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 kapsullemede internet çıkışımız olmayacaktır.

Modemi Bridge Moda alirken dikkat edilmesi gerekenler;

* Modem ile Firewall farkli 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 önerdiğiöiz 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;

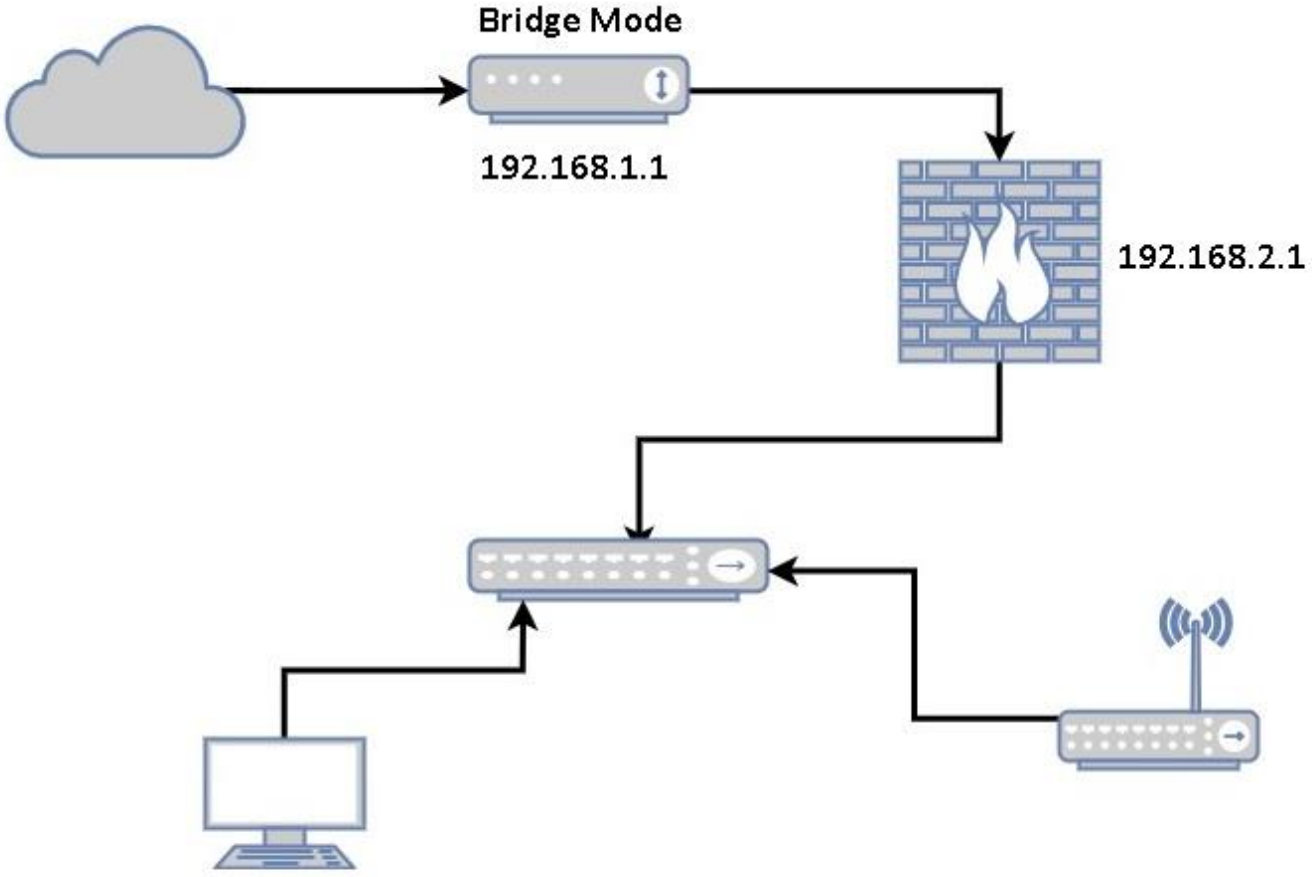
ADSL:
WAN ID Type – PPP Transfer Type – Ağ Protokolü – Kapsülleme: PPPoE
Aktarım Modu – Modülasyon: ATM
VPI / VCI: 8/35

VDSL:
WAN ID Type – PPP Transfer Type – Ağ Protokolü – Kapsülleme: PPPoE
Aktarım Modu – Modülasyon: PTM
VLAN ID: 35

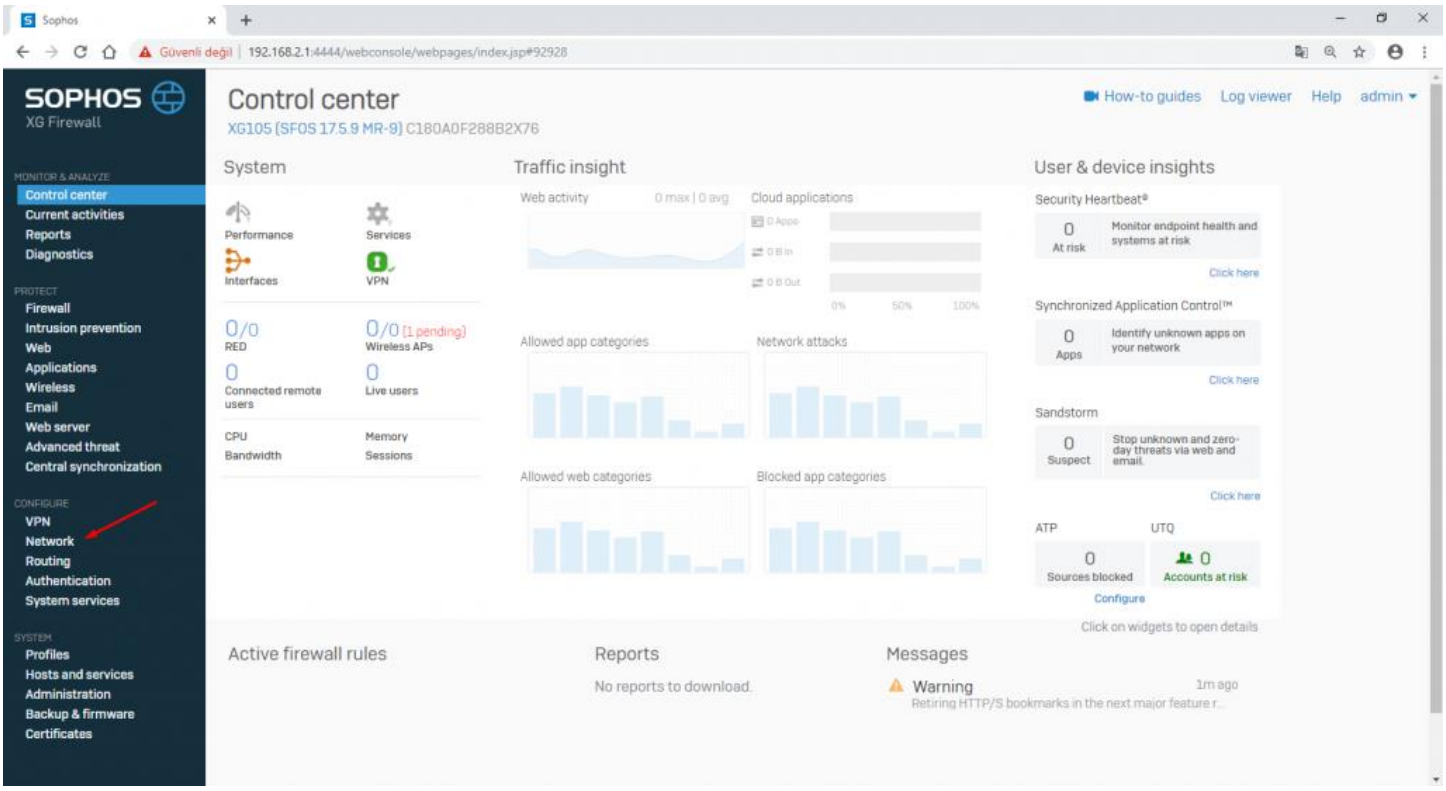
XDSL devrelerinin local santrale olan uzaklıklarını ve data hızlarını aşağıdaki tablodan karşılaştırabiliriz;

