

Sophos XG Firewall xDSL (PPPOE) Bağlantısı Yapılandırma

Merhabalar,

Bridge Mode yani **Köprü Modu** adındanda anlaşılacağı üzere **XDSL** modem kullanılarak santralden gelen data sinyalinin modem aracılığıyla çevrilerek bütün bağlantının arka tarafta bulunan cihaza (**Firewall** veya **Router**) iletilmesini sağlayan bir özelliktir.

Bu özellik sayesinde **modem** köprü moduna geçeceği için direk dışarıdan gelen bağlantı **Firewall** veya **Router** gibi cihazlarda **PPP Username** ve **Password** bilgileri girilerek sonlandırma yapılır.

Eğer devre **ADSL** ise bridge mode alacağımız modemde **VPI/VCI: 8/35** yazacağımız için Firewallda tekrardan bu bilgileri yazmamız gerekmiyor. Yeni nesil **Firewall** ünitelerinde bu değerler artık bulunmuyor.

Eğer **Modem ADSL** değilde **VDSL** olsaydı. **VDSL** modemler **VLAN ID:35** değerini yazmamızı isteyecektir. **Köprü(bridge) moda** alacağımız **VDSL** modemde bu değeri yazacağımız alan karşımıza çıkmazsa **VLAN 35** değerini **Sophos XG** üzerinde **PPPOE DSL Settings / VDSL / Vlan tag** kısmında yazmamız gerekmektedir. Eğer bu değeri yazmazsak kapsullemeye internet çıkışımız olmayacaktır.

Modemi Bridge Moda alırken dikkat edilmesi gerekenler;

* Modem ile Firewall farklı Network bloklarında olması gerekiyor. Örneğin **Modem IP: 192.168.1.1 | Firewall IP: 192.168.2.1** olmak zorunda.

* Modem üzerinde **DHCP**, varsa **Firewall** ve **Wireless** yayınını kapatmalıyız.

** Modem Wireless destekli bir üniteyse ve bu özelliğini kullanmak istiyorsanız **Port-Based Vlan** yapıp **Wireless** yayınını bu vlan grubuna dahil etmeliyiz böylelikle Firewalldan yada Switchten doğrudan bir kablo ayırdığımız **vlan** portuna atayıp Wireless ile bağlanan kullanıcılara erişim verebilirsiniz. Bu yapı önerdiğimiz bir yapı değil çünkü modeme ekstra bir iş yükü bindirmiş oluyorsunuz. Bu durumda yapılması gereken yeni bir **Access Point** alınıp sisteme dahil edilmesi olmalıdır.

ADSL ve VDSL bağlantı değerleri;

ADSL:

WAN ID Type – PPP Transfer Type – Ağ Protokolü – Kapsülleme: PPPoE

Aktarım Modu – Modülasyon: ATM

VPI / VCI: 8/35

VDSL:

