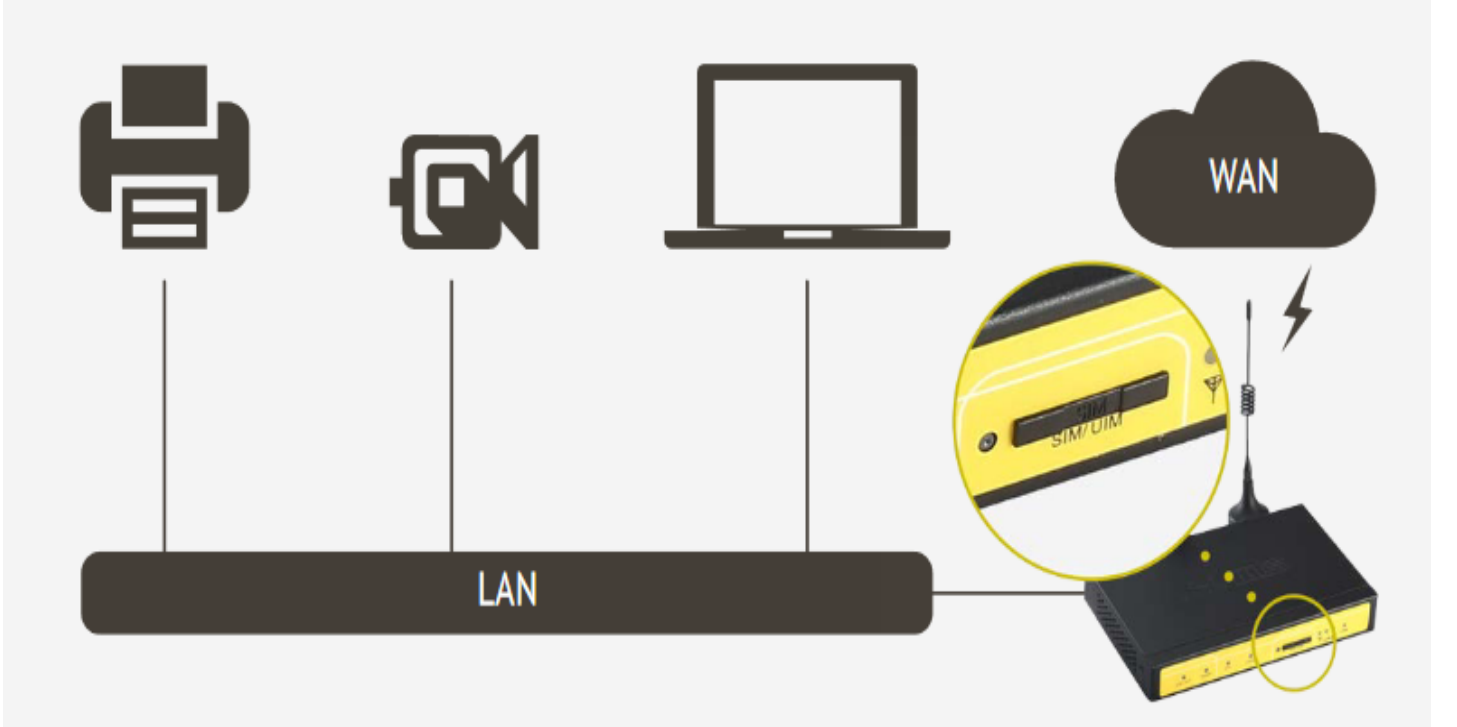


FF Routerlar İin Genel Pratik Kullanım Kılavuzu

1. İnternet Eriřimi

1.1 İlk Baęlantıları Nasıl Yapıyoruz?

1. Cihaz enerjisizken, ilk nce cihaza GSM kartını takıyoruz.
2. Daha sonra anten baęlantımızı yapıyoruz.
3. Cihaza enerji veriyoruz.

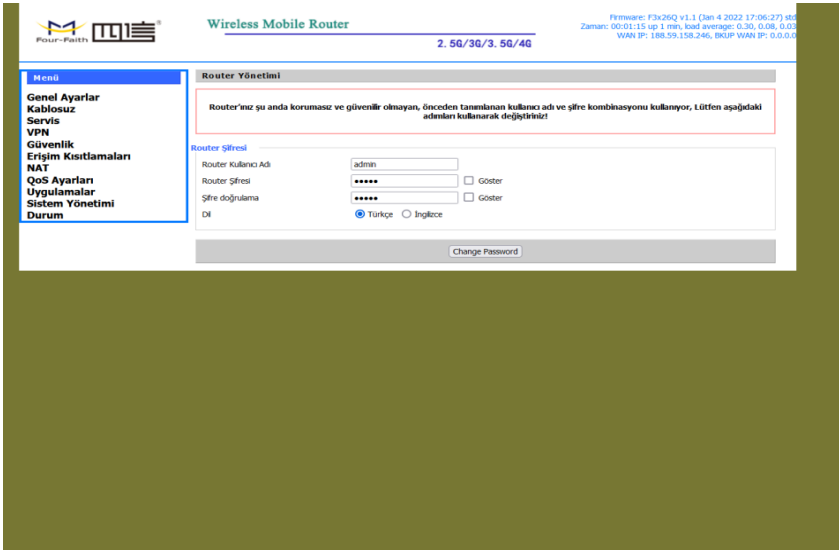


řekil 1. Baęlantı řeması

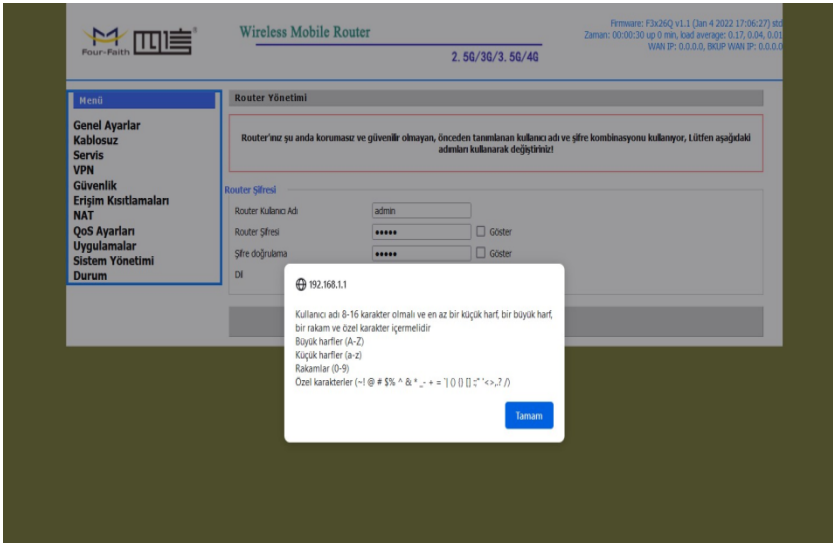
1.2 Cihaz Web Arayüzüne Nasıl Erişiyoruz?

1. Cihazın arkasındaki etiket kısmında yazan IP ile herhangi bir tarayıcı programından (IE Explorer, Google Chrome, Firefox vb.) arayüzüne giriyoruz.
2. 192.168.1.1 Lokal IP üzerinden erişim sağlıyoruz. (Şekil 2.1)
3. İlk kurulumda kullanıcı adı ve şifre belirlememiz gerekiyor. **Kullanıcı adı ve şifre aynı olamaz.** Şekil 2.2 de belirtilen kurallar çerçevesinde belirlenir.

NOT: Kullanıcı adı : admin Şifre: admin girişi kaldırıldı.



Şekil 2.1 Web Ara Yüzü



Şekil 2.2 Kullanıcı Adı ve Şifre Belirleme Kuralları

1.3 Temel Ayarları Nasıl Yapıyoruz?

1. Web arayüzünde “Genel Ayarlar” kısmına girerek “Sistem Ayarları” sekmesine tıklıyoruz. Bu kısım cihazımızla ilgili ana ayarları yapılandırdığımız yerdir (Router IP, DHCP, APN, PING, Saat, Tarih vb.).
2. Burada internet erişimini sağlayabilmek için kullandığınız GSM operatörüne göre APN kısmını uygun şekilde dolduruyoruz ve varsa Sim Kart PIN’ini giriyoruz.
3. İhtiyaç var ise LAN ve DHCP ayarlarını değiştiriyoruz. Daha sonra değiştirdiğimiz ayarların uygulanması için öncelikle sayfanın alt kısmında bulunan “Kaydet” butonuna daha sonra “Ayarları Uygula” butonuna basmamız gerekiyor. Bu işlemin ardından modem kendi kendini yeniden başlatacaktır (restart işlemi), yeniden işlemlerin yapılması için biraz beklenmelidir.

The screenshot displays the configuration interface for a Wireless Mobile Router. The page is titled "Wireless Mobile Router" and shows the "WAN Ayarları" (WAN Settings) section. The interface includes a menu on the left, a main configuration area, and a help section on the right. The main configuration area is divided into several sections: "Yedek Link Seçeneği", "Wan Nat", "Main WAN Bağlantı Tipi", "IPSEC Çevrimi Devam et", and "Özel Ayarlar". The "Main WAN Bağlantı Tipi" section is the primary focus, showing settings for the main WAN connection. The "Yardımlar" section on the right provides information about automatic configuration, host name, domain name, local IP address, and DHCP settings.