		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

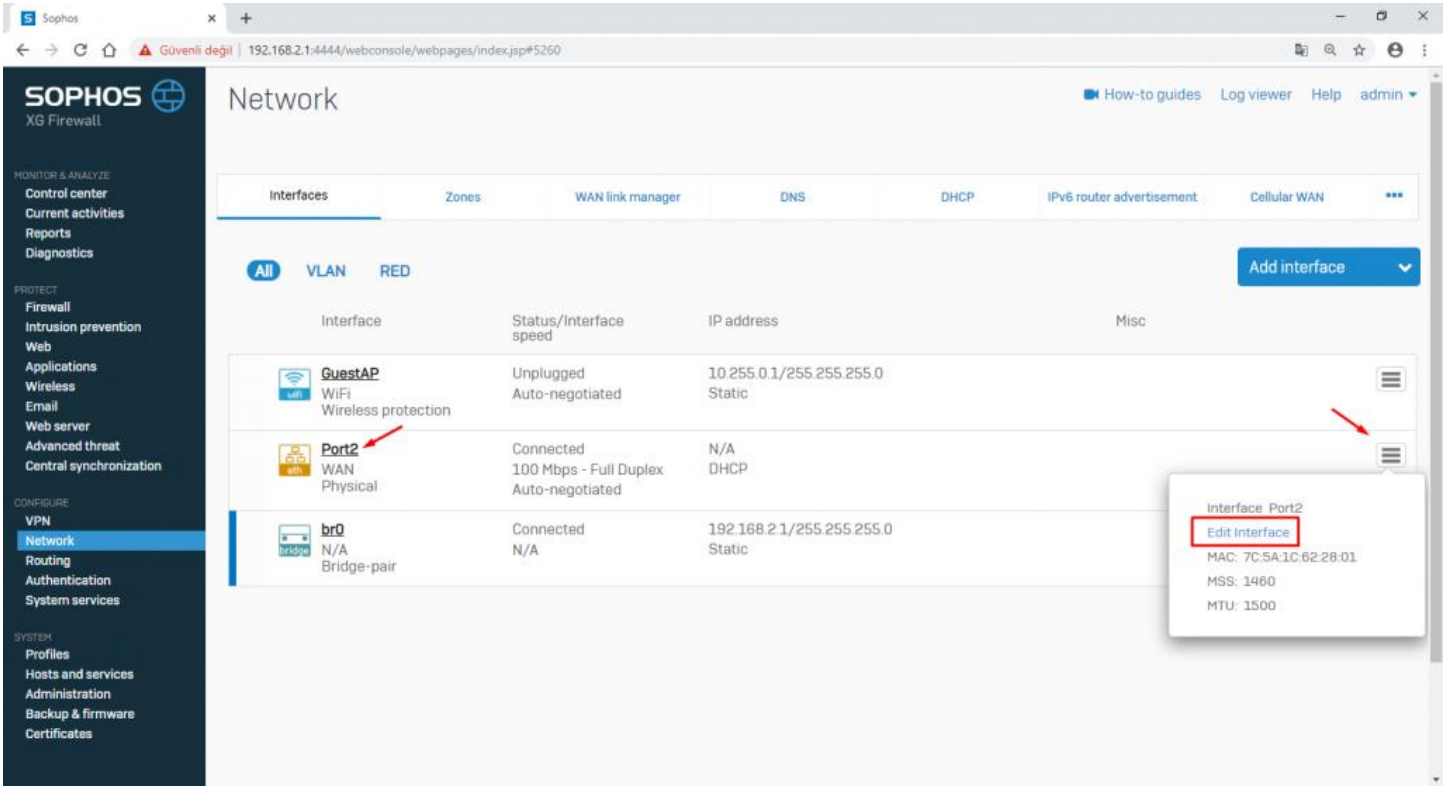
Bridge Mode Şemamız;



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



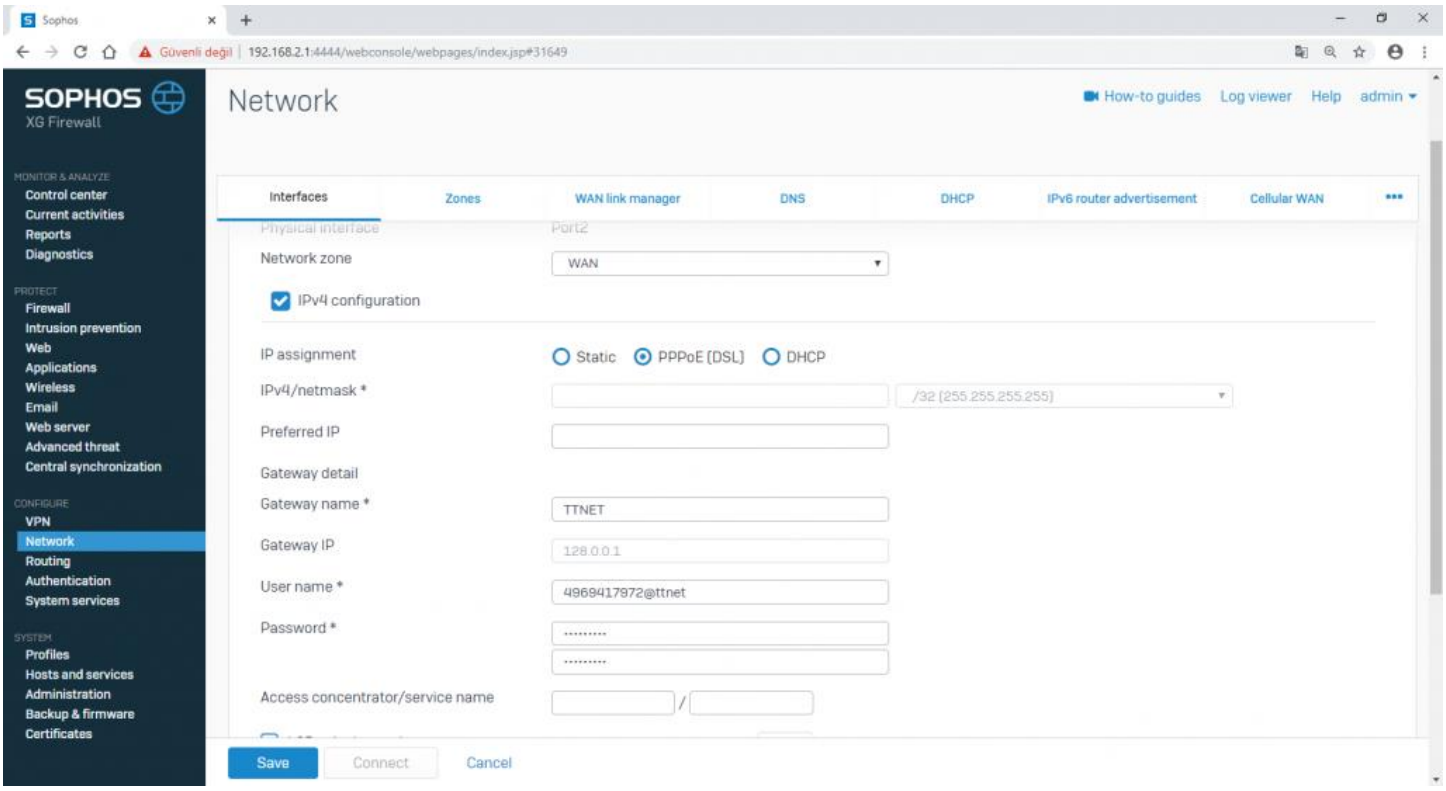
Karşımıza gelen ekranda dilerseniz Interface ismine tıklayabilir yada sağ tarafta alt alta 3 çizgi görünen alana tıklayıp **Edit Interface** diyerek ethernet arayüzünün içerisine giriş yapabiliriz.



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.