WAN ID Type – PPP Transfer Type – Ağ Protokolü – Kapsülleme: PPPoE

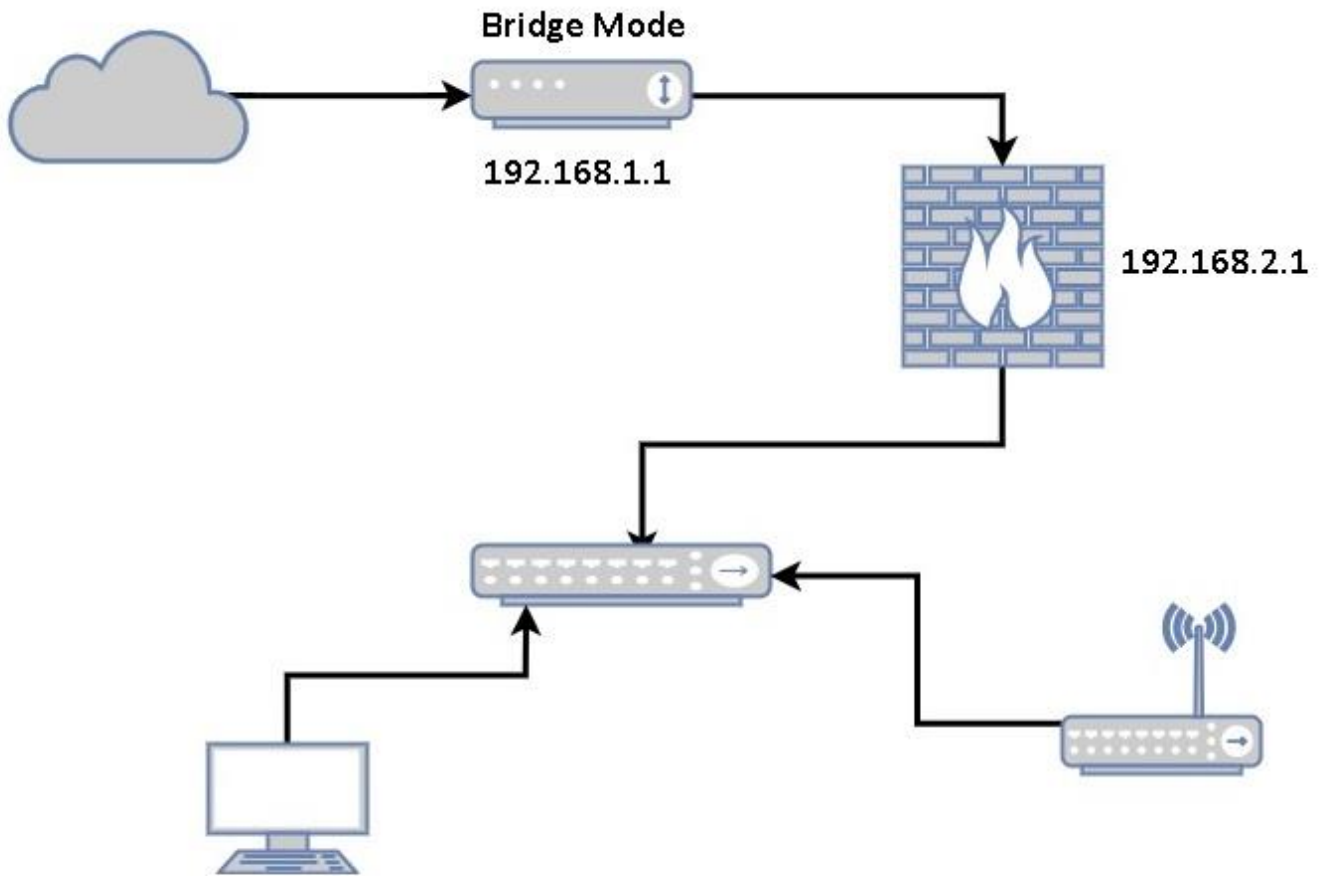
Aktarım Modu – Modülasyon: PTM

VLAN ID: 35

XDSL devrelerinin local santrale olan uzaklıklarını ve data hızlarını aşağıdaki tablodan karşılaştırabiliriz;

		Down Speed	Up Speed	Distance
Asymmetric	G.lite	1.5 Mbps	512 Kbps	18,000 ft
	ADSL	6-8 Mbps	640 Kbps	12,000-18,000 ft
	ADSL2	12 Mbps	1 Mbps	6,000 ft
	ADSL2+	27 Mbps	1 Mbps	3,000 ft
	VDSL	13-52 Mbps	1.5-2.3 Mbps	4,500 ft
Both	VDSL2	200 Mbps	200 Mbps	6,600 ft
Symmetric	IDSL	144 Kbps	144 Kbps	More than 2,000 ft
	SDSL	1.5 Mbps	1.5 Mbps	10,000-18,000 ft
	HDSL	2.3 Mbps	2.3 Mbps	12,000 ft

Bridge Mode Şemamız;



Modemi Bridge Moda aldıktan sonra **Configure / Network** menüsüne giriş yapıyoruz.

The screenshot shows the Sophos Control Center dashboard. The left sidebar is expanded to the 'Configure' section, where 'Network' is highlighted with a red arrow. The main dashboard area is titled 'Control center' and shows various system metrics and traffic insights. The 'Network' menu item is highlighted in the sidebar.

Karşımıza gelen ekranda dilerseniz Interface ismine tıklayabilir yada sağ tarafta alt alta 3 çizgi görünen alana tıklayıp **Edit Interface** diyerek ethernet arayüzünün içerisine giriş yapabiliriz.

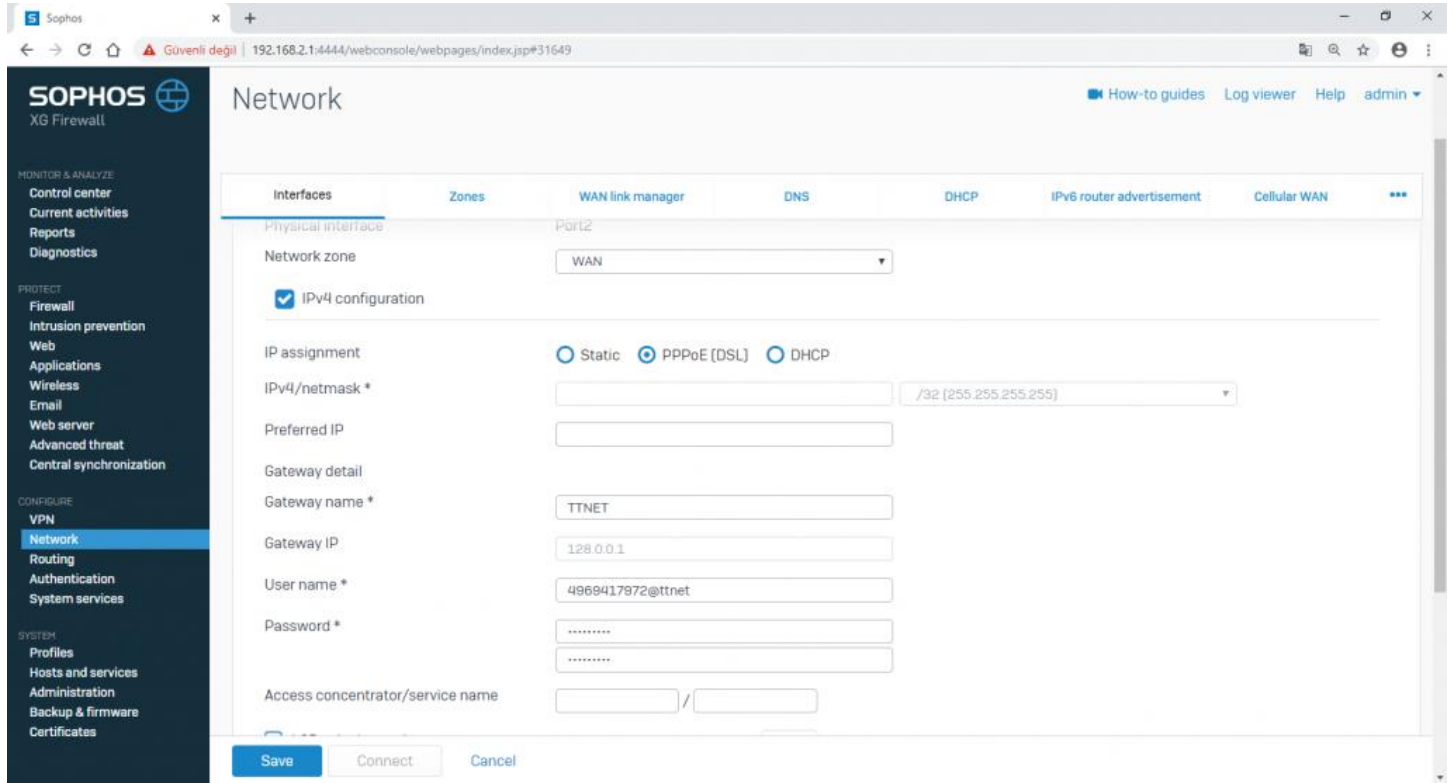
The screenshot shows the Sophos Network configuration page. The 'Interfaces' tab is selected, and a table of network interfaces is displayed. A red arrow points to the 'Port2' interface, and a red box highlights the 'Edit Interface' button in the context menu.

Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	N/A DHCP	
br0 N/A Bridge-pair	Connected N/A	192.168.2.1/255.255.255.0 Static	

Yapılandıracağımız Network Zonunu **WAN** tanımlayıp **PPPoE(DSL)** alanını seçiyoruz.

Eğer **Static IP** kullanıyorsanız **Preferred IP** alanına kullandığınız **Static IP** adresini yazabilirsiniz.

Telekomun bizlere tahsis ettiği **PPP Username** ve **Password** bilgilerini yazıyoruz.



LCP echo interval ve **LCP failure** alanlarını enable ediyoruz.

Link Kontrol Protokolü (LCP): Noktadan noktaya **PPP** bağlantının kurulması **LCP** sayesinde olur. **LCP**, Fiziksel katmanın üzerinde bulunur ve bağlantının kurulması, yapılandırmasının yapılması ve test edilmesi **LCP**'nin görevidir.

Tılgın Modemler Vlan Tag girişini zorunlu tuttuğu için **Vlan:35** değerini **Tılgın modeme** yazıyoruz.

Not: **Vlan id** değerini modeme yazıyorsak tekrardan **Sophos XG Firewalla** yazmıyoruz fakat modemde **vlan:35** **idsini** girecek alan yoksa **Sophos XG Firewalla DSL\Settings\Vlan Tag** alanına yazmamız gerekiyor.

Sophos XG Firewall Network configuration page. The page is titled "Network" and has a sidebar with navigation options like "Control center", "Reports", "Diagnostics", "Firewall", "Intrusion prevention", etc. The main content area shows configuration for "WAN link manager" with tabs for "Interfaces", "Zones", "WAN link manager", "DNS", "DHCP", "IPv6 router advertisement", and "Cellular WAN". Under "WAN link manager", there are settings for "Access concentrator/service name", "LCP echo interval" (20 seconds), "LCP failure" (3 attempts), "Schedule time for reconnect", and "IPv6 configuration". Below this is the "DSL settings" section with "VDSL" and "VLAN tag" (2-4094) options. At the bottom, there are "Advanced settings" and buttons for "Save", "Connect", and "Cancel".

tilgin logo and navigation menu. The menu includes: SETUP, VOIP, SWITCH, ADVANCED, WIRELESS, TOOLS, STATUS, ACCOUNT, PHONE, STORAGE, PRINTING, TESTS, HELP. A user notification says "You are logged in as root." with buttons for "Activate VoIP settings", "Save settings", and "Logout".

WAN Setup menu with sub-sections: Connections (WAN mode, Cellular network, L2TP/IPsec server, IPsec), Provisioning (Management server, Polling, TR-069), and LAN Setup (LAN configuration, Firewall/NAT services).

Edit connection

General

Name: Bridge_Mode
Port: WAN
Type: Bridge (Ethernet bridge)
Description:
Status: Online
Uptime: 1 days 1 hours 29 minutes
Enabled