Wireless Mobile Router
Firmware: F3x26Q v1.1 (Jan 4 2022 17:06:27) st...
Zaman: 15:26:51 up 11 min, load average: 0.03, 0.04, 0.04
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

Menü
Genel Ayarlar
o Sistem Ayarları
o DDNS
o MAC Adres Kopyalama
o Gelişmiş Yönlendirme
o Ağ Oluşturma
Kablosuz
Servis
VPN
Güvenlik
Erişim Kısıtlamaları
NAT
QoS Ayarları
Uygulamalar
Sistem Yönetimi
Durum

WAN Ayarları
Yedek Link Seçeneği
Yedek Link Etkinleştir Devre Dışı bırak
Sinyal ile Değiştir Etkinleştir Devre Dışı bırak
Wan Nat
Wan Nat Etkinleştir Devre Dışı bırak
Main WAN Bağlantı Tipi
Bağlantı Tipi: dhcp 3G-4G
Kullanıcı Adı: ZTff@001
Şifre: ***** Göster
APN: mgbs
Sabit WAN IP: Etkinleştir Devre Dışı bırak
Bu Doğrulamalara İzin Ver: PAP CHAP
Bağlantı Tipi: AUTO LTEPREF(LTE->TDS->GSM->WCDMA->HDR->CDMA)
PIN: Göster
Bağlantı Sorgulama: Ping
Algılama Periyodu: 300 Sn
Terah Edilen Sunucu IP: 8 8 8 8
Diğer Sunucu IP: 8 8 4 4
Bağlantı Hataları Restart: Etkinleştir Devre Dışı bırak (Default: 10 dakika)
Fixed WAN Netmask Address: Etkinleştir Devre Dışı bırak
STP: Etkinleştir Devre Dışı bırak
IPSEC Çevrimi Devam et
Bağlantı Sorgulama: None
Özel Ayarlar
Router Adı: Four-Faith

Yardımlar
daha fazla...
Otomatik Konfigürasyon - DHCP:
Bu ayar genellikle ağ operatörleri tarafından kullanılmaktadır.
Host Adı:
ISP tarafından sağlanan Host adını giriniz.
Domain Adı:
ISP tarafından sağlanan Domain adını giriniz.
Yerel IP Adres:
Router adresi.
Alt Ağ Maskesi:
Router'in alt ağ maskesi.
DHCP Sunucusu:
Router'un ağdaki IP adreslerini yönetmesine olanak sağlar.
Başlangıç IP Adresi:
Bu IP Adresinden itibaren ağdaki cihazlara IP Adresleri dağıtılır.
Maksimum DHCP Kullanıcısı:
Router'ın dağıtmış olduğu adres sayısını sınırlayabilirsiniz. 0 (sıfır) sadece önceden tanımlanan statik adreslerin dağıtılacağı anlamına gelir.
Zaman Ayarı:
Bulunmuş olduğunuz zaman dilimini ve Yaz Saati Uygulama (YSU) dönemini seçiniz. Router yerel zamanı veya UTC zamanını kullanabilir.

Şekil 3. Genel Ayarlar (Sistem Ayarları)

APN AYARI

Vodafone Hatlar İin;

Eęer statik IP'li hat kullanıyorsanız **“internetstatik”**, kullanmıyorsanız **“internet”** giriyoruz.

Turkcell Hatlar İin;

Eęer statik IP'li hat kullanıyorsanız **“mgbs”**, kullanmıyorsanız **“mgb”** giriyoruz.

Türk Telekom Hatlar İin;

Eęer statik IP'li hat kullanıyorsanız **“statikip”**, kullanmıyorsanız **“internet”** giriyoruz.

1.4 Baęlantının Kontrolünü Nasıl Yapıyoruz?

1. Doğru baęlantı ile modem üzerindeki online ışığının sürekli yandığını göreceksiniz.
2. "Online" ışığının sürekli yandığını gördükten sonra sol alt kısımdaki "Durum" menüsüne girerek "WAN" seçeneğini tıklıyoruz ve baęlantı ayarlarının durumunu inceliyoruz.

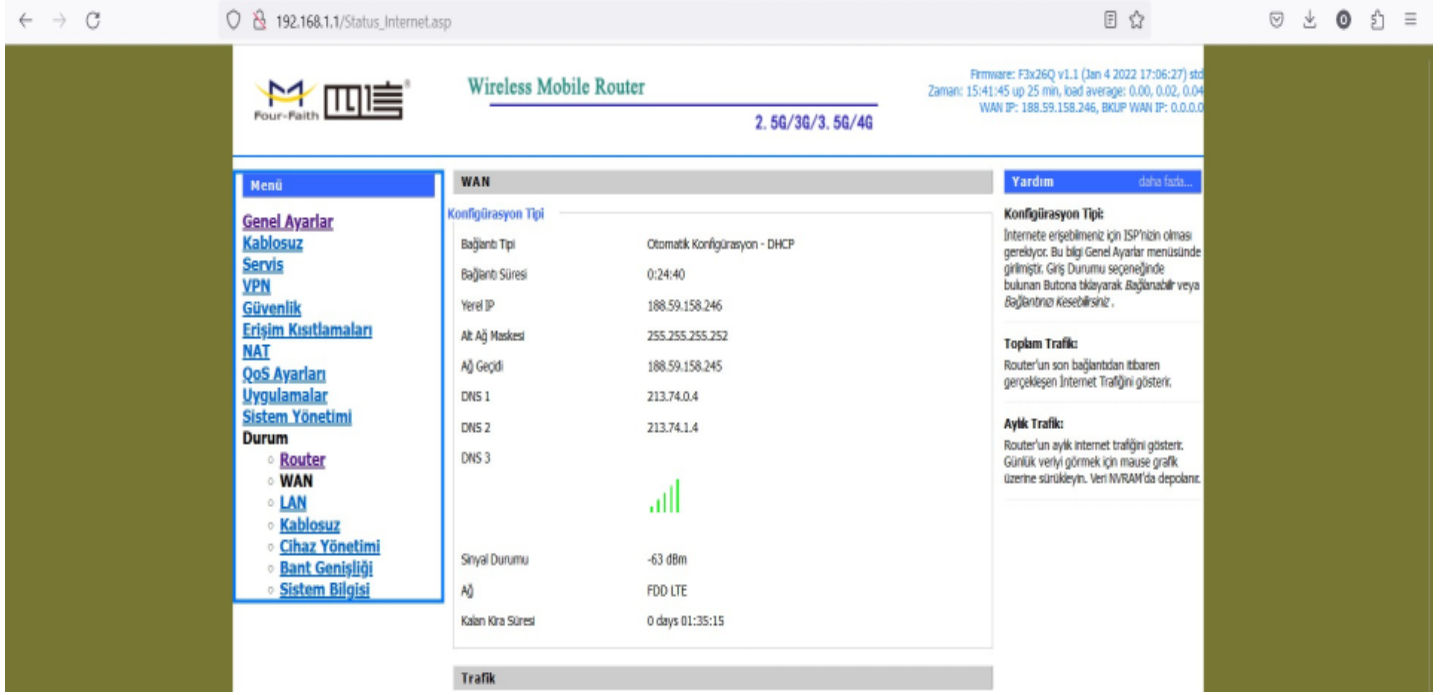


Şekil 4. "Online" Işıęı

"Baęlantı Tipi" kısmı baęlantının olup - olmadığını gösterir.

"Sinyal Durumu" sinyal seviyesinin gösterir. -(55 ila -90 dBm arasındaki deęerler idealdir).

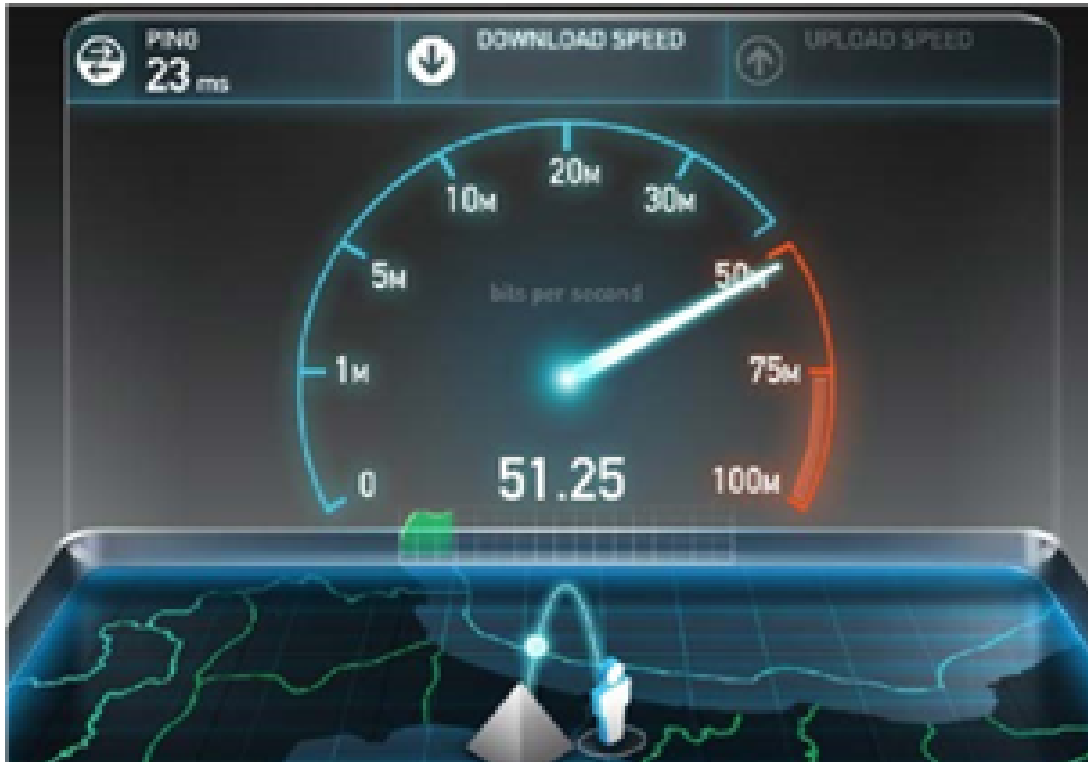
"Yerel IP" kısmında GSM kartımızın IP'sini görebiliriz.



Şekil 5. Durum- WAN

1.5 Hız Testini Nasıl Yapıyoruz?

"www.speedtest.net" ya da tercih edeceğimiz diğer hız testi sitelerinden herhangi biri ile internetimizin indirme ve yükleme hızını kontrol edebilirsiniz.,



Şekil 6. Hız Testi

1.6 Hata Esnasında Ne Yapıyoruz?

SIM kart takılı mı?

Özellikle mini SIM kartların modül ile takılması durumunda temas sorunu yaşanabilir. Kontrol edilmelidir.

SIM ve Anten takıldıktan sonra mı enerji verildi?

Bazen modem enerjili iken SIM kart takılabilmektedir, SIM kart mutlaka modem **enerji verilmeden** takılmalıdır.

SIM'in aktif olduğu GSM operatörü aranarak teyit edildi mi?

SIM kart sinyal göstermesine rağmen APN'ye (özellikle statik IP'li APN'ye) tanımlı olmalıdır. Teyit edilmesi gerekmektedir.

Bulduğunuz bölgede kullandığınız GSM çekiyor mu?

Sinyal seviyesi “-55 dBm ila -90 dBm” arasında mı? Bu aralık dışındaki durumlarda 2G'ye düşme ya da internete hiç erişememe durumları olabiliyor. Anten takılı ise modemin farklı bir lokasyonda denenmesi gerekir.

Anten takılı mı? Anten doğru yere takılı mı?