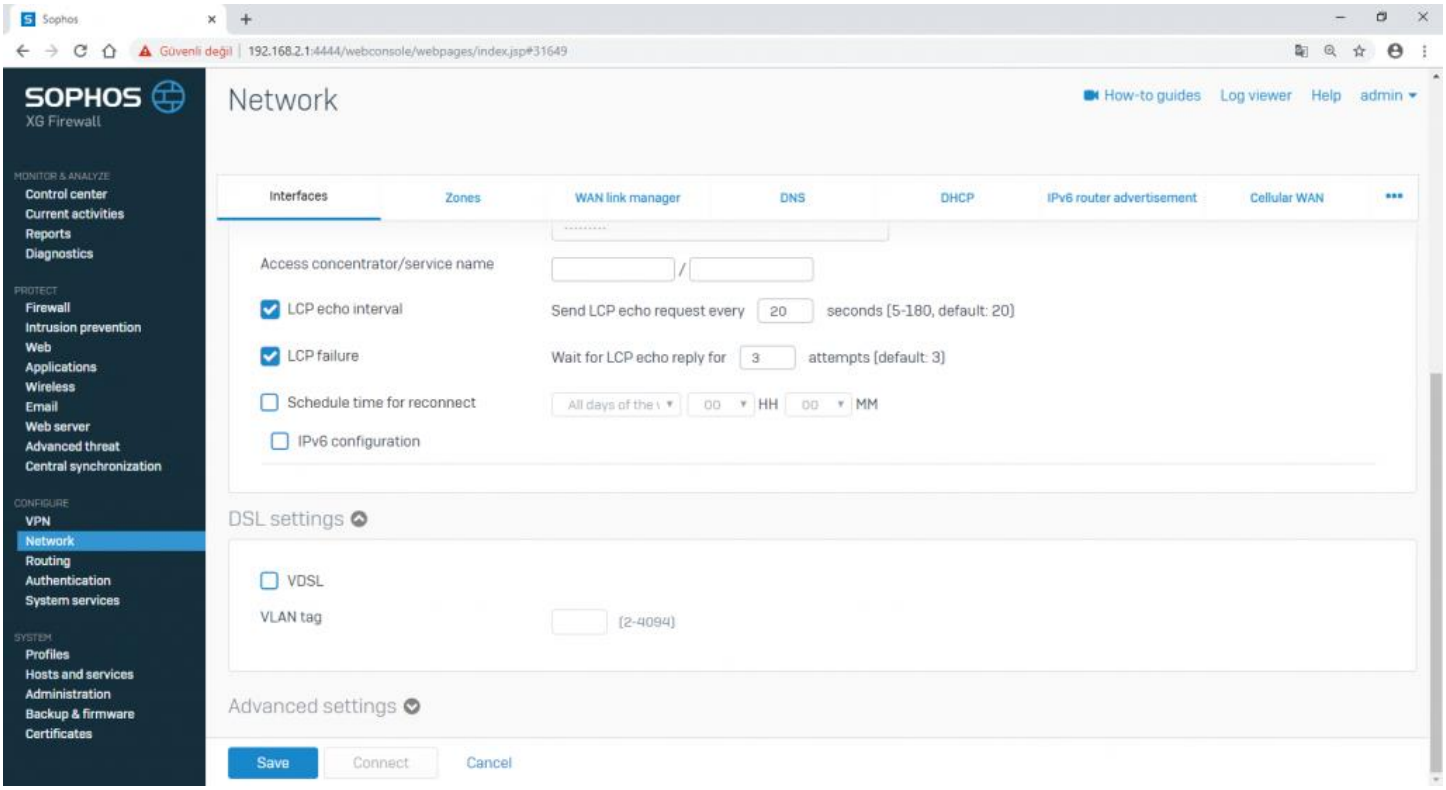


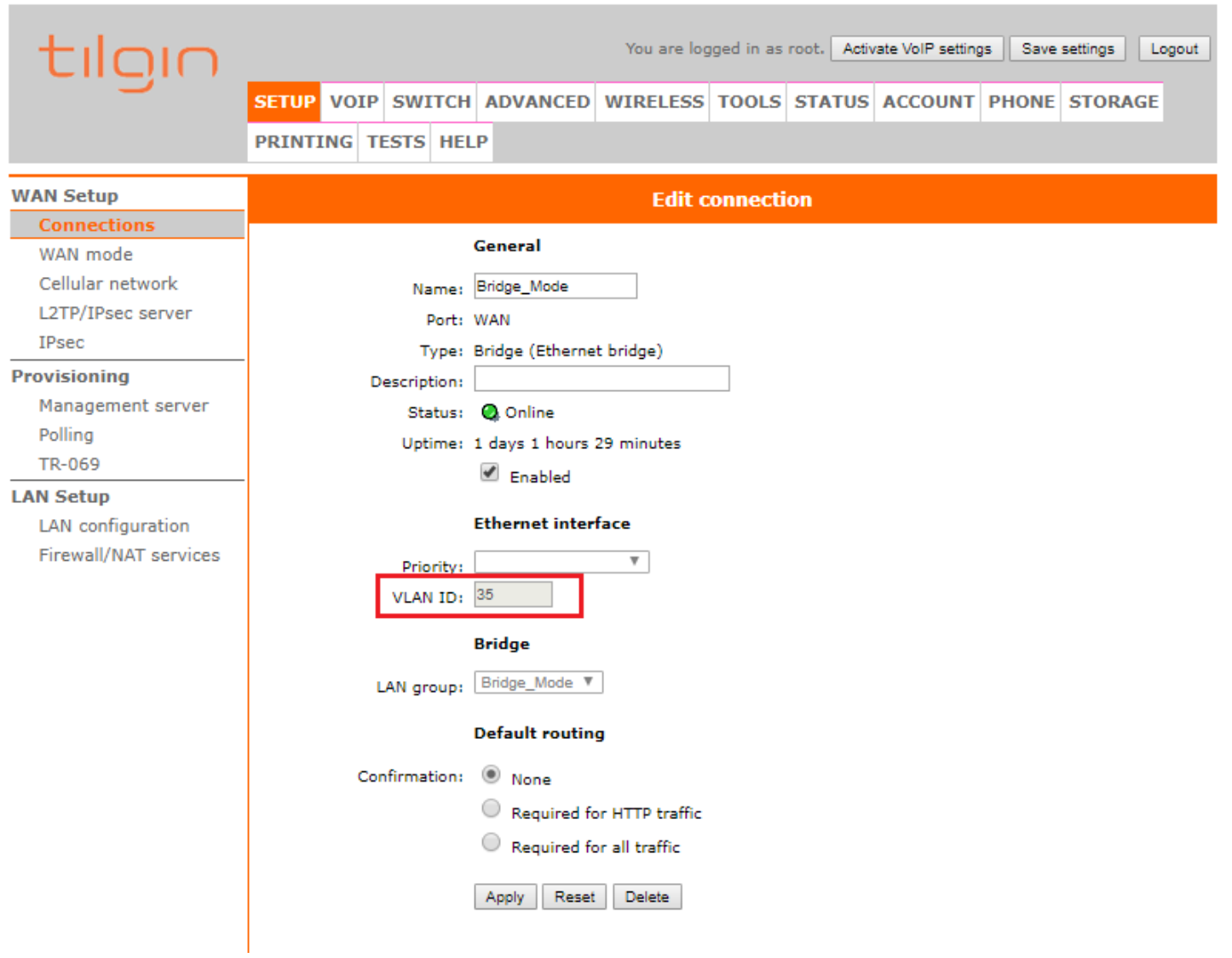
LCP echo interval ve **LCP failure** alanlarını enable ediyoruz.

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 görevlidir.

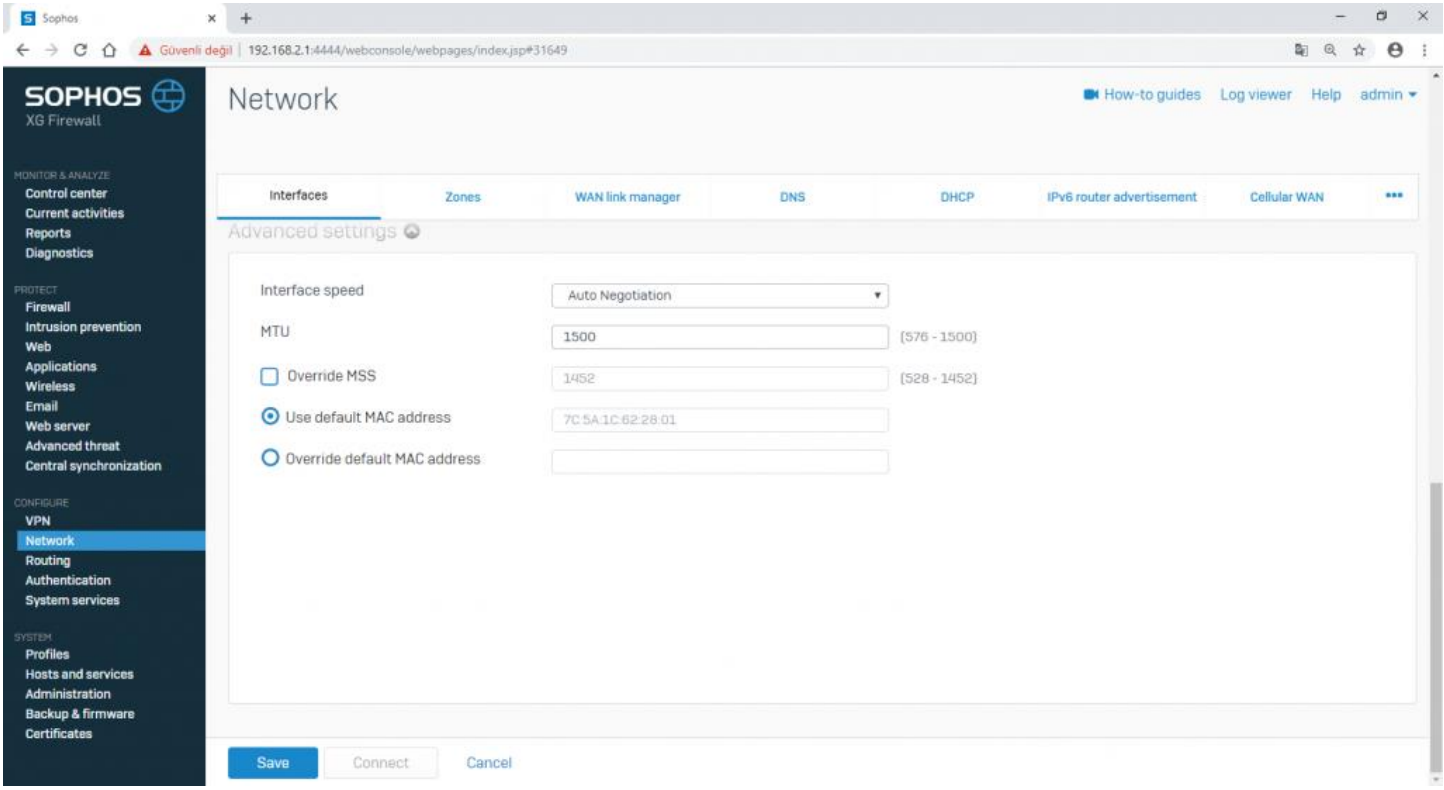
Tılgın Modemler Vlan Tag girişini zorunlu tuttuğu için **Vlan:35** değerini **Tılgın modeme** yazıyoruz.

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.