Ethernet interface

Priority:
VLAN ID: 35

Bridge

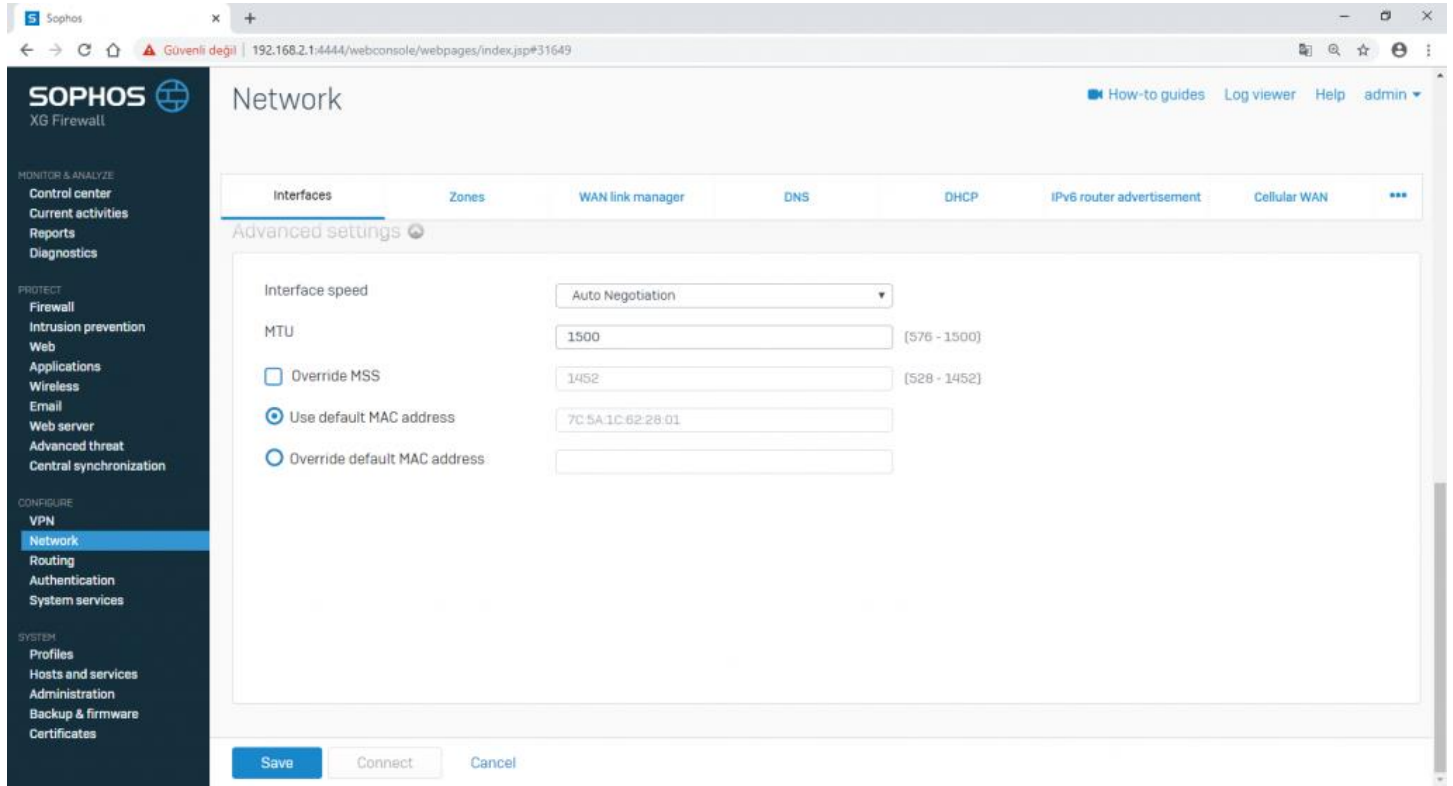
LAN group: Bridge_Mode

Default routing

Confirmation: None, Required for HTTP traffic, Required for all traffic

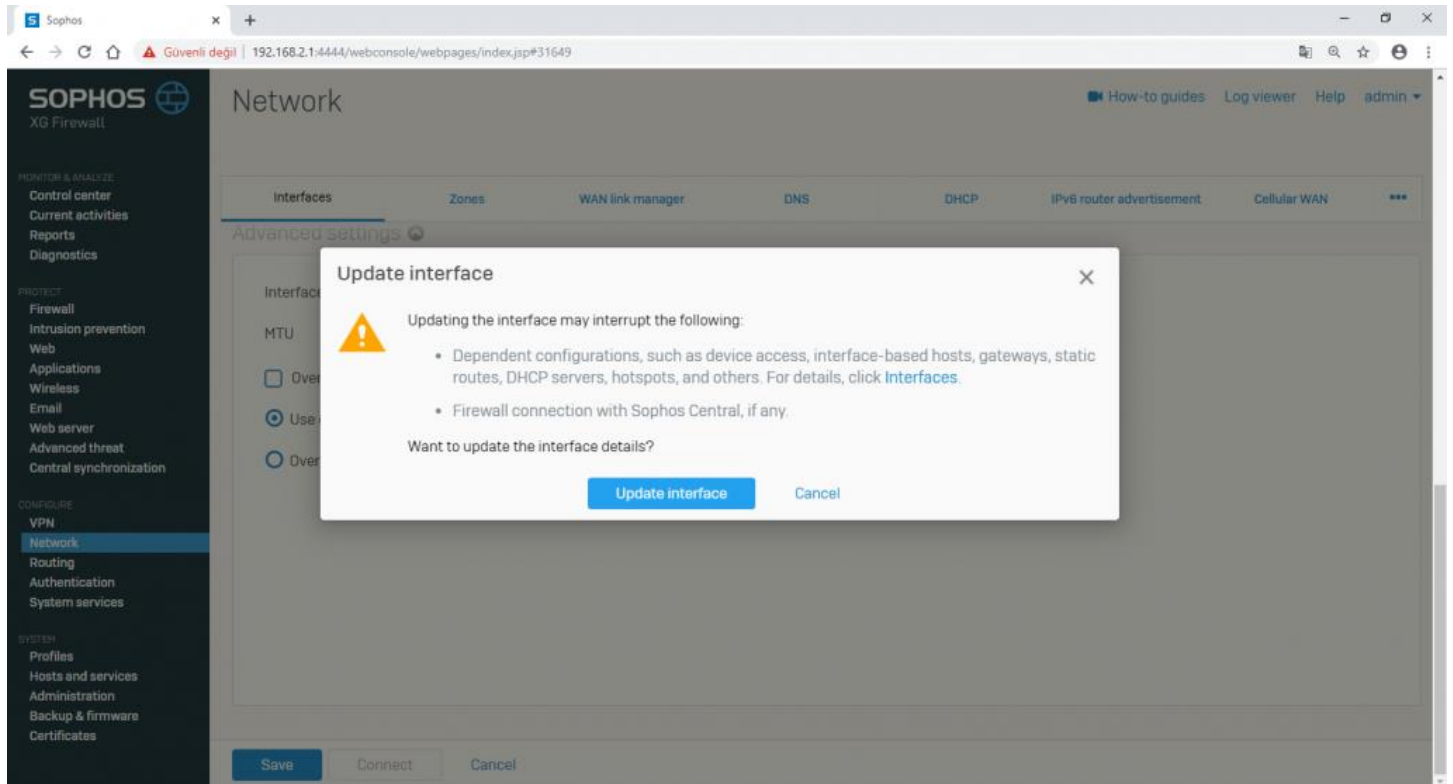
Apply, Reset, Delete buttons

Interface speed değerini **Auto Negotiation** olarak bırakıyoruz. Genellikle piyasada satılan veya Telekomun verdiği **xDSL** modemlerin hız değeri **100mbps** dir.



The screenshot shows the Sophos XG Firewall web console. The left sidebar contains navigation menus for 'MONITOR & ANALYZE', 'PROTECT', 'CONFIGURE', and 'SYSTEM'. The main content area is titled 'Network' and shows the 'Advanced settings' for an interface. The 'Interface speed' is set to 'Auto Negotiation'. Other settings include MTU (1500), Override MSS (1452), and MAC address options. The 'Save' button is highlighted in blue.

Yaptığımız ayarları kaydedip interface arayüzünün güncellenmesini sağlıyoruz.



The screenshot shows the same Sophos XG Firewall web console, but with a warning dialog box open. The dialog box is titled 'Update interface' and contains a warning icon and text: 'Updating the interface may interrupt the following: Dependent configurations, such as device access, interface-based hosts, gateways, static routes, DHCP servers, hotspots, and others. For details, click Interfaces. Firewall connection with Sophos Central, if any. Want to update the interface details?'. The 'Update interface' button is highlighted in blue.