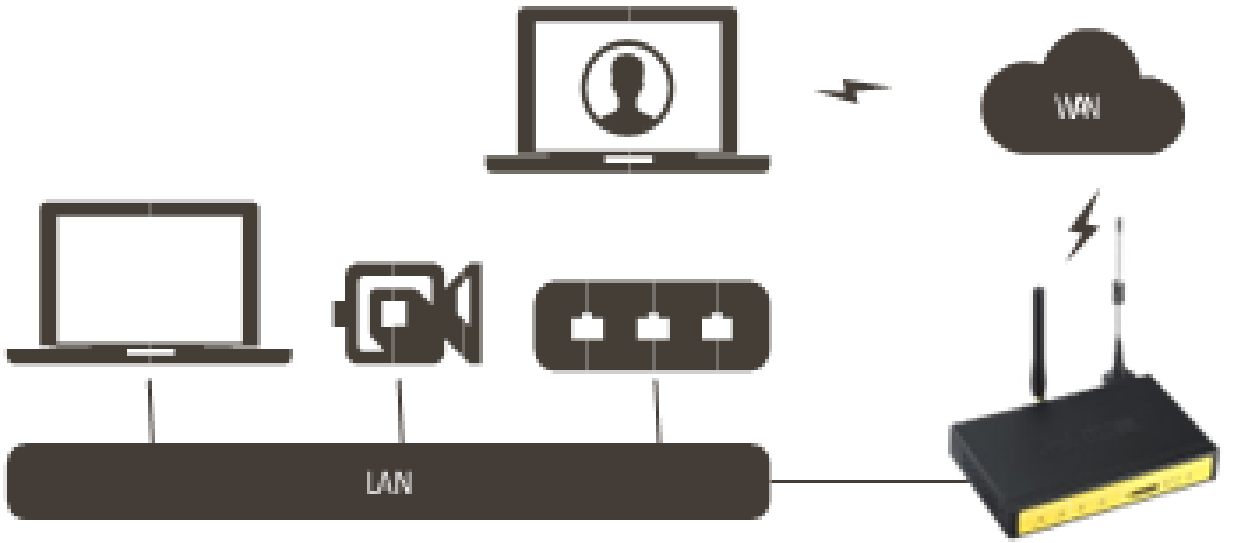
“Antenna” kısmına GSM anteni takılır. Ayrıca anten kablosu gerilim hattının olduğu kablo kanallarına konmamalıdır, çekimi etkiler.

2. Port Yönlendirme Uygulaması

2.1 Port Yönlendirmesi İçin Ne Gerekliyor ?

- Router cihazın arkasındaki kamera, PLC vb. endüstriyel cihazlara uzaktan erişimi sağlamak için Port Yönlendirmenin yapılması gerekmektedir.
- Bu işlemlere başlamadan önce cihazımızın İnternet Erişiminin olması gerekmektedir. İnternet erişimi için “FF_İnternet ErişimKılavuzu” kılavuzundan yararlanabilirsiniz.
- Ayrıca port yönlendirmenin çalışabilmesi için SIM kartınızın Sabit (statik) IP özelliği olması gerekmektedir. Değişken IP’li hatlar ile IP’nizi geçici olarak kontrol ederek yapılacak denemeler dahi başarısız olacaktır.

ŞEKİL 1.
BAĞLANTI
ŞEMASI



2.2 Cihaz Web Arayüzüne Nasıl Erişiyoruz?

- Cihazın arkasındaki etiket kısmında yazan IP ile herhangi bir tarayıcı programından (IE Explorer, Google Chrome, Firefox vb.) arayüzüne giriyoruz.
- Cihaza kombinasyonlu kullanıcı adı ve şifre belirleniyor. Bu bilgilerin girilmesi ile ara yüze ulaşıyoruz.

192.168.1.1

The screenshot displays the web interface of a Wireless Mobile Router. The top header includes the Four-Faith logo, the product name 'Wireless Mobile Router', and the model '2. 5G/3G/3. 5G/4G'. The firmware version is 'F3x26Q v1.1 (Sep 15 2023 12:36:09) std'. The system status shows 'Zaman: 00:01:50 up 1 min, load average: 0.08, 0.03, 0.01' and 'WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0'. The left sidebar contains a menu with options: Genel Ayarlar, Kablosuz, Servis, VPN, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar, Sistem Yönetimi, and Durum. The main content area is titled 'Router Yönetimi' and features a warning message: 'Router'ınız şu anda korumasız ve güvenilir olmayan, önceden tanımlanan kullanıcı adı ve şifre kombinasyonu kullanıyor, Lütfen aşağıdaki adımları kullanarak değiştiriniz!'. Below the warning, the 'Router Şifresi' section allows users to change the password. The 'Router Kullanıcı Adı' field is set to 'admin'. The 'Router Şifresi' and 'Şifre doğrulama' fields are masked with asterisks. There are 'Göster' checkboxes for both password fields. The 'Dil' section has radio buttons for 'Türkçe' (selected) and 'İngilizce'. A 'Change Password' button is located at the bottom of the form.

Şekil 2. Web Ara Yüzü

2.3 Cihazın Port Yönlendirmesini Nasıl Yapıyoruz?

Port yönlendirmeyi 3 farklı seçenek ile yapabiliriz:

Port Yönlendirme: Tek bir portu yönlendirmek için kullanılır.

Port Aralık Yönlendirme: Belirli bir port aralığını yönlendirmek için kullanılır.

DMZ: Tüm portları belirli bir IP'ye yönlendirmek için kullanılır.

“**Port Yönlendirme**” işlemi için “NAT” menüsü altında “Port Yönlendirme” seçeneğine tıklıyoruz ve yönlendirmek istediğimiz cihazın özelliklerini giriyoruz. Bunun için şu adımları takip etmeliyiz:

1. İlk önce “Ekle” diyoruz.
2. Daha sonra Application (uygulamanın ismi), Source Net (filtreleme için kullanılır; tek IP yada tek bir Ağ'ın erişimi isteniyorsa bu kısma yazılarak filtreleme gerçekleşir, boş bırakıldığı takdirde bütün cihazlar erişim sağlayabilir. Örnek olarak (5.229.207.0/24 yazdığımız takdirde sadece 5.229.207.0 ağında bulunan PC'lerin erişimine olanak sağlar), Port From (dışarıdan (external) sorgulanacak port), IP Address (cihazın IP'si; PLC, kamera vb.) ve Port To (iç taraftaki (internal) yönlendirilecek port, cihazın portu) bilgilerini tek tek yazıyoruz.
3. “Enable” yapıyoruz.

The screenshot shows the 'Port Yönlendirme' (Port Forwarding) configuration page in the router's web interface. The page is titled 'Wireless Mobile Router' and shows the current status as '2.5G/3G/3.5G/4G'. The main configuration area contains a table for port forwarding rules:

Sil	Num	Uygulama	Protokol	Kaynak	Harcı Port	Yerel IP	Dahil Port	Etkinleştir
<input type="checkbox"/>	1	TEST	Hepsi		5001	192.168.1.106	5001	<input checked="" type="checkbox"/>

Below the table are buttons for 'Kaydet', 'Ayarları Uygula', and 'Değişiklikleri İptal Et'. The right side of the page has a 'Yardım' (Help) section with a 'Kestime' (Summary) section stating 'En fazla 100 kayıt eklenebilir.' and a 'Port Yönlendirme:' section with detailed instructions in Turkish.

Şekil 3. Port Yönlendirme

“Port Aralık Yönlendirme”de ise bir aralık belirterek, o aralıktaki bütün portlara erişim sağlanır (start port-end port).

(Genel olarak daha basit arayüzü nedeni ile tercih edilebilir).

1. İlk olarak “Ekle” butonuna tıklayarak yönlendirme için yeni bir satır açıyoruz.
2. Daha sonra yerel ağımızdaki hedef cihazımızın IP adresini giriyoruz.

Four-Faith  Wireless Mobile Router

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std
Zaman: 13:09:30 up 1:07, load average: 0.04, 0.05, 0.05
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

Menü

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
 - Port Yönlendirme
 - Port Aralık Yönlendirme**
 - DMZ
 - Sanal IP Eşleme
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Port Aralık Yönlendirme

Yönlendirme

Sil	Num	Uygulama	Başlangıç	Bitiş	Protokol	Yerel IP	Etkinleştir
<input type="checkbox"/>	1	TEST	5000	5005	Hepsi	192.168.1.10f	<input checked="" type="checkbox"/>

Ekle

Kaydet Ayarları Uygula Değişiklikleri İptal Et

Yardım daha fazla...

Kısıtlama
En fazla 60 kayıt eklenebilir.

Port Aralık Yönlendirme:
Bazı uygulamaların doğru bir şekilde çalışması için özel portların açılması gerekir. Bu uygulamalara sunucular ve bazı online oyunlar örnek gösterilebilir. İnternette belli bir porta istek geldiğinde, Router veriyi belirlediğiniz cihaza yönlendirecektir. Olabilecek Güvenlik sorunlarından dolayı, port yönlendirmeyi kullandığınız portlarla sınırlamak daha güvenli olacaktır. Port yönlendirme işlemiyle işiniz bittikten sonra onay kutusundaki Etkinleştir işaretini kaldırınız.

Şekil 4. Port Aralık Yönlendirme

“DMZ” kısmında ise belirlediğimiz bir IP adresinin bütün portlarına uzaktan erişim sağlanır.

1. Bu bölüm diğer uygulamalara kıyasla biraz daha geneldir. Öncelikle DMZ’yi “Enable” yapıyoruz.
2. Yönlendireceğimiz cihazın IP adresini giriyoruz. Böylelikle bu IP adresinde olan bütün portlara uzaktan erişimi açıyoruz.