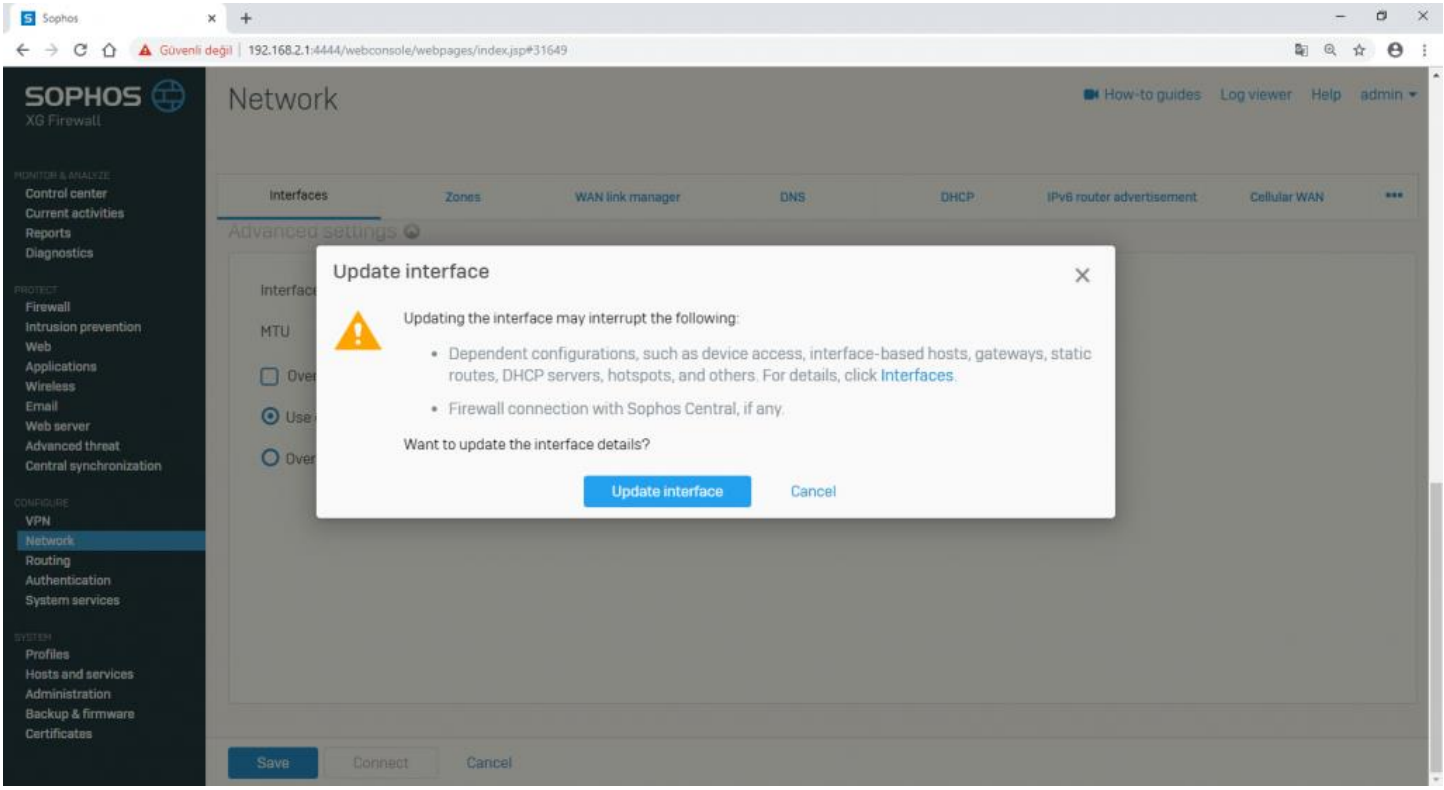

Sophos
Güvenli değil | 192.168.2.1:4444/webconsole/webpages/index.jsp#31649
SOPHOS
XG Firewall
Network
How-to guides
Log viewer
Help
admin
MONITOR & ANALYZE
Control center
Current activities
Reports
Diagnostics
PROTECT
Firewall
Intrusion prevention
Web
Applications
Wireless
Email
Web server
Advanced threat
Central synchronization
CONFIGURE
VPN
Network
Routing
Authentication
System services
SYSTEM
Profiles
Hosts and services
Administration
Backup & firmware
Certificates
Interfaces
Zones
WAN link manager
DNS
DHCP
IPv6 router advertisement
Cellular WAN
Access concentrator/service name
LCP echo interval
Send LCP echo request every 20 seconds (5-180, default: 20)
LCP failure
Wait for LCP echo reply for 3 attempts (default: 3)
Schedule time for reconnect
IPv6 configuration
DSL settings
VDSL
VLAN tag
(2-4094)
Advanced settings
Save
Connect
Cancel


tilgin
You are logged in as root.
Activate VoIP settings
Save settings
Logout
SETUP
VOIP
SWITCH
ADVANCED
WIRELESS
TOOLS
STATUS
ACCOUNT
PHONE
STORAGE
PRINTING
TESTS
HELP
WAN Setup
Connections
WAN mode
Cellular network
L2TP/IPsec server
IPsec
Provisioning
Management server
Polling
TR-069
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

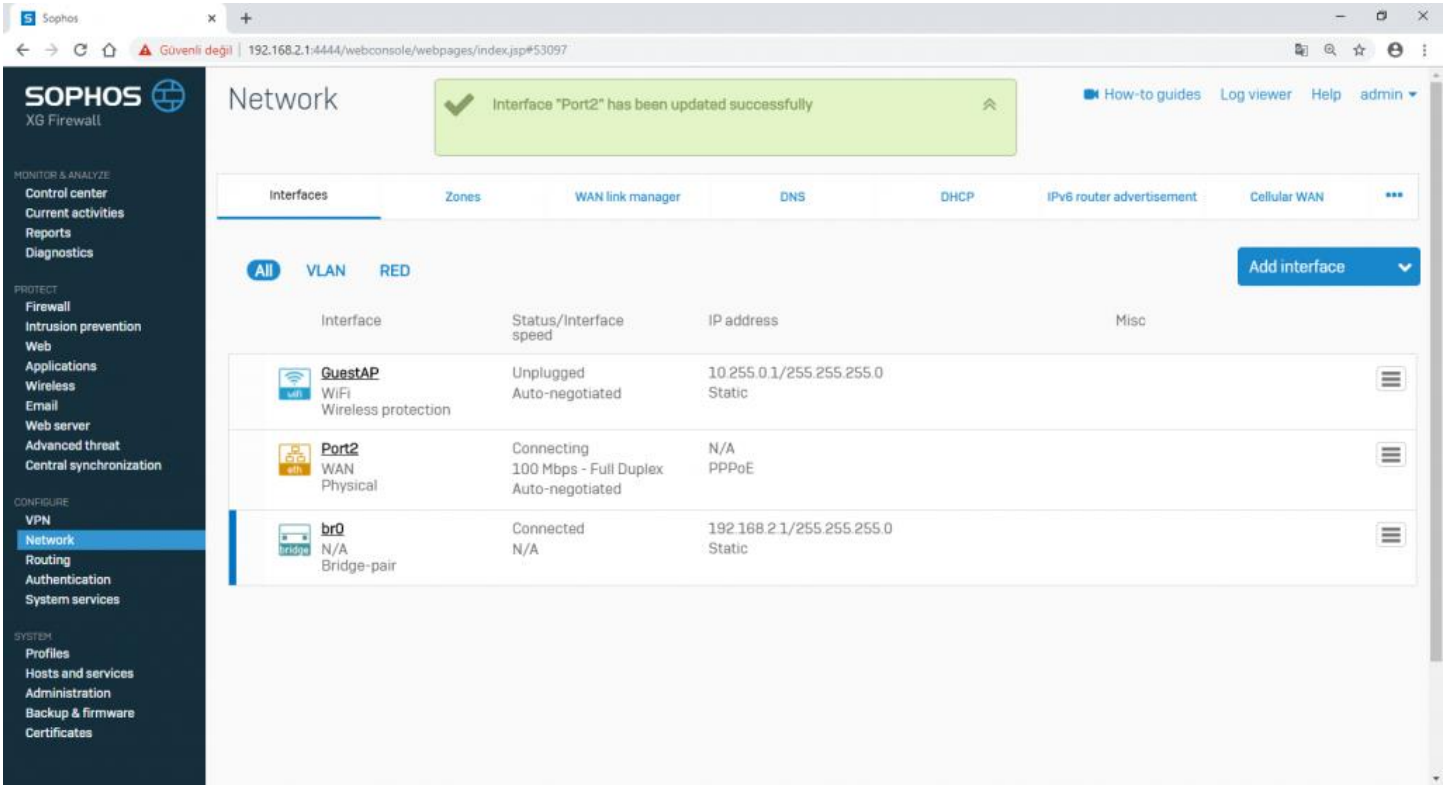
Interface speed değerini **Auto Negotiation** olarak bırakıyoruz. Genellikle piyasada satılan veya **Telekomun** verdiği **xDSL** modemlerin hız değeri **100mbps** dır.



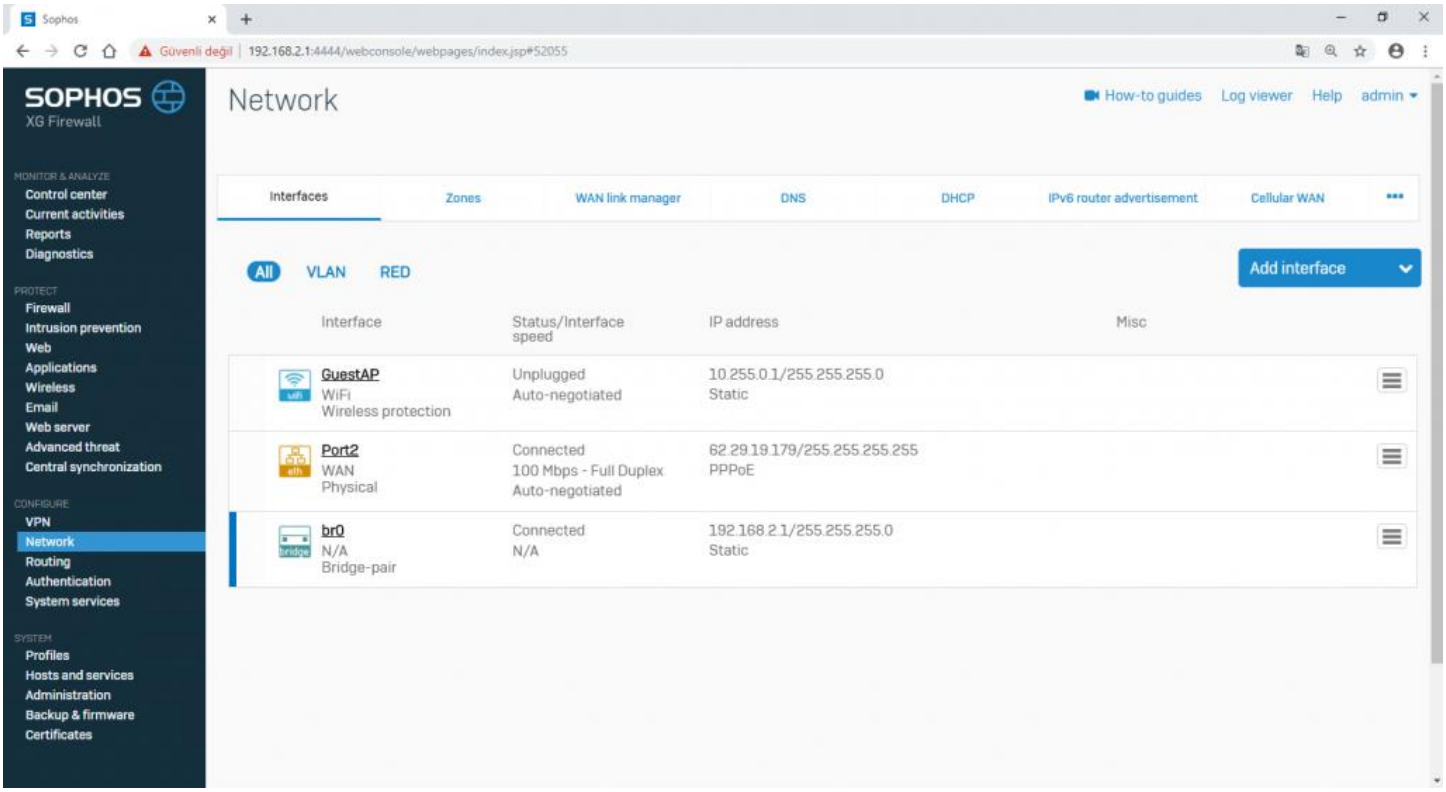
Yaptığımız ayarları kaydedip interface arayüzünün güncellenmesini sağlıyoruz.