Ayarları kaydettikten sonra **PPPOE** devresi için Firewall bağlantı istekleri gönderecektir. Bu süre içerisinde interface üzerinde **Connecting** yazısını görebilirsiniz.

The screenshot shows the Sophos XG Firewall Network configuration page. A green notification banner at the top states "Interface 'Port2' has been updated successfully". The page is divided into several sections: "MONITOR & ANALYZE" (Control center, Current activities, Reports, Diagnostics), "PROTECT" (Firewall, Intrusion prevention, Web, Applications, Wireless, Email, Web server, Advanced threat, Central synchronization), "CONFIGURE" (VPN, Network, Routing, Authentication, System services), and "SYSTEM" (Profiles, Hosts and services, Administration, Backup & firmware, Certificates). The "Network" section is active, showing a table of interfaces. The "Port2" interface is highlighted in blue and is in a "Connecting" state. The table also shows "GuestAP" and "br0" interfaces.

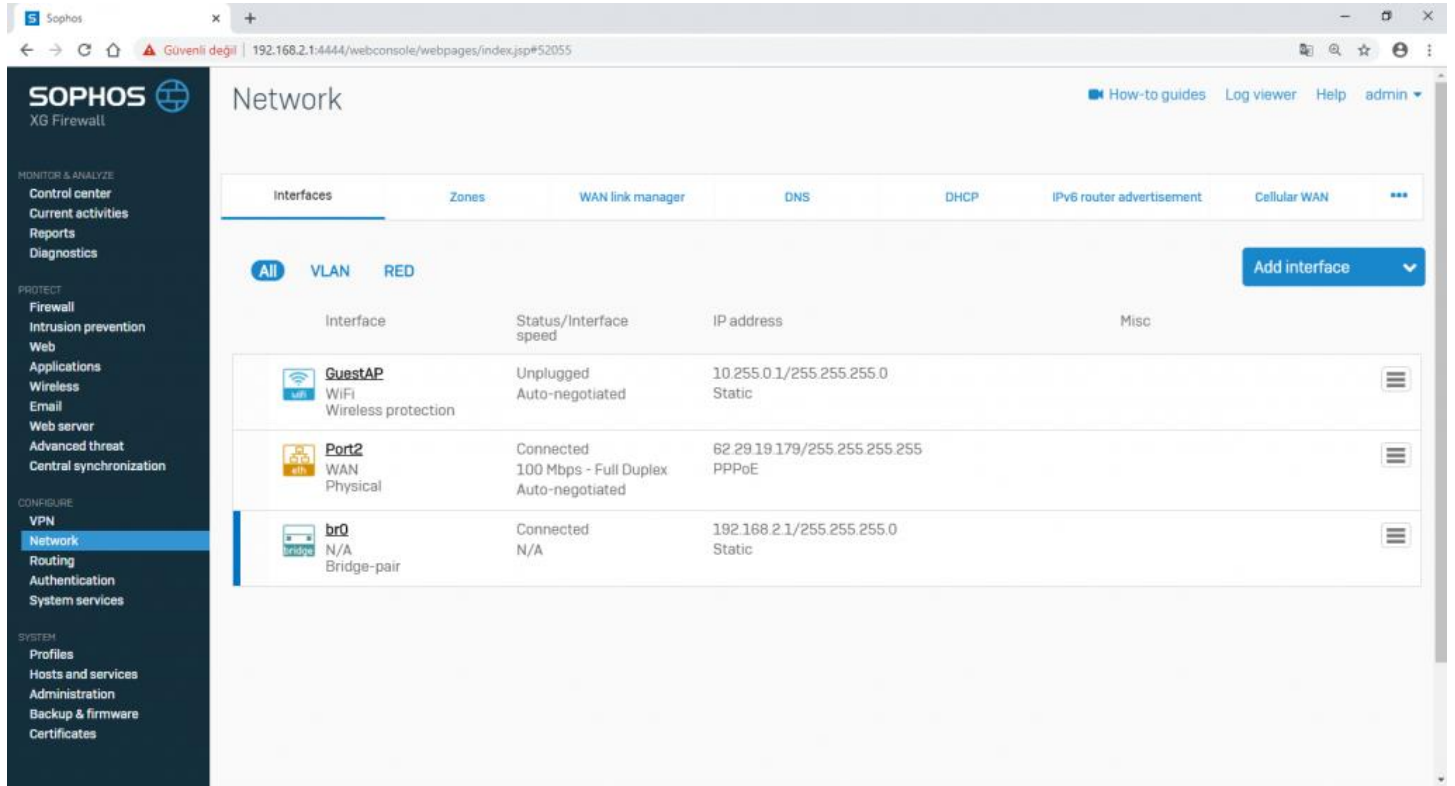
Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
Port2 WAN Physical	Connecting 100 Mbps - Full Duplex Auto-negotiated	N/A PPPoE	
br0 N/A Bridge-pair	Connected N/A	192.168.2.1/255.255.255.0 Static	