Wireless Mobile Router

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std
Zaman: 13:16:19 up 1:13, load average: 0.01, 0.04, 0.04
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

Menü

Genel Ayarlar
Kablosuz
Servis
VPN
Güvenlik
Erişim Kısıtlamaları
NAT
o Port Yönlendirme
o Port Aralık
o Yönlendirme
o DMZ
o Sanal IP Eşleme
QoS Ayarları
Uygulamalar
Sistem Yönetimi
Durum

Demilitarized Zone (DMZ)

DMZ

DMZ Kullan Etkinleştir Devre Dışı bırak

DMZ Host IP Adresi 192.168.1.108

Kaydet Ayarları Uygula Değişiklikleri İptal Et

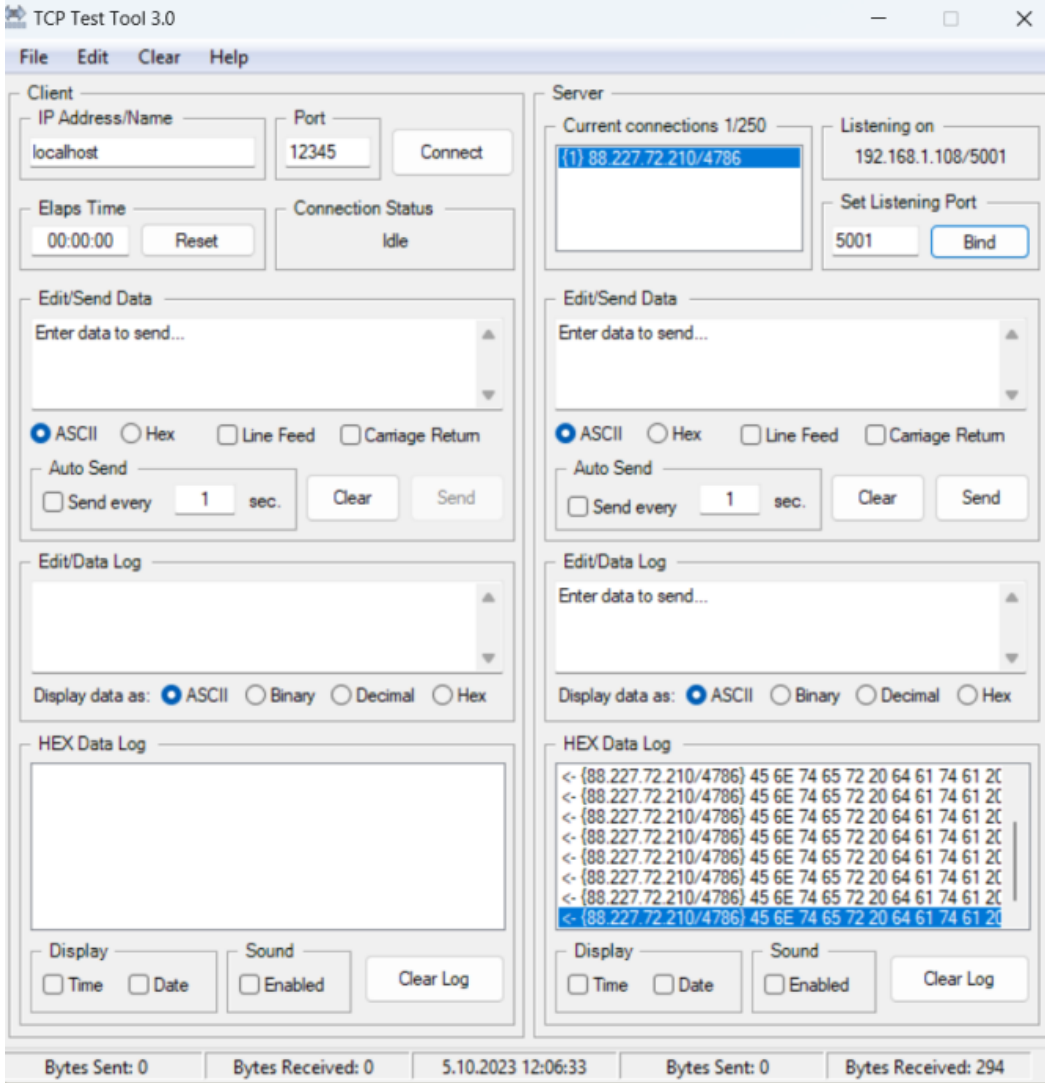
Yardım daha fazla...

DMZ:
Bu seçeneğin etkinleştirilmesi halinde belirtilen IP adresini internete çıkartacaktır. Bütün portlar internetten erişilebilir olacaktır.

Şekil 5.DMZ

2.4 Baęlantının Kontrolünü Nasıl Yapıyoruz?

1. İşlemlerin doğruluęunu test etmek için "Tera Term" yada TCP Test Tool "(bunlar sadece önerilen, isterseniz "cmd" komut sayfasından telnet seçeneęi ile de test edebilirsiniz) gibi terminal programlarını kullanarak test edebiliriz.
2. Terminal programına modemimizin SIM karttan aldığı IP'yi girdikten sonra açtığımız portu da giriyoruz. Connect/Baęlan komutundansonra baęlantının açılması ile port yönlendirmenin başarılı olduğunu teyit ediyoruz.



Şekil 6. Başarılı Port Yönlendirme Örneęi

NOT: Eğer Router cihaza uzaktan ping atmak isteniyorsa “Güvenlik” menüsüne girerek “WAN İsteklerini Engelleme” sekmesinden “WAN'dan Gelen İstekleri Engelle (ping)” kutucuğunu şekilde görüldüğü gibi devre dışı bırakmak gerekmektedir.

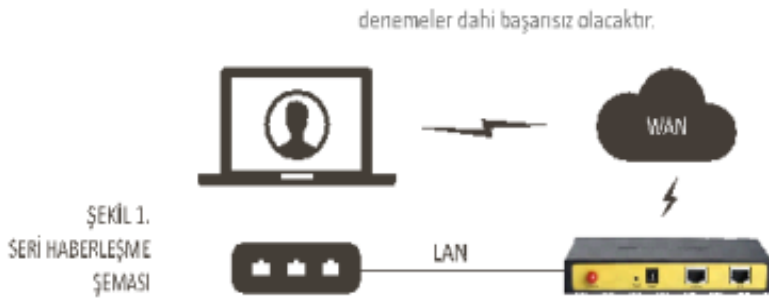
The screenshot displays the configuration page for a Wireless Mobile Router. The interface is in Turkish. The main menu on the left includes 'Genel Ayarlar', 'Kablosuz Servis', 'VPN', 'Güvenlik', 'Erişim Kısıtlamaları', 'NAT', 'QoS Ayarları', 'Uygulamalar', 'Sistem Yönetimi', and 'Durum'. The 'Güvenlik' menu item is highlighted. The 'Güvenlik' section is active, showing 'Güvenlik Duvarı Koruması' with 'SPI Güvenlik Duvarı' set to 'Etkinleştir'. Below this, the 'Ek Filtreler' section includes 'Proxy Filtrele', 'Çerezleri Filtrele', 'Java Uygulamalarını Filtrele', and 'ActiveX Filtrele'. The 'WAN İsteklerini Engelleme' section is highlighted, showing 'WAN'dan Gelen İstekleri Engelle (Ping)' is unchecked, 'IDENT (Port 113) Filtrele' is checked, and 'WAN SNMP Erişimini Engelle' is checked. The 'WAN DoS/Bruteforce Engelleme' section includes 'SSH Erişimini Sınırla', 'Telnet Erişimini Sınırla', 'PPTP Sunucu Erişimini Sınırla', and 'L2TP Sunucu Erişimini Sınırla'. The 'Log Yönetimi' section shows 'Log' is set to 'Devre Dışı bırak'. At the bottom, there are buttons for 'Kaydet', 'Ayarları Uygula', and 'Değişiklikleri İptal Et'. The top right corner shows the firmware version 'F3x26Q v1.1 (Sep 15 2023 12:36:09) str', the time 'Zaman: 13:44:24 up 1:42, load average: 0.01, 0.04, 0.0', and the WAN IP 'WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.1'.

Şekil 7. Ping Engelleme

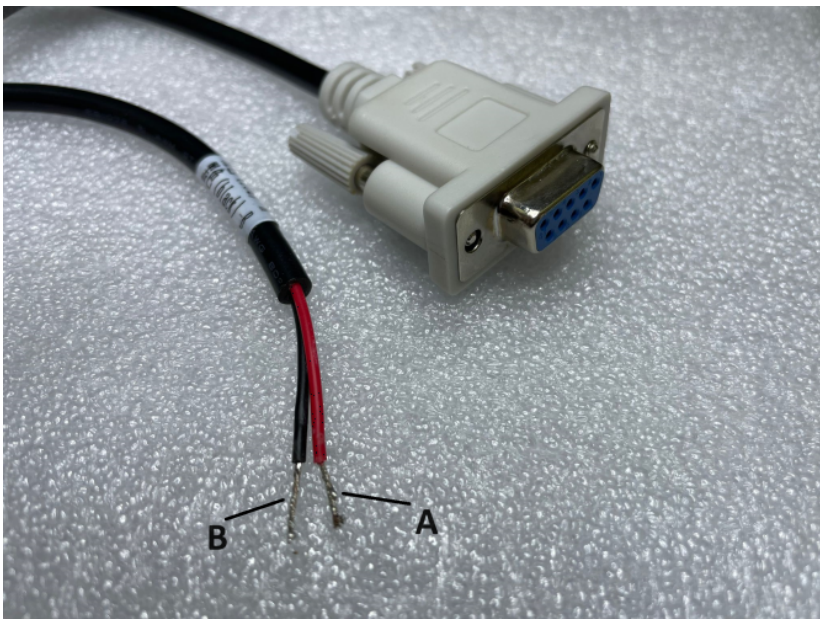
3. Seri Haberleşme

3.1 İlk Bağlantıları Nasıl Yapıyoruz ?

1. Çoğu otomasyon uygulaması Seri-Ethenernet haberleşme dönüşümünü gerektirmektedir. Bu sebepten dolayı Four-Faith marka Router'larda "Console" adı altında seri çıkışlar bulunmaktadır. Bu kısımdan hem RS232 hem de RS485 bağlantısı desteklenmektedir.
2. Bu işlemlere başlamadan önce cihazımızın İnternet Erişiminin olması gerekmektedir. İnternet erişimi için "FF_İnternet Erişim Kılavuzu" kılavuzundan yararlanabilirsiniz.
3. Ayrıca seri haberleşmenin çalışabilmesi için SIM kartınızın Sabit (statik) IP özelliği olması gerekmektedir. Değişken IP'li hatlar ile IP'nizi geçici olarak kontrol ederek yapılacak denemeler dahi başarısız olacaktır.
4. Modem ile birlikte RS232 ve RS485 kabloları teslim edilir. Dilersek şemaya göre biz de ilgili kabloyu yapabiliriz



RS485 (iki Tel DB9 Uç) Kablo



RS485 (iki Tel RJ45 Uç) Kablo



RS485 ve RS232 (RJ45 ve DB9 Uç) Kablo



3.2 Cihaz Web Arayüzüne Nasıl Erişiyoruz?

1. Cihazın arkasındaki etiket kısmında yazan IP ile herhangi bir tarayıcı programından (IE Explorer, Google Chrome,Firefox vb.) arayüzüne giriyoruz.
2. Cihaza kullanıcı adı ve şifre belirliyoruz. Bu bilgilerin girilmesi ile ara yüze ulaşıyoruz.