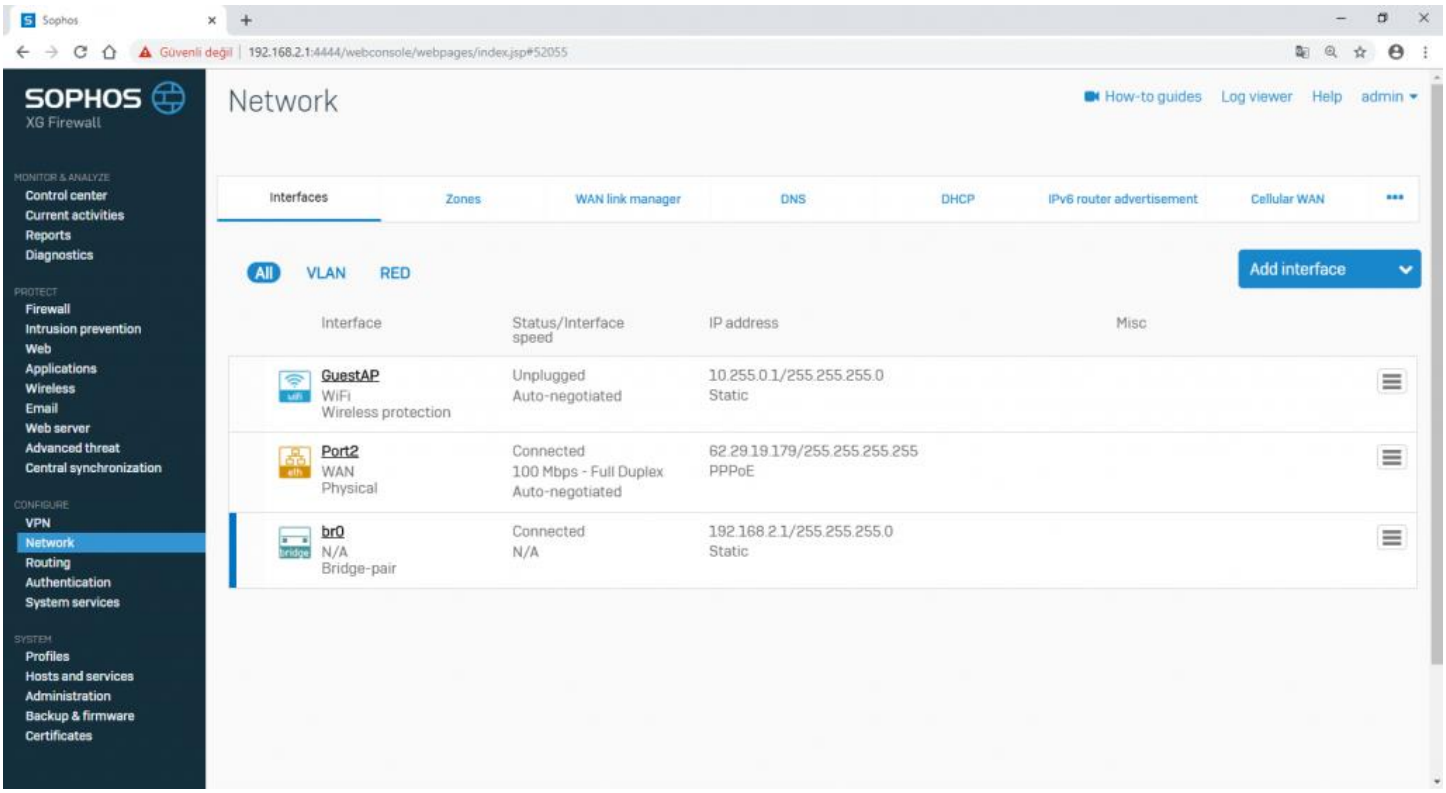
Ayarları kaydettikten sonra **PPPOE** devresi için Firewall bağlantı istekleri gönderecektir. Bu süre içerisinde interface üzerinde **Connecting** yazısını görebilirsiniz.



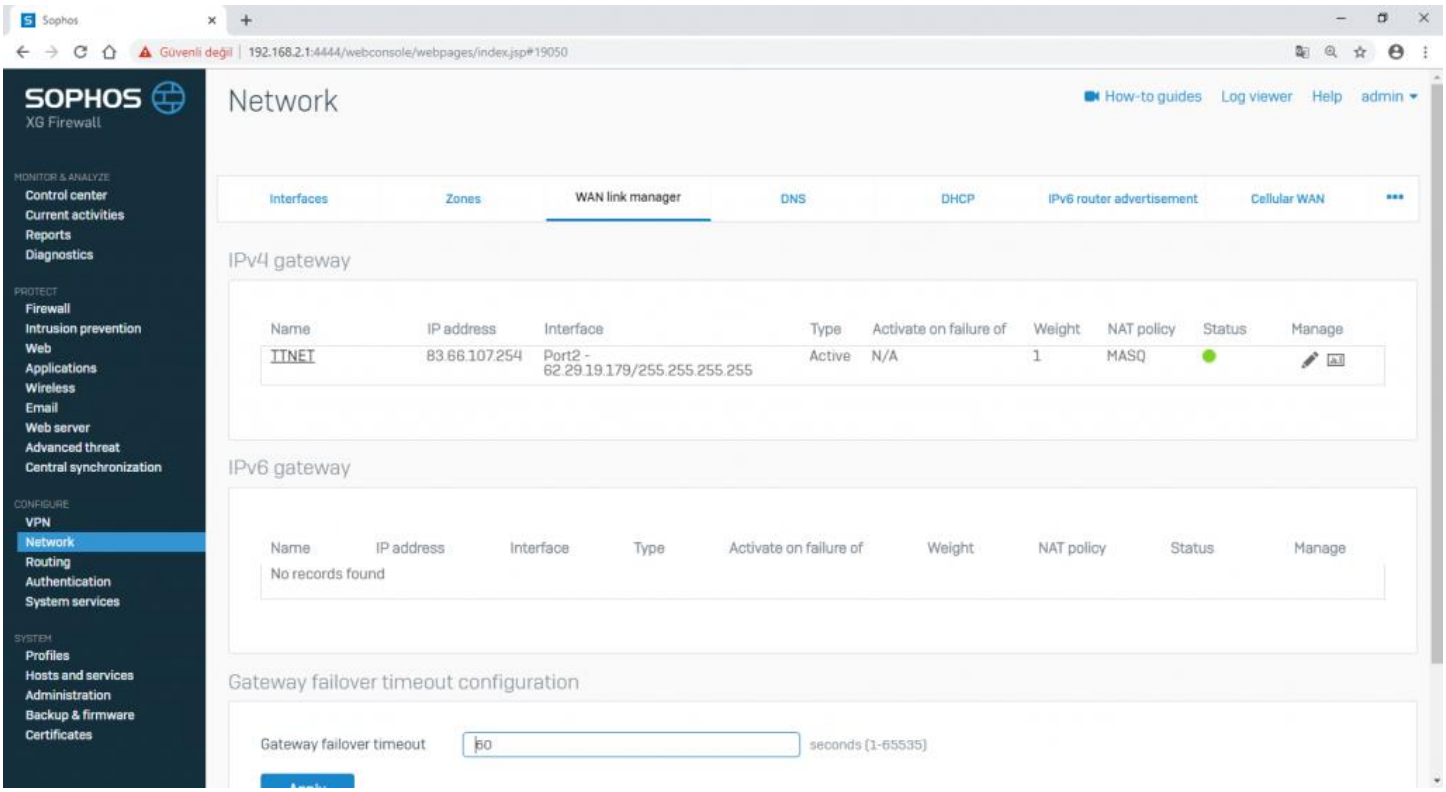
PPP(Point to Point Protocol) bağlantısı sağlandıktan sonra bağlantının **Connected** olduğunu görebilirsiniz.