PPP(Point to Point Protocol) bağlantısı sağlandıktan sonra bağlantının **Connected** olduğunu görebilirsiniz.

The screenshot shows the Sophos XG Firewall Network configuration page. The "Port2" interface is now in a "Connected" state. The table of interfaces is updated accordingly.

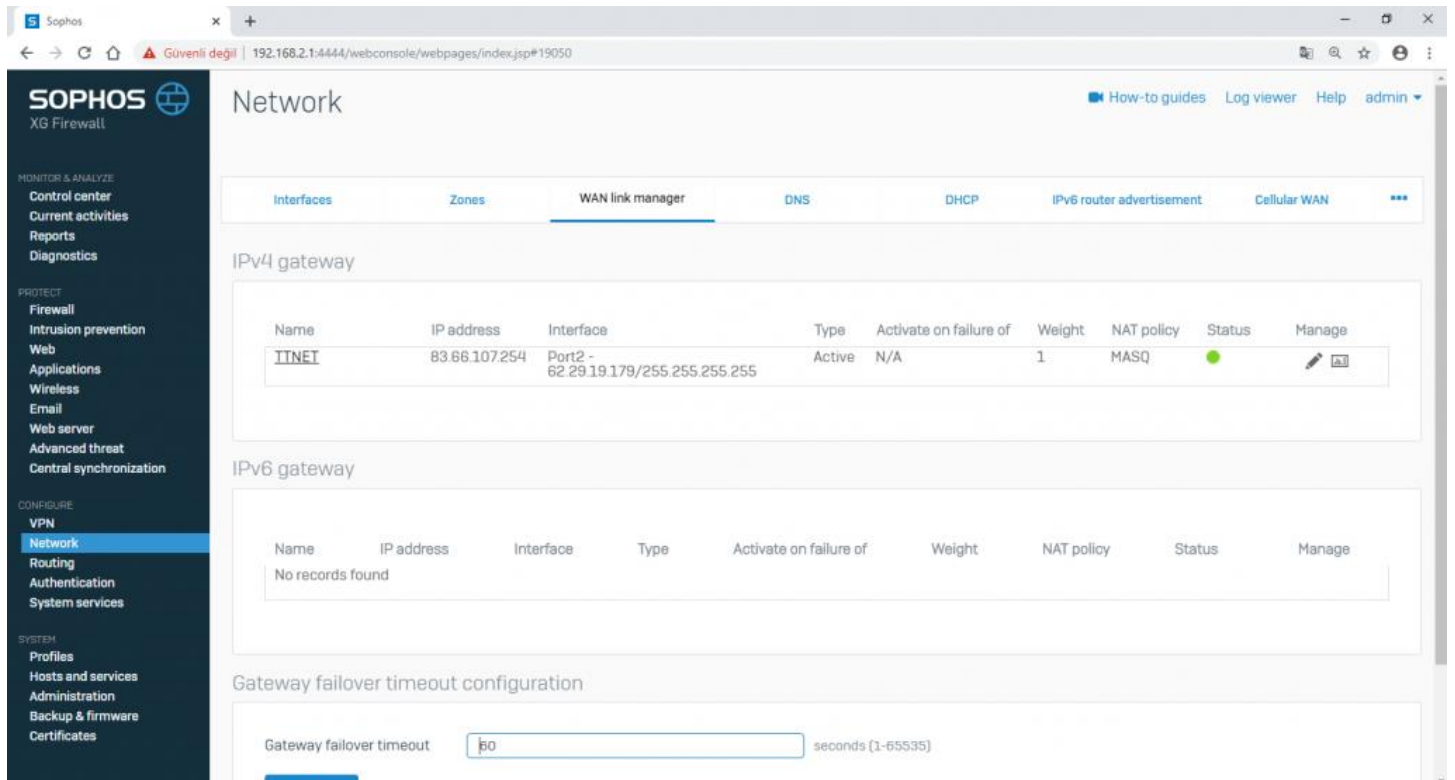
Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	62.29.19.179/255.255.255.255 PPPoE	
br0 N/A Bridge-pair	Connected N/A	192.168.2.1/255.255.255.0 Static	



PPPOE bağlantı sağlandıktan sonra ilk iş cihaza **Public DNS** olmalıdır çünkü cihazın herhangi bir şekilde **DNS** problemi yaşamaması gerekmektedir.