The screenshot displays the web management interface of a Four-Faith Wireless Mobile Router. The browser's address bar shows the URL '192.168.1.1/apply.cgi'. The page title is 'Wireless Mobile Router' and the status bar indicates '2.56/30/3.56/40'. The interface is organized into several sections:

- Sistem Bilgisi (System Information):**
 - Router:** Router Adı: Four-Faith, Router Modeli: Four-Faith Router, LAN MAC: 54:00:85:36:19:65, WAN MAC: 54:00:85:36:19:68, Kablolu MAC: 54:00:85:36:19:68, WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0, LAN IP: 192.168.1.1
 - Kablolu (Wired):** Radyo: Radyo Kapalı, Mod: Erişim Noktası(AP), Ağ: Devre Dışı, SSSD: Four-Faith, Kanal: 0 (2407 MHz), TX Gücü: Devre Dışı, Rate: Devre Dışı
 - Kablolu Paket Bilgisi (Wired Packet Information):** Alınan (RX): 0 OK, Hayır Hata; Gönderilen (TX): 0 OK, Hayır Hata
- Servis (Services):**
 - DHCP Sunucusu (DHCP Server):** ETKİN, radauth: Devre Dışı, ETKİN
 - Nasılca (Usage):** Kullanılabilir Toplam: 121.7 MB / 128.0 MB, Boy: 94.2 MB / 121.7 MB, Kullanılan: 27.5 MB / 121.7 MB, Arabellek: 3.9 MB / 27.5 MB, Önbellek: 11.7 MB / 27.5 MB, Aktif: 5.0 MB / 27.5 MB, Aktif Olmayan: 12.4 MB / 27.5 MB
- DHCP İstisnalar (DHCP Exclusions):**

İstisna Adı	Yazıl IP	MAC Adresi	İstisna Erişim Süresi
OF	192.168.1.108	xxxxxx:xxxx:99:C1	1 day 00:00:00

Şekil 3. Web Ara Yüzü

3.3 Seri Ayarları Nasıl Yapıyoruz?

1. “Uygulamalar” menüsü içerisinde “Seri Haberleşme” seçeneğine tıklayarak seri ayar ekranına giriyoruz. İlk önce bu özelliği aktifleştirmek için “Etkinleştir” seçeneğine tıklıyoruz
2. Çıkan ekranda ilgili seri haberleşme parametrelerini (parity, baudrate, stopbit vb.) doğru bir şekilde giriyoruz. Bu kısımdaki ayarlar modeme bağlayacağınız cihaz ile aynı olmalıdır.
3. «Protocol» kısmında ise çalışma şeklimizi belirliyoruz. Cihazı Modbus Gateway (Modbus TCP -> Modbus RTU dönüşümü için) olarak kullanacaksak “MODBUS TCP” seçeneğini, Transparan Gateway olarak kullanacaksak “TCP SERVER” seçeneğini tercih ediyoruz.
4. “Listen Port” kısmında TCP erişimimizde kullanacağımız portu istediğimiz şekilde giriyoruz ve Daha sonra “Kaydet” ve “Ayarları Uygula” tıklayarak kaydediyoruz.

The screenshot displays the configuration page for a Wireless Mobile Router. The page is titled "Wireless Mobile Router" and shows the status "2. 5G/3G/3. 5G/4G". The firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) str". The system time is "Zaman: 00:05:09 up 5 min, load average: 0.17, 0.10, 0.02" and the WAN IP is "WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0".

The left sidebar contains a menu with the following items: Genel Ayarlar, Kablosuz, Servis, VPN, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar (highlighted), Seri Haberleşme (highlighted), To Master, To RTU, Sayısal operasyon, SMS Ayarları, Sistem Yönetimi, and Durum.

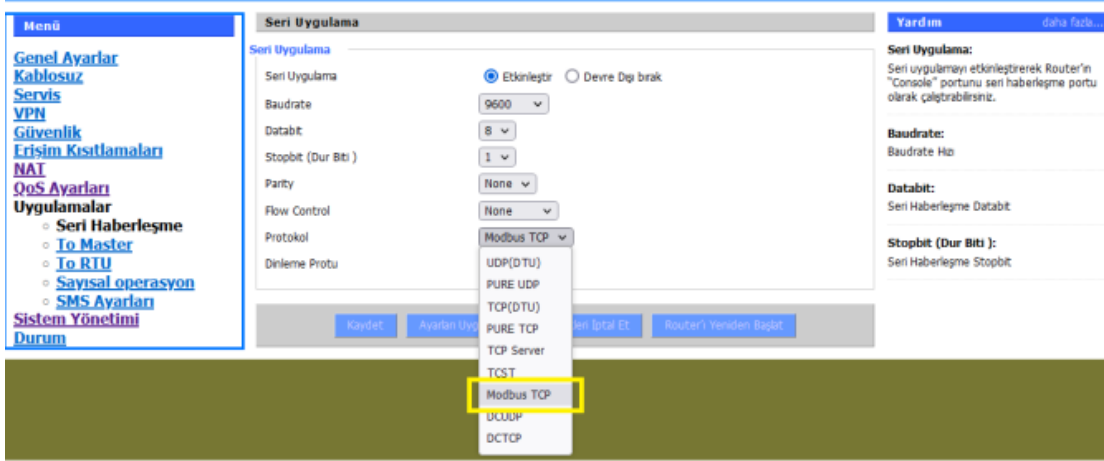
The main content area is titled "Seri Uygulama" and contains the following settings:

- Seri Uygulama: Etkinleştir Devre Dışı bırak
- Buttons: Kaydet, Ayarları Uygula, Değişikliği İptal Et, Router'i Yenisinden Başlat

The right sidebar contains the following settings:

- Yardım: daha fazla...
- Seri Uygulama: Seri uygulamayı etkinleştirerek Router'in "Console" portunu seri haberleşme portu olarak çalıştırabilirsiniz.
- Baudrate: Baudrate Hızı
- Databit: Seri Haberleşme Databit
- Stopbit (Dur Biti): Seri Haberleşme Stopbit

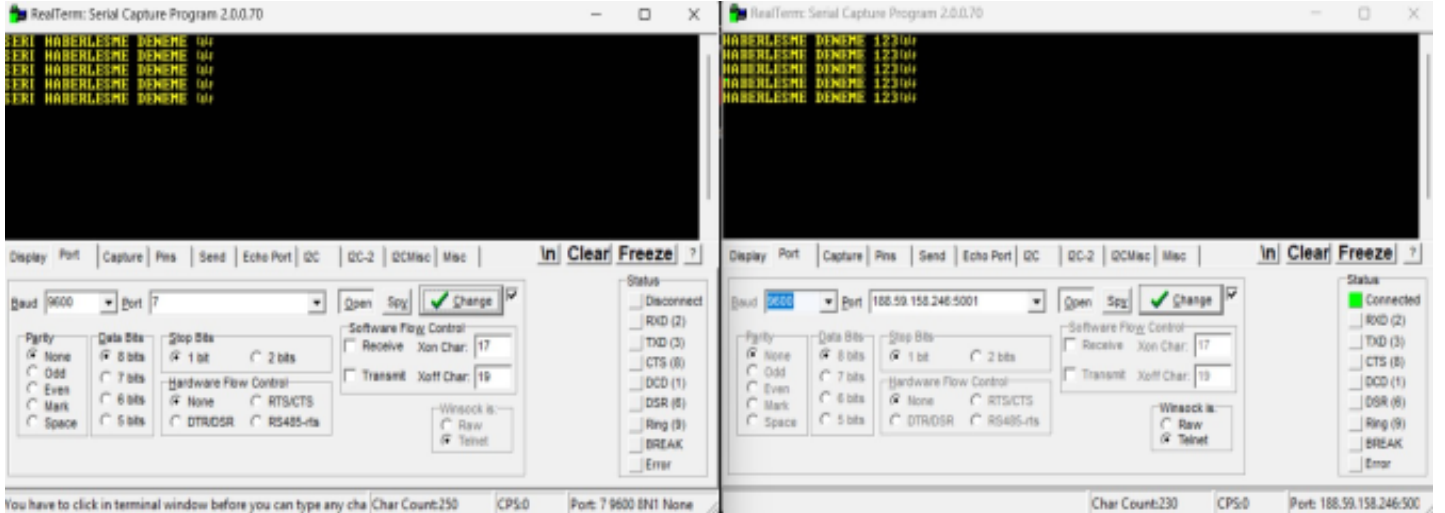
Şekil 4. Seri Haberleşme



Şekil 5. Seri Ayarlar ve Protokol Seçimi

3.4 Bağlantının Kontrolünü Nasıl Yapıyoruz?

1. Cihaz ile haberleşme için gerekli yazılım üzerinden modemimizin sabit IP'sini ve ayarladığımız TCP portunu giriyoruz ve haberleşmeyi gerçekleştiriyoruz.



Şekil 6. Seri Haberleşme Örneği

3.5 Hata Esnasında Ne Yapıyoruz?

Seri haberleşme parametreleri doğru girildi mi?

“Seri Uygulama” altında bulunan parity, stopbit, baudrate gibi parametrelerin doğruluğu kontrol edilmelidir.

Kablo bağlantınız doğru mu?

Kutu içerisinden çıkan kabloları kullanınız ve daha sonradan yapılan kabloların ilgili şemalara uygun olduğundan emin olunuz.

Modemin Seri haberleşme Protokolü doğru seçildi mi?

Modemi Modbus Gateway (Modbus TCP->Modbus RTU dönüşümü için) olarak kullanacaksak “MODBUS TCP”, Transparan Gateway olarak kullanacaksak “TCP SERVER” olarak seçmemiz gerekmektedir.

Modem internete erişiyor mu?

İnternet erişimi için “FF_İnternet Erişim Kılavuzu” kılavuzundan yararlanabilirsiniz.

Seri haberleşilecek cihaz açık mı?

Yerel ağda kullandığımız cihazın açık olduğunu ve modemimize bağlandığı kontrol edilmelidir.

Seri haberleşme kablosu doğru bir şekilde takıldı mı?

Modemin arkasında bulunan RJ45 çıkışları “LAN”, (opsiyonel “WAN”) ve “CONSOLE” çıkışlarıdır. Seri bağlantımızı “CONSOLE” çıkışına bağlamamız gerekmektedir.