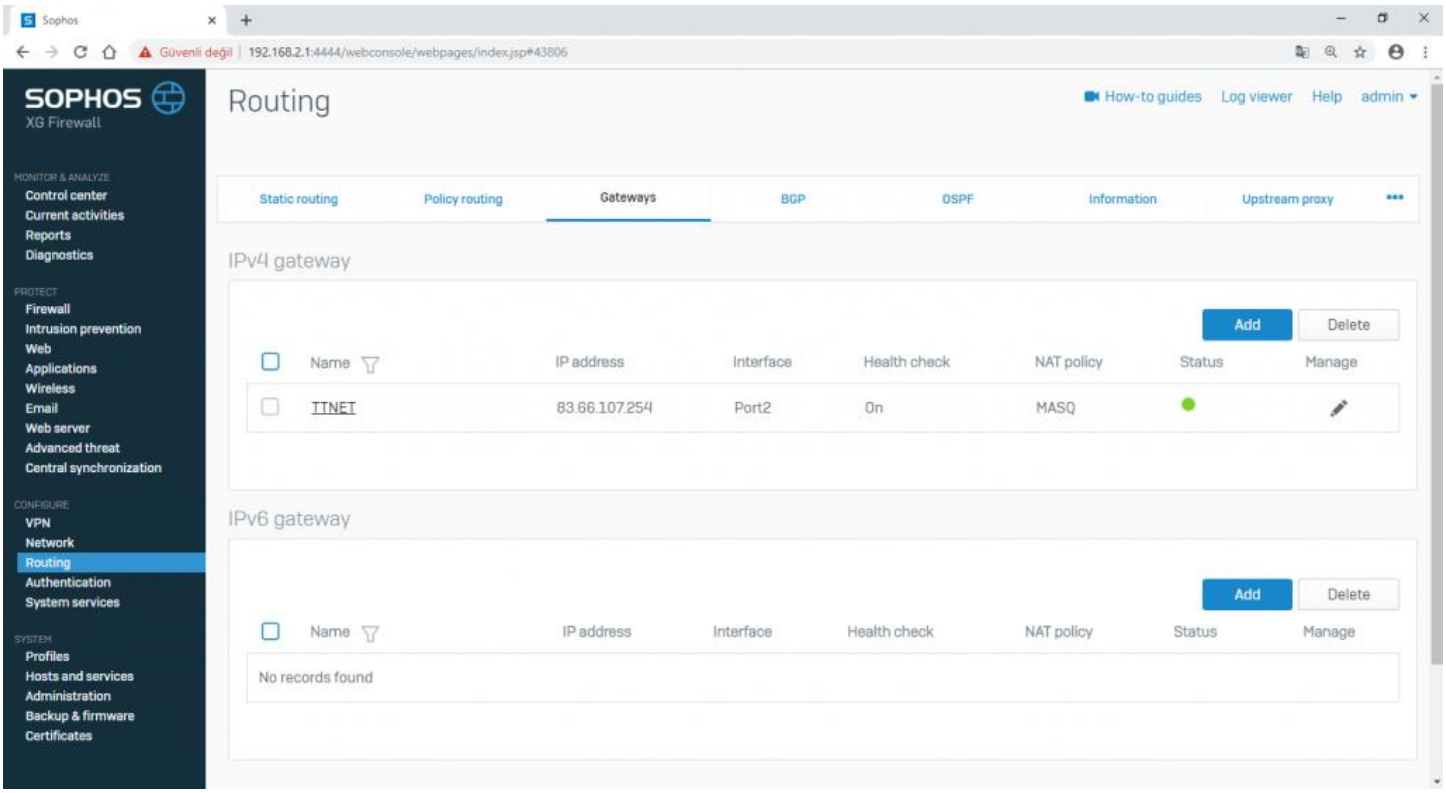


PPPOE bağlantı sağlandıktan sonra ilk iş cihaza **Public DNS** olmalıdır çünkü cihazın herhangi bir şekilde **DNS** problemi yaşamaması gerekmektedir.

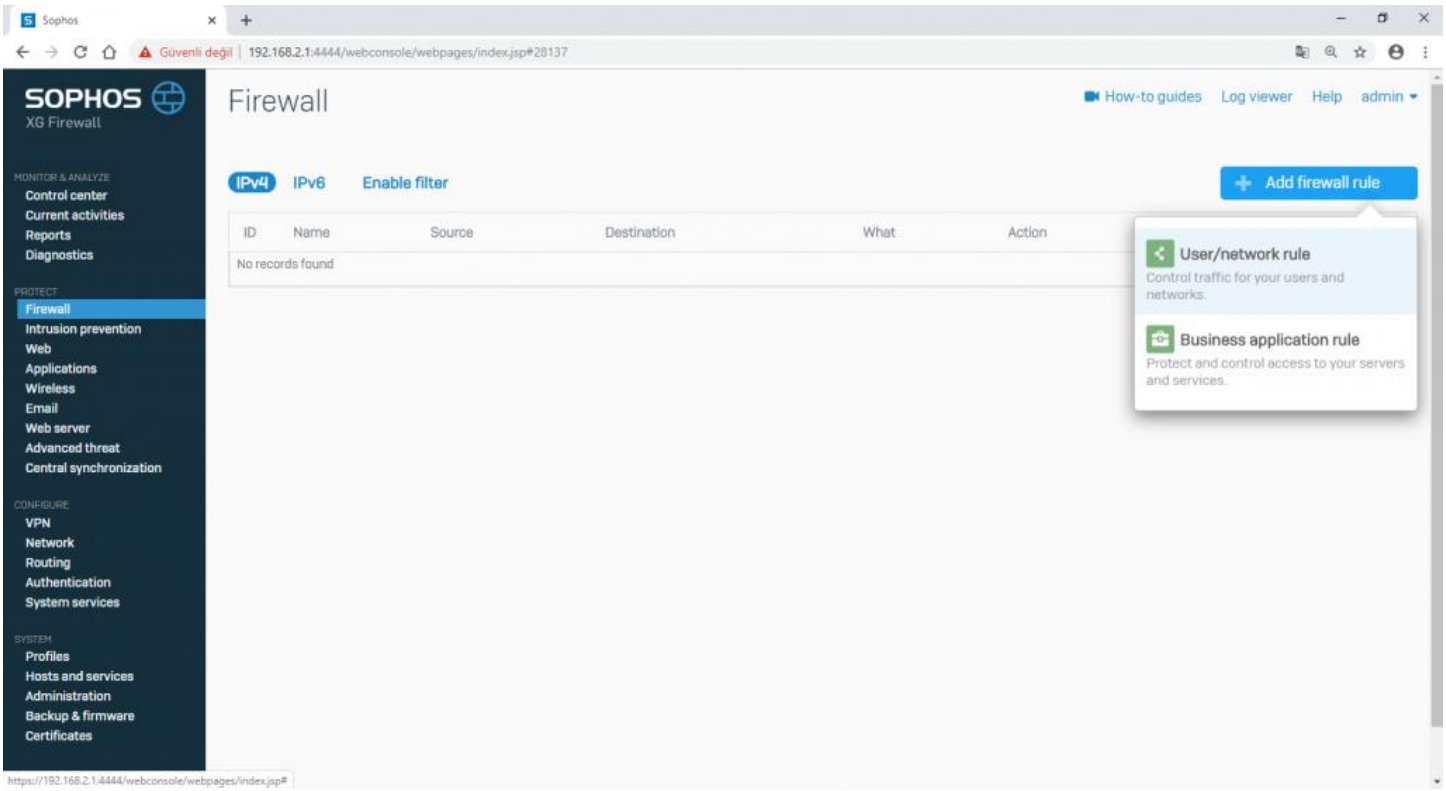


PPPOE devresini oluşturduğumuzda Firewall bizim için **Default Gateway MASQ** objesini kendini otomatik yaratmaktadır. Böylelikle basit bir şekilde kural yazarak internete çıkışımızı vermektedir.





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



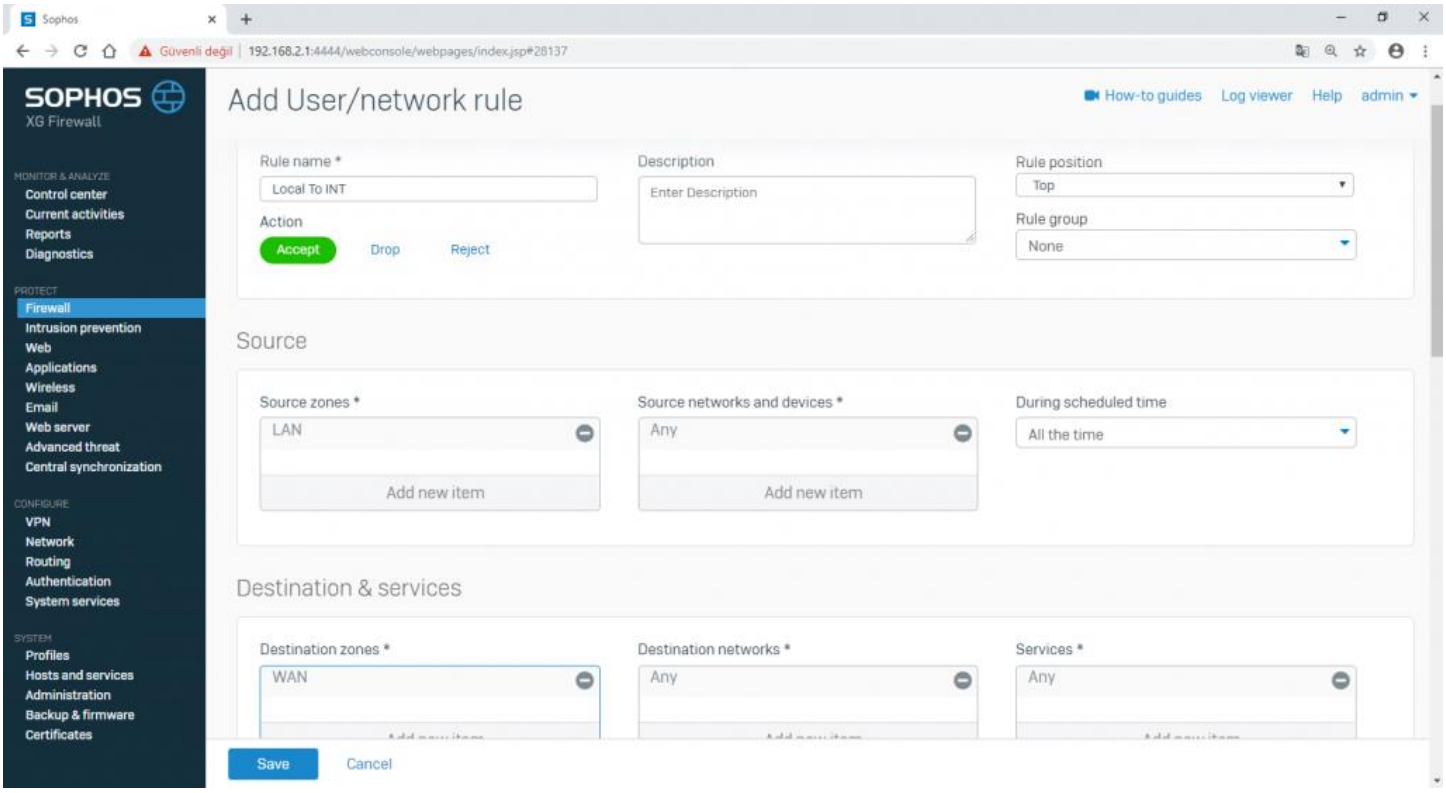
Local(Private) alandan **Wan(Public)** alana doğru **Public Network** adresimizi seçerek **Dynamic Nat** kuralı yazmalıyız.

