

SOPHOS SG firewall cihazıma logon oluyorum. Karşıma gelen ara yüzden ilk olarak cihaz ve port tanımlamalarımı yapacağım.

Bu nedenle **"Host and Services"** sekmesinden **"IPHost"** kısmına gelip **"Add"** butonuna tıklıyorum.

The screenshot shows the Sophos Firewall management interface. The left sidebar contains the following menu items:

- 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
  - VPN
  - Network
  - Routing
  - Authentication
  - System services
- SYSTEM
  - Sophos Central
  - Profiles
  - Hosts and services**
  - Administration
  - Backup & firmware
  - Certificates

The main area is titled 'Hosts and services'. It features a tabbed interface with the following tabs: IP host, IP host group, MAC host, FQDN host, FQDN host group, Country group, Services, and Service group. The 'IP host' tab is selected. Below the tabs, there is a table with the following columns: Name, Type, Address detail, IP version, and Manage. The table is currently empty. To the right of the table, there is an 'Add' button and a 'Delete' button. A red arrow points from the 'Add' button to the 'IP host' tab. Another red arrow points from the 'Hosts and services' menu item in the sidebar to the 'IP host' tab.

Karşıma gelen menüden portunu yönlendirmek istediğim cihazımın ip bilgisini tanımlıyorum. Ben örneğimde Kamera kayıt cihazının portunu yönlendireceğim için bir isim verip onun ip bilgisini giriyorum.

Bu tanımlamalar çok önemli yazacağınız kurallarda veya ileride yapılacak herhangi bir düzenlemede kafa karışıklığını ortadan giderecektir.

Bilgilerimi girdikten sonra **"Save"** diyip kayıt ediyorum.

**SOPHOS** FW  
Sophos Firewall

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

VPN

Network

Routing

Authentication

System services

SYSTEM

Sophos Central

Profiles

Hosts and services

Administration

Backup & firmware

Certificates

Edit IP host

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

IP host

IP host group

MAC host

FQDN host

FQDN host group

Country group

Services

Service group

Name \*

DVR3

IP version \*

IPv4

Type \*

IP

IP address \*

192.168.1.223

IP host group

Add new item

Save

Cancel

Sonraki adımda hangi portu yönlendireceksem bu sefer yine aynı arayüzün **“Services”** sekmesine gelip **“Add”** butonuna tıklıyorum.

**SOPHOS** Firewall

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

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services**
- Administration
- Backup & firmware
- Certificates

Hosts and services

Feedback How-to guides Log viewer Help admin

IP host IP host group MAC host FQDN host FQDN host group Country group **Services** Service group

☐ Name Protocol Details Manage

**Add** Delete

[1 of 4]

Karşıma gelen menüden portum için bir isim belirliyorum. Sonrasında protokolü **TCP** seçiyorum. Burada önemli bir detay belirtmek istiyorum. Source port kısmına **\*** veya **1:65535** numarasını girerek dışardan gelecek tüm port aralığına izin vermiş oluyorum yine bu nedenle yönlendirmelerinizin çalışması için **Source port** kısmının mutlaka bu şekilde kalması gerekmektedir.

**Destination port** kısmına da cihazımın port bilgisini giriyorum ve **"Save"** diyerek işlemimi tamamliyorum.

Böylece yönlendirmek istediğimiz cihazımın ip ve port bilgilerinin tanımını tamamlamış olduk.

**SOPHOS** Firewall

Feedback How-to guides Log viewer Help admin

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

- VPN
- Network
- Routing
- Authentication
- System services

SYSTEM

- Sophos Central
- Profiles
- Hosts and services**
- Administration
- Backup & firmware
- Certificates

Edit service

IP host IP host group MAC host FQDN host FQDN host group Country group **Services** Service group

Name \* DVR\_3

Type \* TCP/UDP

Protocol Source port Destination port

TCP 1:65535 8800

Save Cancel

Sonraki adımda firewall ana menüsünden “Rules and Policies” sekmesine tıklıyorum. Karşıma gelen ekrandan “Add firewall rule” butonunun altından “Server Access assistant [DNAT]” seçeneğini tıklıyorum.