4. Haberleşme Sürekliliğini Sağlanması ve Bağlantı Kopmalarının Engellenmesi için Uygulamalar

4.1 Haberleşme Uygulamalarında Stabilite'nin Önemi

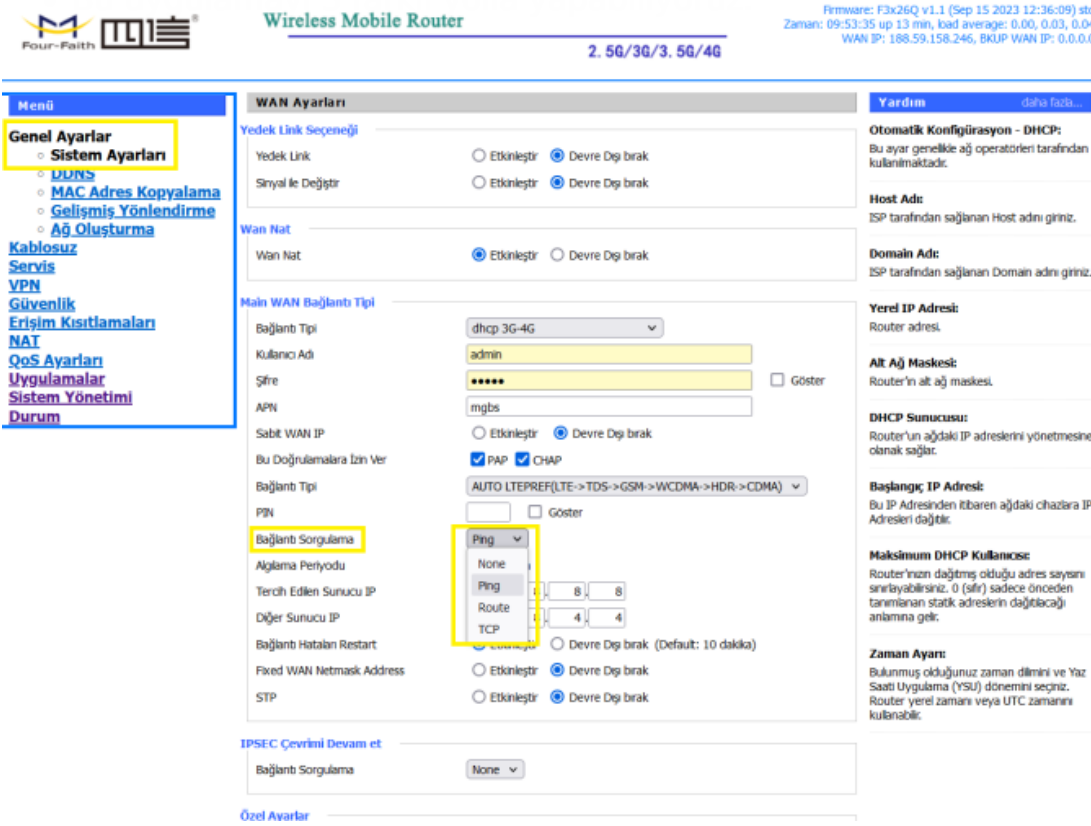
- 2M (Makineden Makineye Haberleşme) haberleşme sistemlerinde her zaman haberleşmenin kesintisiz olması istenir. Bundan dolayı haberleşme stabilitesini artırıcı uygulamalara başvurmak zorundayız.
- Haberleşme stabilitesini artırıcı uygulamalar yazılımsal ya da donanımsal olarak yapılabilmektedir.
- Four-Faith marka modemler haberleşme stabilitesini arttırma amacı ile üç farklı uygulamayı destekler:

1. **Bağlantı Sorgulama**
2. **Canlı Tutma**
3. **SMS**

4.2 Modemin Haberleşmesini Nasıl Kesintisiz Hale Getiriyoruz

Bağlantı Sorgulama:

- Bu uygulama ile cihazımızın internet erişimini farklı yollar ile belirli periyotlarda sorgulayarak bağlantının olup olmadığını algılamasını sağlıyoruz.



The screenshot displays the configuration page for a Wireless Mobile Router. The main heading is 'WAN Ayarları' (WAN Settings). The 'Bağlantı Sorgulama' (Link Check) section is highlighted with a yellow box. It includes a dropdown menu for 'Bağlantı Sorgulama' with options: 'None', 'Ping', 'Route', and 'TCP'. The 'Ping' option is selected. Below this, there are input fields for 'Ağlama Periyodu' (Polling Period) set to 8 and 'Tercih Edilen Sunucu IP' (Preferred Server IP) set to 8. There are also input fields for 'Diğer Sunucu IP' (Other Server IP) set to 4 and 4. The 'Bağlantı Hatahan Restart' (Link Error Restart) section has radio buttons for 'Etkinleştir' (Enable) and 'Devre Dışı bırak' (Disable), with 'Devre Dışı bırak' selected. The 'Fixed WAN Netmask Address' and 'STP' sections also have radio buttons for 'Etkinleştir' and 'Devre Dışı bırak', with 'Devre Dışı bırak' selected. The 'IPSEC Çevrimi Devam et' (IPSEC Loop Continue) section has a dropdown menu for 'Bağlantı Sorgulama' set to 'None'. The 'Özel Avarlar' (Special Alerts) section is empty. The right sidebar contains 'Yardım' (Help) and 'Otomatik Konfigürasyon - DHCP' (Automatic Configuration - DHCP) sections. The top of the page shows the router's status: '2. 5G/3G/3. 5G/4G' and 'Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std'. The bottom of the page shows the 'Genel Ayarlar' (General Settings) menu with 'Sistem Ayarları' (System Settings) highlighted.

Şekil 1. Bağlantı Sorgulama

Ping : Ping ile cihazımız belirli bir periyot aralığında(saniye cinsinden), belirlediğimiz IP'lere (Primary Detection Server IP ve backup Detection Server IP) ping atarak modem internet erişiminin olup olmadığını ("online" ya da "offline") teşhis eder. Eğer cihaz "offline" ise ISS'yi (Internet Servis Sağlayıcısına) tekrar arayarak bağlantıyı kurmaya çalışır. (Primary ve Backup IP'ler için önerilen adresler Google 'a ait olan ya da her zaman açık olan: 8.8.8.8, 8.8.4.4, 4.2.2.1, 4.2.2.2 vb. adresleridir).

Route ve PPP seçenekleri data teknik özellikleri içerir ancak kullanımı tercih edilmemektedir.

The screenshot shows the router's configuration interface for the Main WAN connection. The 'Bağlantı Sorulma' (Connection Test) section is highlighted with a yellow box. It is set to 'Ping' with a '300 S'n' (300 seconds) interval. The 'Tercih Edilen Sunucu IP' (Preferred Server IP) is set to '8.8.8.8' and the 'Diğer Sunucu IP' (Other Server IP) is set to '8.8.4.4'. Other settings include 'Bağlantı Tipi' (Connection Type) set to 'dhcp 3G-4G', 'Kullanıcı Adı' (Username) as 'admin', and 'Şifre' (Password) as '*****'. The 'Bağlantı Hataları Restart' (Restart on Connection Errors) is set to 'Etkinleştir' (Enabled).

Şekil 2. Ping

Yapacağımız değişiklikleri ilk önce kaydedip daha sonra uygulamamız gerekir. Sayfanın alt kısmında bulunan "Kaydet" butonuna tıkladıktan sonra "Ayarları Uygula" kısmına tıklayarak uygulamayı kaydediyoruz.

NOT: Önerilen uygulama "PING" ile internet erişimi tespitidir. İnternet erişimi kontrolünde "PING" atılmayan bir IP girilmemesi çok önemlidir. Aksi takdirde cihaz internet bağlantısı yok varsayarak sürekli yeniden bağlanmaya çalışır.

Canlı Tutma:

- Bu uygulama ise modem uzun süreli veri alışverişi olmadan beklemesi sonucu oluşabilecek kilitlemeleri önlemek için belirli zaman aralıklarında (saniye cinsinden) modemi yeniden başlatarak (“restart”) cihazın şebekeye yeniden bağlanmasını sağlamaktadır.
- Baz istasyonlarının 5-6 dakika veri transferi yapmayan istemcileri şebekeden attığı gerçeği göz önüne alındığında haberleşme stabilitesi açısından önemli bir uygulamadır.
- Canlı Tutma uygulamasına “Sistem Yönetimi” menüsü altında “Canlı Tutma” seçeneğine tıklayarak ayarlayabiliyoruz.
- İlk önce “Zamanlanmış Restart” kısmını “Etkinleştir” yapıyoruz.

Şekil 3. Canlı Tutma

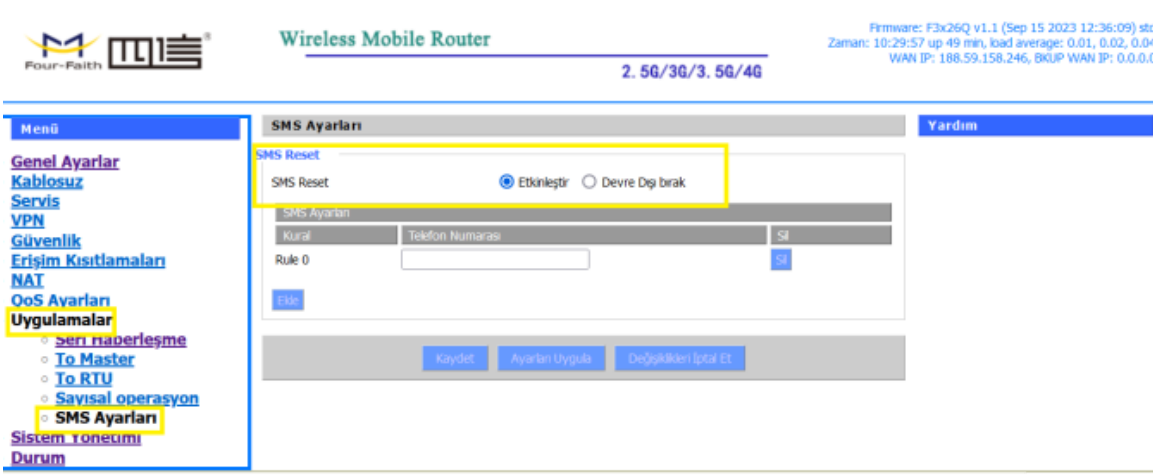
Burada karşımıza iki seçenek çıkıyor:

- Belirli periyot ile: Yani modemimiz belirlenen bir periyotta kendi kendini yeniden başlatır.
- Belirli günün belirli saatinde: Bu seçenekte ise cihazımız belirlenen bir gün/günler de ve belirlenen saat geldiğinde periyotta cihaz kendini yeniden başlatır.

İlgili ayarları girdikten sonra **“Kaydet”** butonuna ve ardından **“Ayarları Uygula”** butonuna tıklayarak uygulamaya alıyoruz.

4.3 Sms İle Restart

- Bu uygulama ile cihazımıza uzaktan “restart” edebiliyoruz. Bu şekilde cihazın WEB arayüzüne ya da cihazın yanına gitmemize gerek kalmadan uzaktan “restart” işlemi gerçekleştirebiliyoruz.
- “Uygulamalar” menüsü altında “SMS Ayarı” seçeneğini “Etkinleştir” yapmamız yeterlidir (“Ekle” diyerek bir numara girmemize gerek kalmadan herhangi bir cep telefonu ile bu uygulamayı gerçekleştirebiliriz).
- Daha sonra cep telefonumuzdan modeme taktığımız hattın numarasına “reset” yazan kısa mesaj yolluyoruz ve modem bu mesajı alır almaz kendi kendine “restart” ediyor.