Yazacağımız kural aşağıdaki gibi olmalıdır;

Action: Accept

Source Zone: LAN **Source**
Local Network: Any
Services: Any

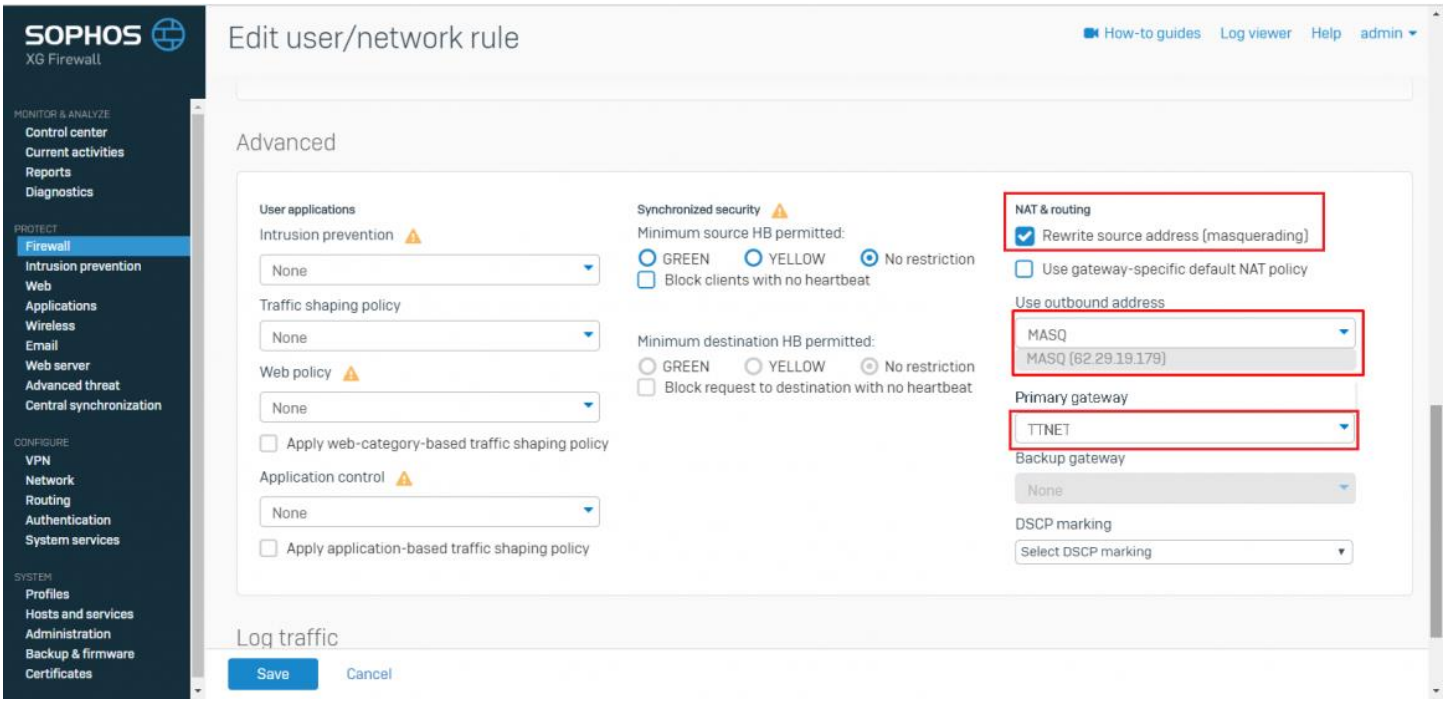
Destinatination Zone: Wan
Destinatination Network: Any
Services: Any



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

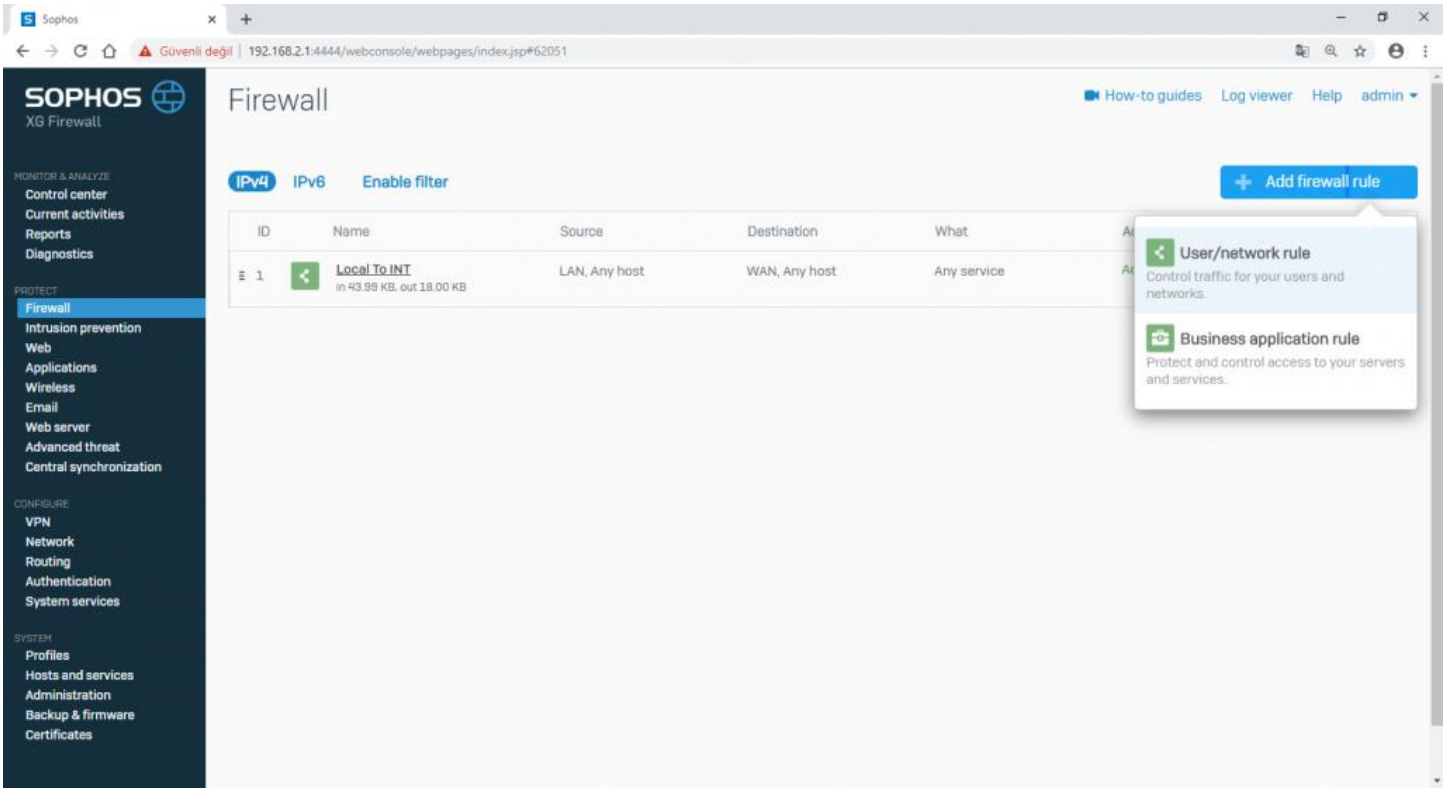
Yazdığımız kuralı internete natlamak için **"Rewrite source adress(masquerading)"** alanını işaretledikten sonra **"Use outbound address"** alanından default **MASQ'yu** ve **Primary ISP** devremizi seçiyoruz.

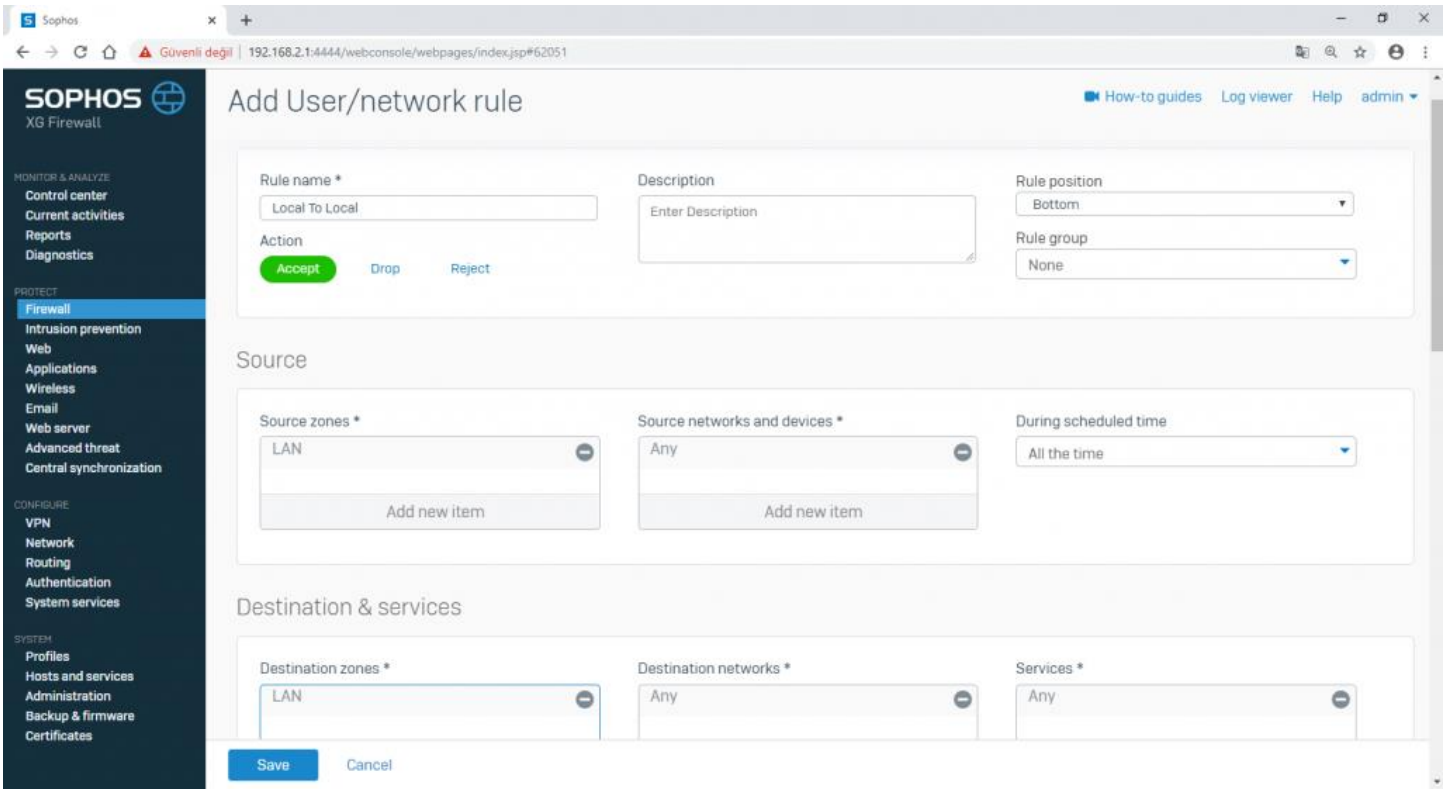
Kural üzerinden geçecek trafiği izlemek için loglamayı açmalıyız.