The screenshot displays the Sophos Firewall 'Rules and policies' configuration page. The left sidebar contains the following menu items: 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 (VPN, Network, Routing, Authentication, System services), and SYSTEM (Sophos Central, Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The main area is titled 'Rules and policies' and includes tabs for 'Firewall rules', 'NAT rules', and 'SSL/TLS inspection rules'. The 'Firewall rules' tab is active, showing a list of rules. A red box highlights the 'Add firewall rule' button, and a red arrow points to the 'Server access assistant (DNAT)' option in the dropdown menu. The list of rules includes: 1. Zamanbaz\_Internet (LAN, Zamanbaz, WAN, Any host, Any service, #23, Accept), 2. test-report (LAN, 68, WAN, Any host, Any service, #14, Accept), 3. PDKS\_MSQLSRV (WAN, turkiye, LAN, #Port2, PDKS\_MSQLSRV, #12, Accept), 4. AKINSOFT\_RULE (WAN, Any host, LAN, #Port2, AKINSOFT\_PORT, #11, Accept), 5. Traffic to Interna... (To LAN, WIFI, VPN, DMZ. Firewall rules with the destination zone as LAN, WIFI, VPN, DMZ would be added to this group on the first match basis if user selects automatic grouping option...), 6. Traffic to WAN (Outbound traffic to WAN. Firewall rules with the destination zone as WAN would be added to this group on the first match basis if user selects automatic grouping option. This is the d...), 7. Traffic to DMZ (Inbound traffic to DMZ. Firewall rules with the destination zone as DMZ would be added to this group on the first match basis if user selects automatic grouping option. This is the de...), 8. Auto-added-firewal... (Any zone, Any host, Any zone, Any host, SMTP, SMTP(S), SMTP S\_465, #1, Accept), 9. #Default\_Network\_P... (LAN, Any host, WAN, Any host, Any service, #5, Accept), 10. Drop all (Any zone, Any host, Any zone, Any host, Any service, #0, Drop). The bottom of the page shows 'Showing 26 of 26. Selected 0'.

Karşıma gelen ekrandan üst adımda oluşturduğumuz cihazımızı seçiyorum. Next diyerek ilerliyorum.

Server access assistant (DNAT)

Internal server IP address

Specify the private IP address of the internal server to access from the internet.

☒ DVR3 - 192.168.1.223

☐ Type IP (Creates an IP host with the specified IP address and name.)

Cancel 1 of 5 Next

Karşıma gelen ekranda İnternet yani WAN bacağıımızı soruyor. Hangi port ise onu seçiyorum. Next ile ilerliyorum.

Server access assistant (DNAT)

Public IP address

Specify the public IP address through which users can access the server.

☒ #Port2 - 192.168.2.254

☐ Type IP (Creates an IP host with the specified IP address and name.)

Cancel 2 of 5 Back Next

Karşıma gelen ekranda hangi yönlendirme yapmak istediğimiz portu soruyor. Yukarıdaki adımlarda tanımladığımız portu seçiyor ve Next ile ilerliyorum.

Server access assistant (DNAT)

Services

Users can access the selected services on the internal server.

DVR\_3

Add new item

Cancel 3 of 5 Back Next

Sonraki adımda gelen ekrana any olarak bırakıyorum ve Next diyorum.

Server access assistant (DNAT)

External source networks and devices

Users can access the internal server from the selected source networks and devices.

Any

Add new item

Cancel 4 of 5 Back Next

Karşıma yaptığımız işlemlerle alakalı bilgilendirme yaptığımız tanımlamalardan eminsek “save and finish” diyerek yönlendirme işlemimizi tanımlıyoruz.

Server access assistant (DNAT)

Review your selection

Select Save to add NAT rules and firewall rules with the following configuration:

Internal server to access from the internet

IP host: **192.168.1.223**

Hostname: **DVR3**

Public IP address through which users access the internal server

IP host: **192.168.2.254**

Hostname: **#Port2**

Services that users can access:

**DVR\_3**

Sources from which users can access the server:

**Any**

Creates three NAT rules:

Inbound NAT (DNAT): Traffic destined to the public IP address **192.168.2.254** is translated to the internal server address **192.168.1.223**

Outbound NAT (SNAT): Masquerades outbound traffic from the internal server **192.168.1.223** with the public IP address **192.168.2.254**

Loopback NAT: Internal network uses the same public IP address **192.168.2.254** to access the internal server **192.168.1.223**

Creates one firewall rule:

Allows access to the internal server for **DVR\_3** services from the sources **Any**

The rules are added at the top of the table and are turned on by default.

Cancel

5 of 5

Back

Save and finish

Son olarak da her zaman olduğu gibi test adımına geçiyorum. Görüldüğü üzere başarılı olmuşuz.