Interface	Status/Interface speed	IP address	Misc
GuestAP WiFi Wireless protection	Unplugged Auto-negotiated	10.255.0.1/255.255.255.0 Static	
Port2 WAN Physical	Connected 100 Mbps - Full Duplex Auto-negotiated	62.29.19.179/255.255.255.255 PPPoE	
br0 N/A Bridge-pair	Connected N/A	192.168.2.1/255.255.255.0 Static	

PPPOE devresini oluşturduğumuzda Firewall bizim için **Default Gateway MASQ** objesini kendini otomatik yaratmaktadır. Böylelikle basit bir şekilde kural yazarak internete çıkışımızı vermektedir.



Name	IP address	Interface	Type	Activate on failure of	Weight	NAT policy	Status	Manage
TTNET	83.66.107.254	Port2 - 62.29.19.179/255.255.255.255	Active	N/A	1	MASQ	●	 

Gateway failover timeout configuration

Gateway failover timeout: seconds (1-65535)

SOPHOS
XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Routing

Static routing Policy routing Gateways BGP OSPF Information Upstream proxy

IPv4 gateway

Name	IP address	Interface	Health check	NAT policy	Status	Manage
TINET	83.66.107.254	Port2	On	MASQ	●	

IPv6 gateway

No records found

Basic internet kuralı yazmak için **Protect / Firewall** —> **Add firewall rule** butonuna tıkladıktan sonra **User/network rule** eklememiz gerekmektedir.

SOPHOS
XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Firewall

IPv4 IPv6 Enable filter

+ Add firewall rule

ID	Name	Source	Destination	What	Action
No records found					

User/network rule
Control traffic for your users and networks.

Business application rule
Protect and control access to your servers and services.

https://192.168.2.1:4444/webconsole/webpages/index.jsp#

Local(Private) alandan **Wan(Public)** alana doğru **Public Network** adresimizi seçerek **Dynamic Nat** kuralı yazmalıyız.

Yazacağımız kural aşağıdaki gibi olmalıdır;

Action: Accept

Source Zone: LAN **Source**

Local Network: Any

Services: Any

Destination Zone: Wan

Destination Network: Any

Services: Any

The screenshot shows the Sophos XG Firewall web console interface for adding a user/network rule. The rule name is 'Local To INT'. The action is set to 'Accept'. The source zone is 'LAN', and the source networks and devices are set to 'Any'. The destination zone is 'WAN', and the destination networks are set to 'Any'. The rule position is 'Top' and the rule group is 'None'. The 'During scheduled time' is set to 'All the time'. The 'Save' button is highlighted in blue.

NAT'ın görevi genel olarak yerel network'ümüzde sahip olduğumuz **Private IP** adresimizi yönlendirilebilir **Public IP** adresine çevirmektir.

Yazdığımız kuralı internete natlamak için **“Rewrite source adres(masquerading)”** alanını işaretledikten sonra **“Use outbound address”** alanından default **MASQ'yu** ve **Primary ISP** devremizi seçiyoruz.

Kural üzerinden geçecek trafiği izlemek için loglamayı açmalıyız.

SOPHOS XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Edit user/network rule

How-to guides Log viewer Help admin

Advanced

User applications

Intrusion prevention ⚠
None

Traffic shaping policy
None

Web policy ⚠
None

Apply web-category-based traffic shaping policy

Application control ⚠
None

Apply application-based traffic shaping policy

Synchronized security ⚠

Minimum source HB permitted:
 GREEN YELLOW No restriction
 Block clients with no heartbeat

Minimum destination HB permitted:
 GREEN YELLOW No restriction
 Block request to destination with no heartbeat

NAT & routing

Rewrite source address (masquerading)

Use gateway-specific default NAT policy

Use outbound address
MASQ
MASQ (62.29.19.179)

Primary gateway
TTNET

Backup gateway
None

DSCP marking
Select DSCP marking

Log traffic

Save Cancel

Local To Local erişim sağlamak için Lan Networkümüzden Lan Networkümüze doğru kural yazmalıyız

Yazacağımız kuralı **Sophos XG** Local bir kural olduğunu algılayıp Natlamayı otomatik kapatacaktır..

Sophos

Güvenli değil | 192.168.2.1:4444/webconsole/webpages/index.jsp#62051

Firewall

How-to guides Log viewer Help admin

IPv4 IPv6 Enable filter

+ Add firewall rule

ID	Name	Source	Destination	What
1	Local To INT in 43.99 KB, out 18.00 KB	LAN, Any host	WAN, Any host	Any service

User/network rule
Control traffic for your users and networks.

Business application rule
Protect and control access to your servers and services.

Sophos XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Add User/network rule

How-to guides Log viewer Help admin

Rule name * Local To Local
Description Enter Description
Rule position Bottom
Action **Accept** Drop Reject
Rule group None

Source

Source zones * LAN
Source networks and devices * Any
During scheduled time All the time

Destination & services

Destination zones * LAN
Destination networks * Any
Services * Any

Save Cancel

Sophos XG Firewall

MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics

PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization

CONFIGURE
VPN
Network
Routing
Authentication
System services

SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates

Add User/network rule

How-to guides Log viewer Help admin

User applications
Intrusion prevention ⚠️ None
Traffic shaping policy None
Web policy ⚠️ None
Application control ⚠️ None

Synchronized security ⚠️
Minimum source HB permitted:
 GREEN YELLOW No restriction
 Block clients with no heartbeat