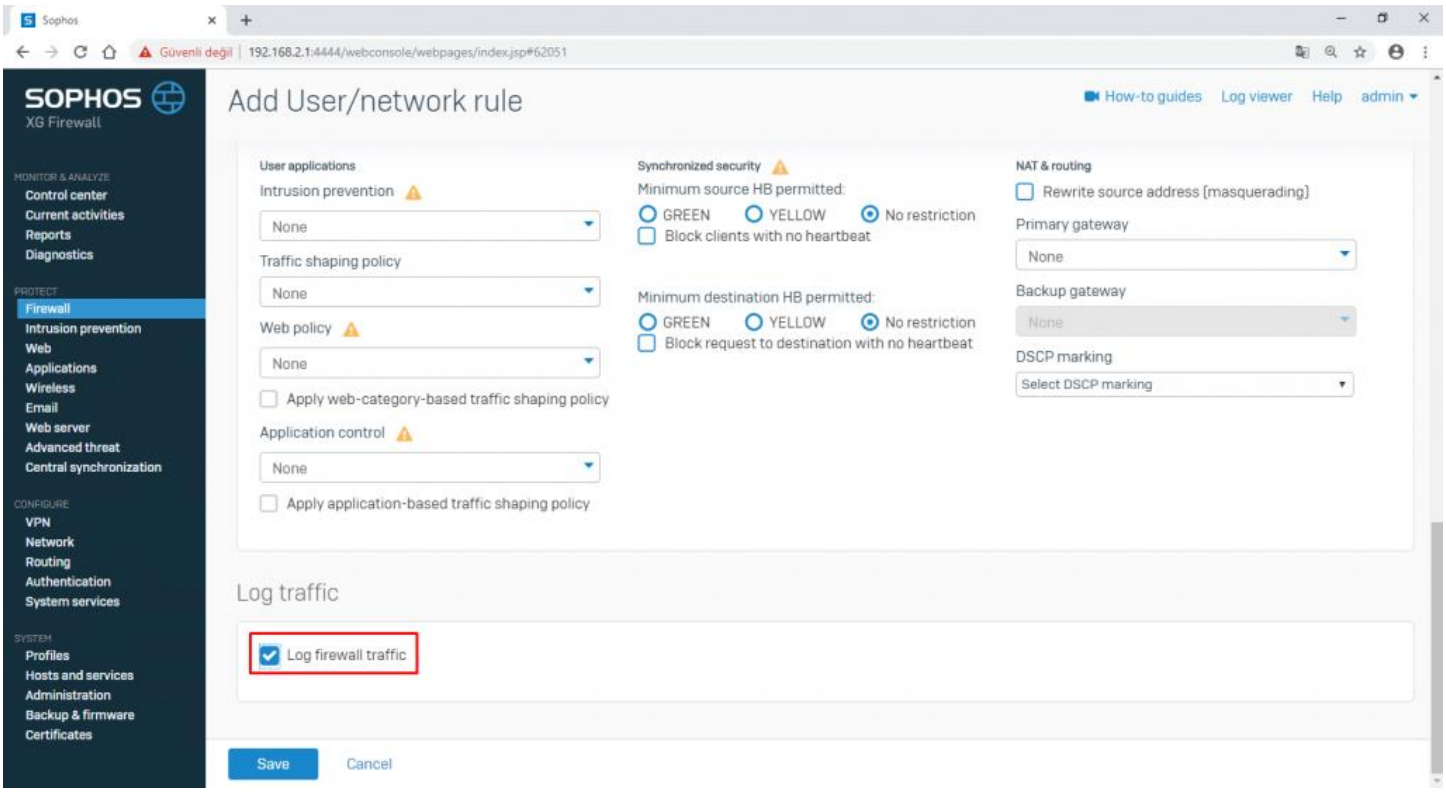


Local To Local erişim sağlamak için Lan Networkümüzden Lan Networkümüze doğru kural yazmalıyız

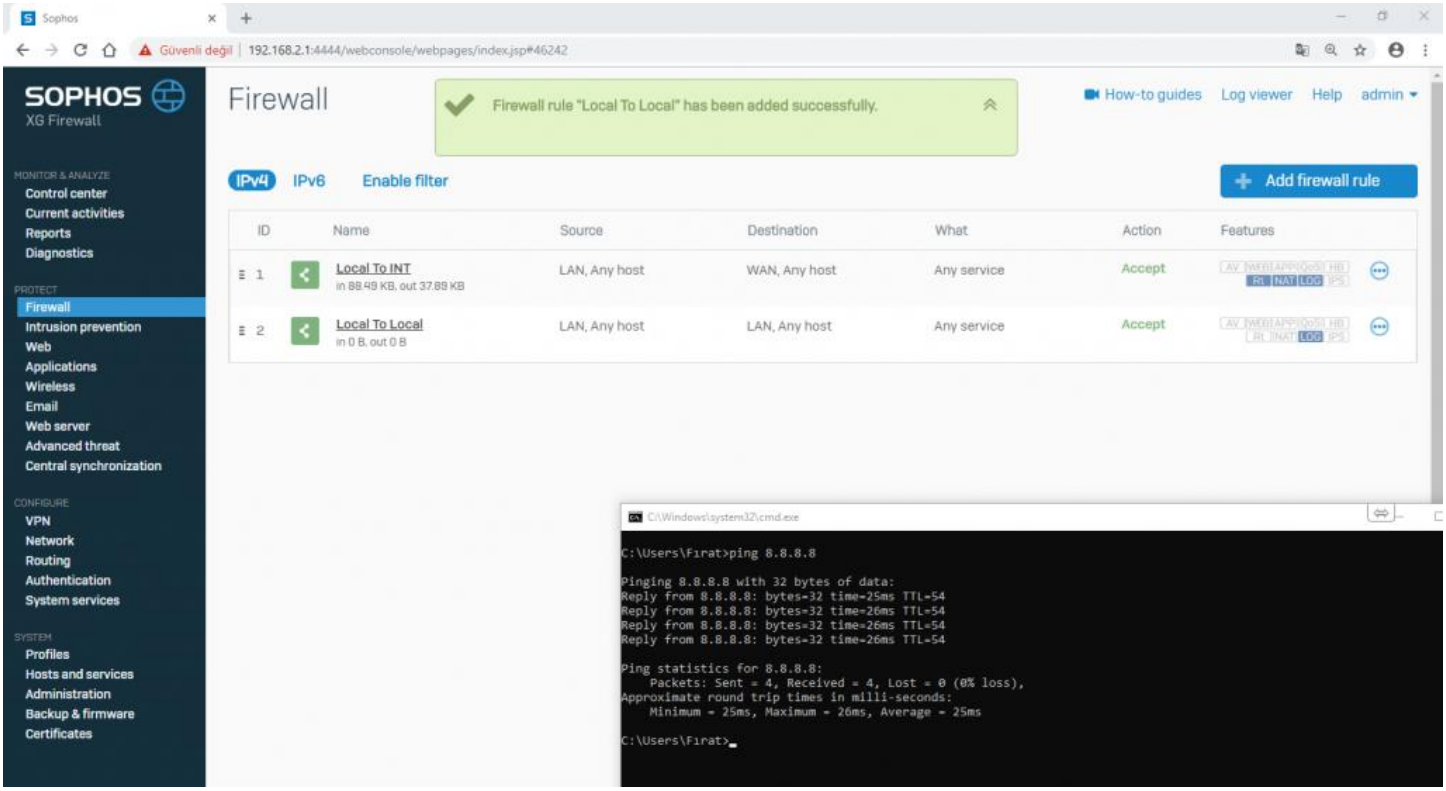
Yazacağımız kuralı **Sophos XG** Local bir kural olduğunu algılayıp Natlamayı otomatik kapatacaktır..




Sophos
Güvenli değil | 192.168.2.1:4444/webconsole/webpages/index.jsp#62051
SOPHOS
XG Firewall
Add User/network rule
How-to guides
Log viewer
Help
admin
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
Rule name *
Local To Local
Action
Accept
Drop
Reject
Description
Enter Description
Rule position
Bottom
Rule group
None
Source
Source zones *
LAN
Add new item
Source networks and devices *
Any
Add new item
During scheduled time
All the time
Destination & services
Destination zones *
LAN
Destination networks *
Any
Services *
Any
Save
Cancel


Sophos
Güvenli değil | 192.168.2.1:4444/webconsole/webpages/index.jsp#62051
SOPHOS
XG Firewall
Add User/network rule
How-to guides
Log viewer
Help
admin
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
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)
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.



Umarım sizler için faydalı bir paylaşım olmuştur.
Fırat Meray | Network and Information Security Specialist