 'Rules and policies' section of the Sophos Firewall interface. The 'Add firewall rule' button is highlighted with a red box. A dropdown menu is open, showing 'New firewall rule' as the selected option. The table below lists existing rules, including 'DNAT to DVR3_1649...', 'Zamanbaz Internet', 'host-report', 'PDKS_MSQSRV', 'AKINSOFT-RULE', 'Traffic to Interna...', 'Traffic to WAN', 'Traffic to DMZ', 'Auto-added firewall...', '#Default-Network-P...', and 'Drop all'.

Karşıma gelen ekrandan kuralıma isim veriyorum. Source zone kısmını LAN seçiyorum. Source network and devices kısmında ise oluşturmuş olduğum vlan150 bilgisini gireceğim. Bu nedenle add altından Network e tıklıyorum.

The screenshot shows the 'Add firewall rule' configuration page. The 'Rule name' field is set to 'Vlan150_to_NET'. The 'Action' is 'Accept'. The 'Source' is 'LAN'. The 'Source networks and devices' list includes 'LAN' and 'Vlan150'. The 'Destination and services' section is empty. The 'Rule position' is 'Bottom'. The 'Rule group' is 'Traffic to WAN'. The 'During scheduled time' is 'All the time'. The 'Summary' section shows 'Vlan150_to_NET'.

Karşıma gelen menüden VLAN150 için bilgilerimi aşağıdaki gibi giriyorum. "Save" diyerek işlemimi tamamlıyorum.Siz kendi vlan bilgilerinize göre doldurabilirsiniz.

Add IP host

Name *

IP version * ☒ IPv4 ☐ IPv6

Type * ☒ IP ☐ Network ☐ IP range ☐ IP list

IP address *

IP host group

[Add new item](#)

[Save](#) [Cancel](#)

Sonrasında destination kısmını WAN seçiyorum. Services kısmında ben kendi tercihlerime göre kullanıcılarımın sadece http ve https protokollerini kullanması için o seçeneklerle ilerliyorum.

Son olarak Kuralıma daha öncesinden oluşturduğum web filter ı da ekleyim "Save" diyerek işlemimi sonlandırıyorum.

Add firewall rule

Feedback [How-to guides](#) [Log viewer](#) [Help](#) [admin](#)

Rule status

Rule name * Description

Action ☒ Log firewall traffic

Log firewall traffic: Logs traffic matching this firewall rule, on the appliance (by default) or on the configured syslog server.

Source

Select the source zones, networks, and devices. The rule applies to traffic from these sources during the scheduled time period.

Source zones * [Add new item](#)

Source networks and devices * [Add new item](#)

During scheduled time [Select to apply the rule to a specific time period day of the week.](#)

Destination and services

Select the destination zones, networks, devices, and services. The rule applies to traffic to these destinations.

Destination zones * [Add new item](#)

Destination networks * [Add new item](#)

Services * [Add new item](#)

Services are traffic types based on a combination of protocols and ports.

☒ Match known users

[Add exclusion](#)

[Creates linked NAT rule](#)

Security features

☒ Web filtering

Web policy

☐ Apply web category-based traffic shaping

☒ Block QUIC protocol

Malware and content scanning

☐ Scan HTTP and decrypted HTTPS

☐ Use zero-day protection

☐ Scan FTP for malware

Filtering common web ports

☐ Use web proxy instead of DPI engine

☒ DPI engine or web proxy?

Web proxy options

☐ Decrypt HTTPS during web proxy filtering

[Save](#) [Cancel](#)