Şekil 4. SMS İle Restart

NOT: “RESTART” etme için yazacağımız SMS sadece “reset” kelimesini içermelidir. Aksi takdirde çalışmaz.



Şekil 4.1 SMS İle Restart

5. Wireless (Kablosuz) Erişimi

Four Faith marka router modemlerde kablosuz haberleşmenin tercih edildiği projelerde kullanılmak üzere WIFI kablosuz ağ özelliği mevcuttur. Kablosuz Ağ özelliği farklı modlarda çalışarak farklı ihtiyaçlara cevap verebilir. 802.11 b/g/n standartlarını desteklemenin yanı sıra 43 farklı çalışma modunu da desteklemektedir:

AP (Access Point)

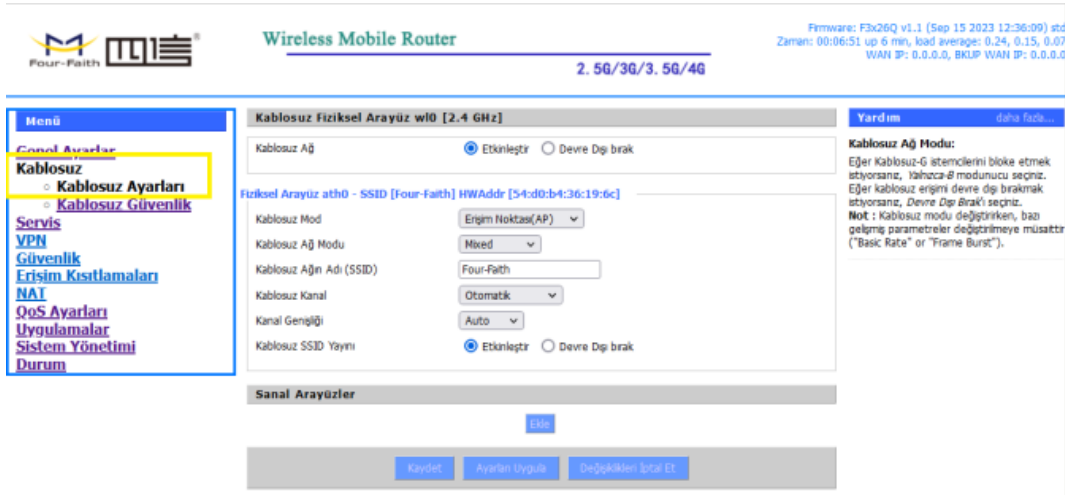
Client (İstemci)

Repeater (Tekrarlayıcı)



5.1 Wireless Ayarlarını Nasıl Yapıyoruz?

Cihazımızın web ara yüzünde “Kablosuz” menüsünün altında “Kablosuz Ayarları” sekmesini tıklıyoruz , “Kablosuz Ağ” seçeneğini “Etkinleştir” yapıyoruz.



Şekil 2. Kablosuz Ayarları

Kablosuz Mod: Çalışma modlarını içerir. Uygulamaya göre seçilmelidir.

Kablosuz Ağ Modu: Uygulamaya göre b/g/n standartlarını ayarlanabilmektedir.

Kablosuz Ağın Adı (SSID): Kablosuz ağın ismi.

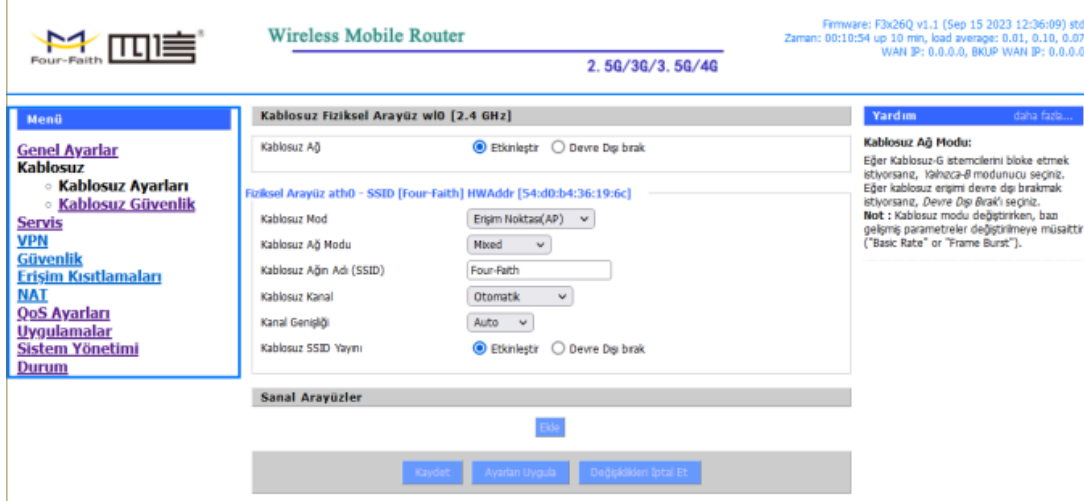
Kablosuz Kanal: Kablosuz ağın kanalı.

Kanal Geniřliđi: Kablosuz yayın yaptığımız kanalın frekansı.

AP (Access Point):

AP çalışma modu 3G / 4G ya da Backup_WAN portundan aldığı interneti WIFI ile dağıtmasını sağlamaktadır. Aşağıdaki adımları takip ederek AP modunu aktif edip kullanabiliriz:

Aşağıdaki şekilde gösterildiđi gibi Wireless Mode “AP” seçilir diđer bütün ayarlar uygulamamıza göre düzenlenerek önce “Kaydet” butonuna, daha sonra “Ayarları Uygula” butonuna tıklayarak ayarlarımızı uyguluyoruz.



Şekil 3. Wireless Ayarları (AP)

“Kablosuz” menüsü altında “Kablosuz Güvenlik” sekmesine tıklıyoruz. Şekil: 4 ‘deki ekran açılıyor. Bilgilerimizi aşağıdaki gibi giriyoruz:

Güvenlik Modu: Uygulamadaki diđer cihazlarında desteklediđi güvenlik modunu seçiyoruz (tavsiye edilen WPA2 Personal).

WPA Algoritması: Uygulamamıza göre her hangi birini seçebiliriz.

WPA Şifresi: Şifremizi giriyoruz (en az 8 karakter olmalıdır).

“Kaydet” butonuna tıklayıp kaydediyoruz ve “Ayarları Uygula” diyerek uyguluyoruz. Böylelikle kablosuz ağımıza biz istemediğimiz sürece dışarıdan bir erişim olmayacaktır.

Menü

- Genel Ayarlar
- Kablosuz
 - Kablosuz Ayarları
 - Kablosuz Güvenlik
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Kablosuz Güvenlik wif0

Fiziksel Arayüz ath0 SSID [Four-Faith] HWAddr [54:d0:b4:36:19:6c]

Güvenlik Modu: WPA2 Personal

WPA Algoritması: AES

WPA Şifresi: [Göster]

Key Yenileme Periyodu (Sn): 3600 (Default: 3600, Aralık: 1 - 99999)

Kaydet Ayarları Uygula

Yardım

Güvenlik Modu:

Devre Değ, WEP, WPA Personal, WPA Enterprise, veya RADIUS'dan seçebilirsiniz. Ağınızda bütün cihazlar aynı güvenlik modunu kullanmalı. N-Mode ile WPA2/AES kullanmazsınız

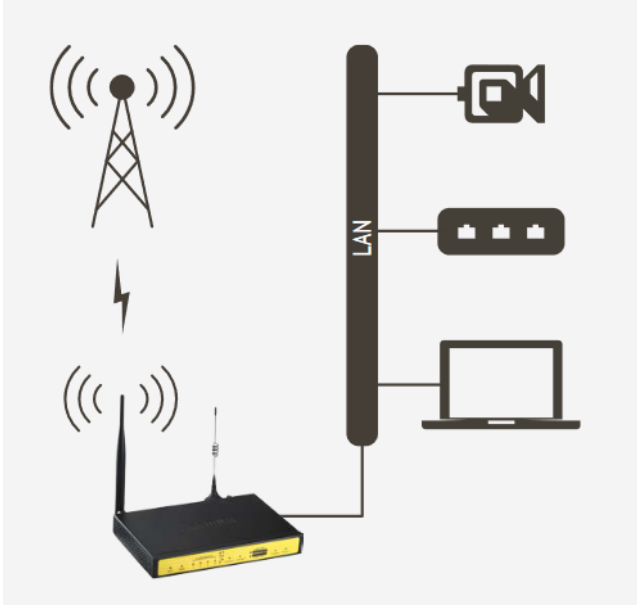
Şekil 4. Kablosuz Güvenlik (AP)

Client (İstemci):

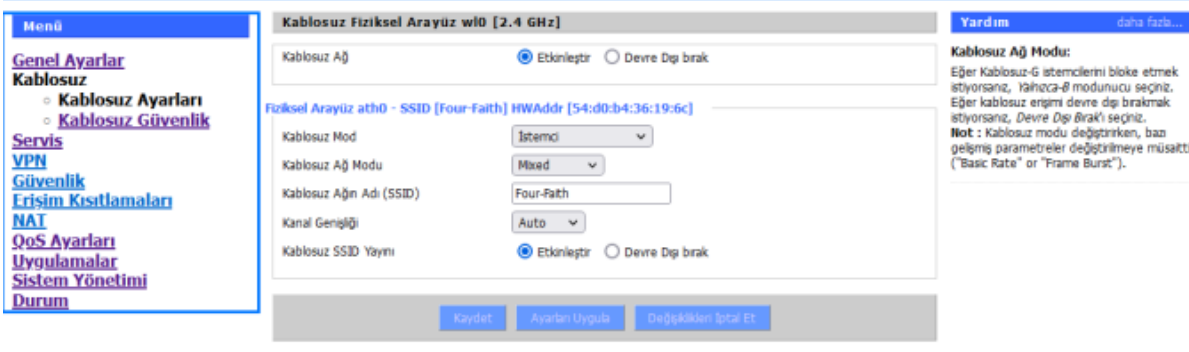
Client çalışma modu router modemden WIFI portundan aldığı (yerelde bulunan AP'e(Erişim Noktası)) bağlanarak interneti ETH kablosu üzerinden dağıtmasını sağlamaktadır.