Minimum destination HB permitted:
 GREEN YELLOW No restriction
 Block request to destination with no heartbeat

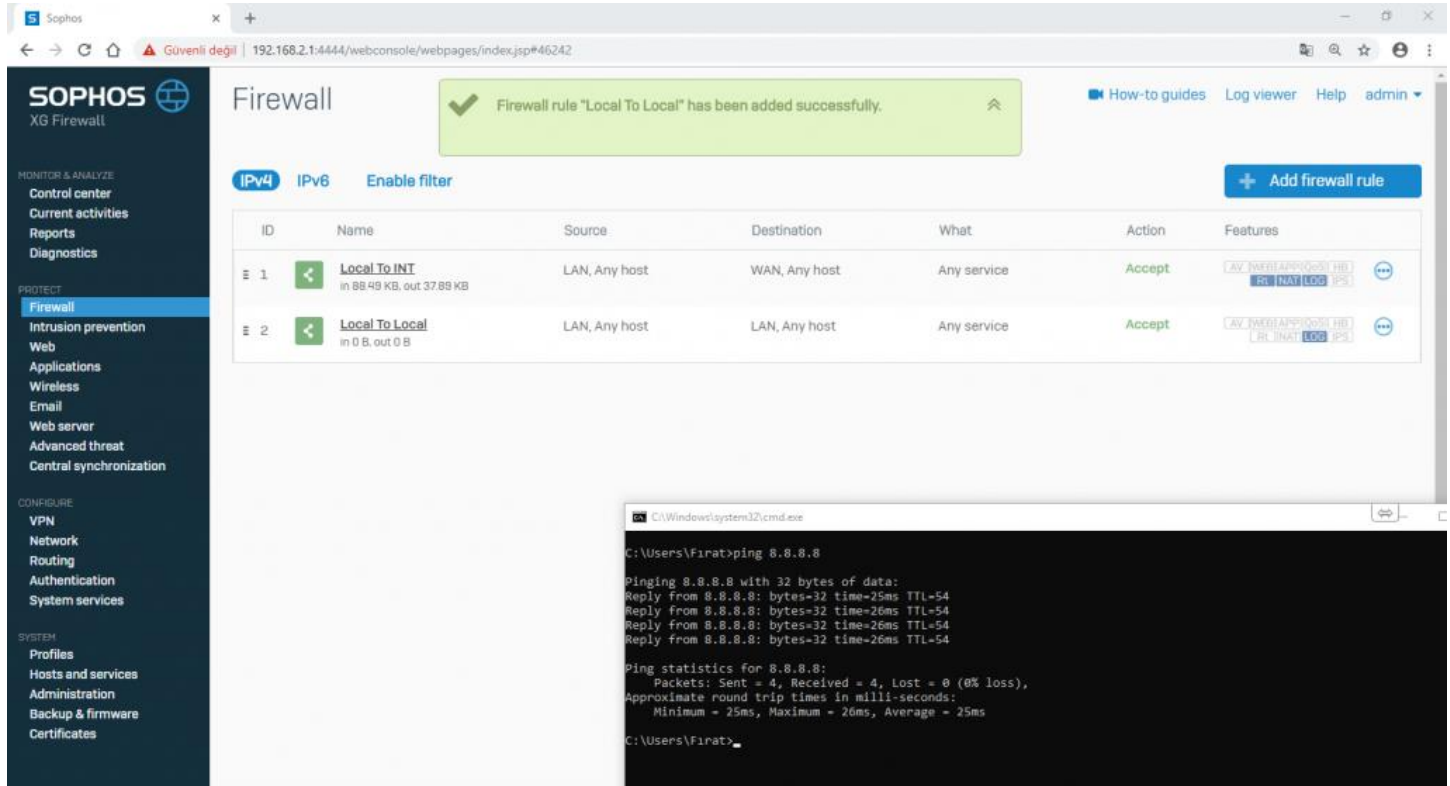
NAT & routing
 Rewrite source address (masquerading)
Primary gateway None
Backup gateway None
DSCP marking Select DSCP marking

Log traffic

Log firewall traffic

Save Cancel

Kuralımızı kaydettikten sonra internet çıkışı için google'nin kullanmış olduğu public dns adreslerine ping atmamız yeterli olacaktır.



The screenshot displays the Sophos XG Firewall web console. A green notification banner at the top states: "Firewall rule 'Local To Local' has been added successfully." The main interface shows a table of firewall rules with the following columns: ID, Name, Source, Destination, What, Action, and Features. Two rules are listed:

ID	Name	Source	Destination	What	Action	Features
1	Local To INT in 88.48 KB, out 37.89 KB	LAN, Any host	WAN, Any host	Any service	Accept	AV, TWEET, APP, GOS, HE, RI, NAT, LOG, IPS
2	Local To Local in 0 B, out 0 B	LAN, Any host	LAN, Any host	Any service	Accept	AV, TWEET, APP, GOS, HE, RI, NAT, LOG, IPS

Below the table, a terminal window shows the command prompt results for a ping test to 8.8.8.8:

```
C:\Windows\system32\cmd.exe
C:\Users\Firat>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=25ms TTL=54
Reply from 8.8.8.8: bytes=32 time=26ms TTL=54
Reply from 8.8.8.8: bytes=32 time=26ms TTL=54
Reply from 8.8.8.8: bytes=32 time=26ms TTL=54

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 25ms, Maximum = 26ms, Average = 25ms

C:\Users\Firat>
```

Umarım sizler için faydalı bir paylaşım olmuştur.

Firat Meray | Network and Information Security Specialist