Aşağıdaki adımları takip ederek Client modunu aktif edip kullanabiliriz:

Aşağıdaki şekilde gösterildiği gibi Kablosuz Mod **"İstemci"** seçilir diğer bütün ayarlar bağlanacağımız AP'e göre düzenlenerek önce **"Kaydet"** butonuna, daha sonra **"Ayarları Uygula"** butonuna tıklayarak ayarlarımızı uyguluyoruz.

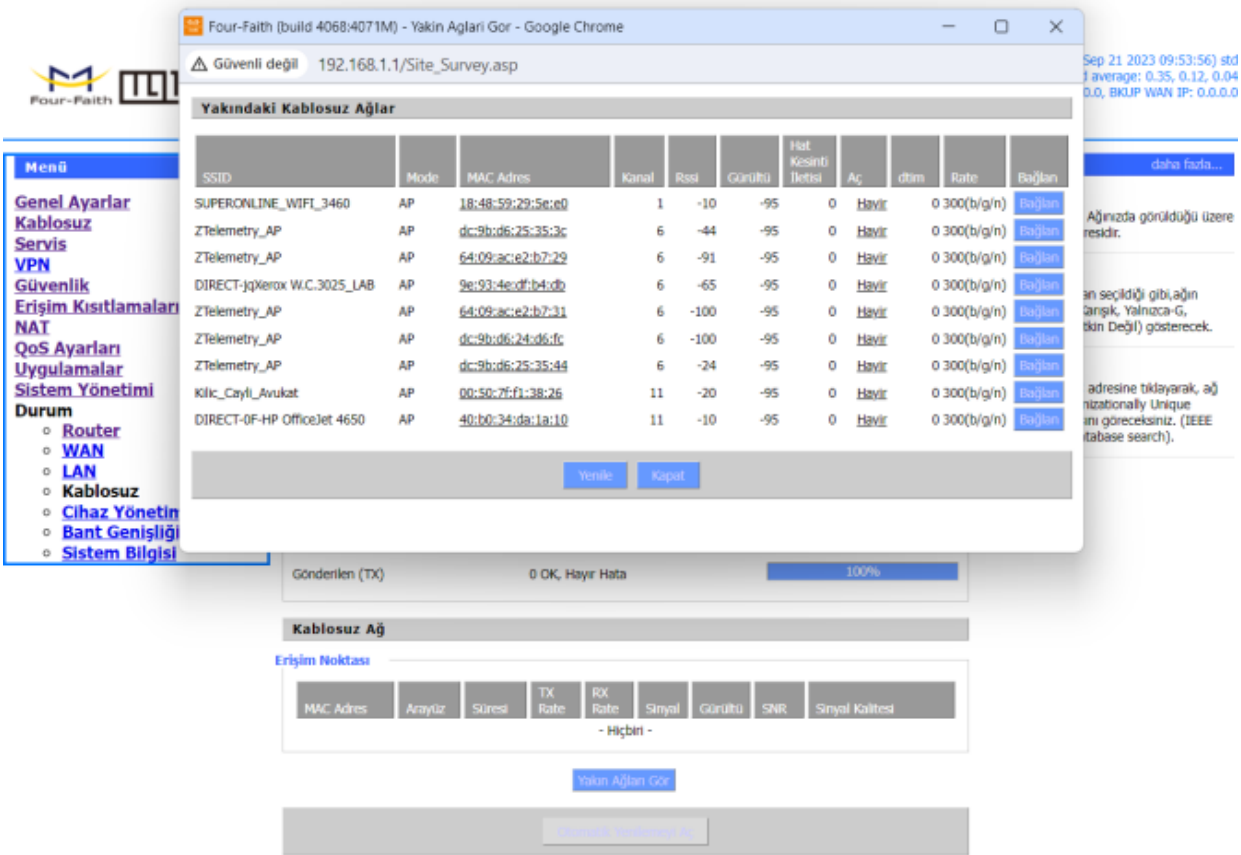


Şekil 5. Client (İstemci) Modu



řekil 6. Kablosuz Ayarları (Client)

5.2 Wireless Eriřimi Kontrolü



řekil 7. Kablosuz Ayarlarına Eriřim

Uygulanacak Adımlar

1. Kablosuz'u etkinleřtirdikten sonra "Durum" sekmesini açıyoruz.
2. Durum sekmesinden "Kablosuz" sekmesini açıyoruz.

6. Firmware Upgrade ve Konfigürasyon Yedekleme

6.1 Firmware Upgrade Nasıl Yapıyoruz?

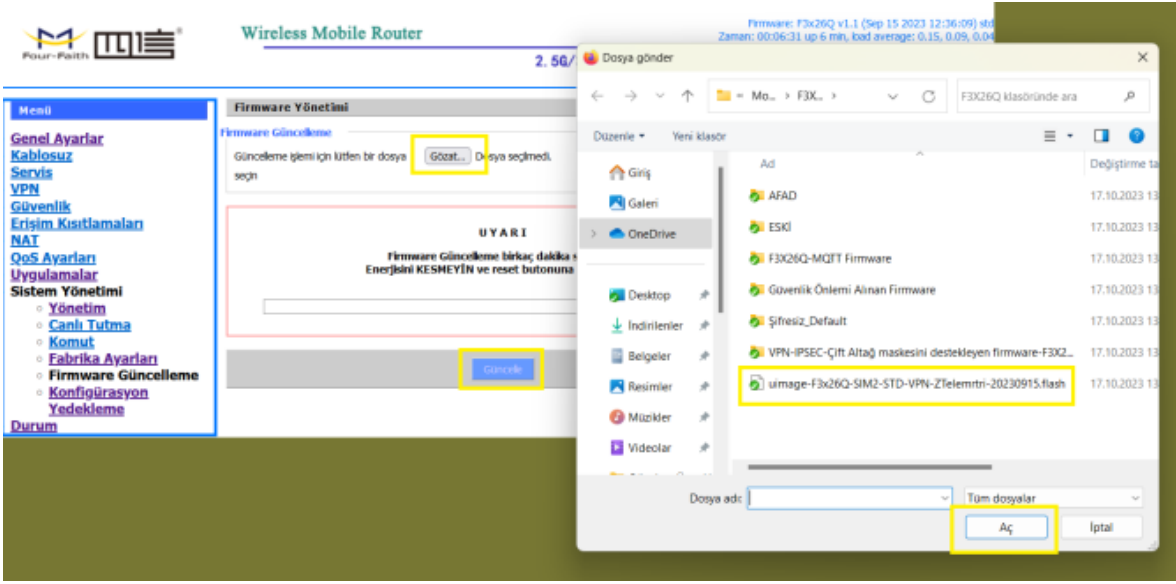
Bu uygulama ile modemlerin içinde çalışan yazılımın güncellemesini yapabiliyoruz. Bunun için “Sistem Yönetimi” menüsü altında “Firmware Güncelleme” seçeneğine tıklıyoruz.



Şekil 1. Firmware Güncelleme

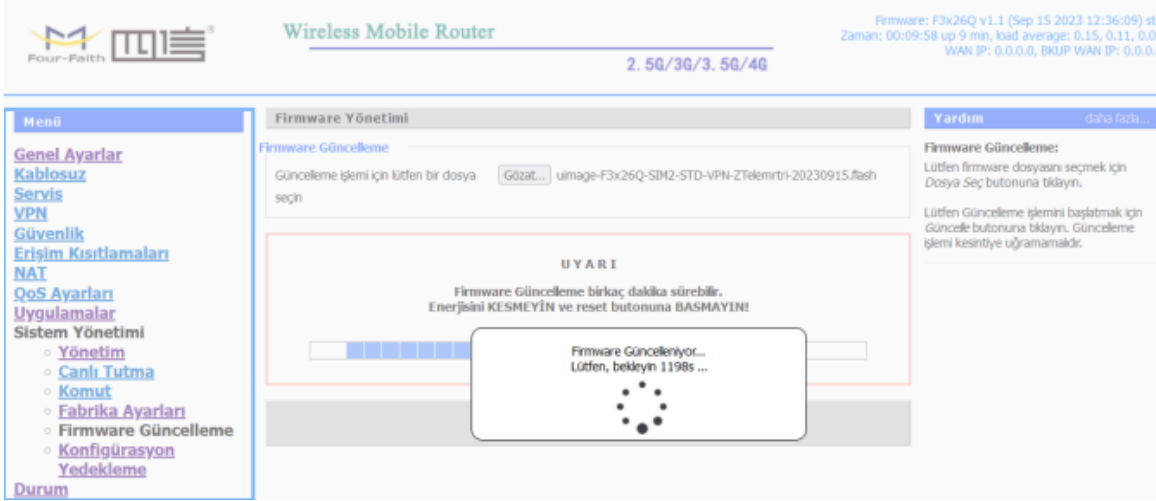
Karşımıza çıkan sayfada “**Dosya Seç**” ‘i tıkladıktan sonra sadece ve sadece firmamızın sağladığı dosyayı seçip “**Güncelle**” düğmesine tıklayarak yüklemeyi tamamlıyoruz.

NOT: Bu işlem sadece firmamızca onaylandıktan sonra firmamızın sağlayacağı dosya ile yapılmalıdır. Aksi takdirde modemizin garanti kapsamı dışında kalır.



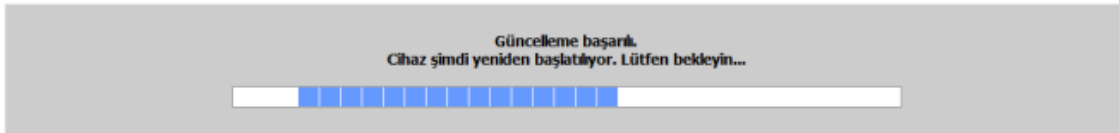
Şekil 2. Firmware Upgrade Dosya Seçimi

“Güncelleme” esnasında öncelikle dosyanın modeme aktarımı gerçekleştirilecektir.



Şekil 3. Firmware Upgrade Süreci

“Güncelleme Başarılı” yazısı ile güncelleme tamamlanmış anlamına gelir. Başarılı bir işlemin ardından cihaz yeniden başlatacaktır.



Şekil 4. Firmware Upgrade İşleminin Sonlandırılması

6.2 Konfigürasyon Yedeklemeyi Nasıl Alıyoruz?

1. Bu uygulama ile yüklü olan konfigürasyon ayarlarını yedeklememiz (“Yedekle”) mümkün oluyor. “Sistem Yönetimi” menüsü altında “Konfigürasyon Yedekle” seçeneğini tıklıyoruz ve ilgili sayfada “Yedekle” düğmense basmamız ile cihaz konfigürasyonu bilgisayarınıza indiriliyor (“.bin” formatında)..
2. Yedeklenen konfigürasyonlar aynı menü altında “Yükle” düğmesi ile aynı seri modemlere yüklenebiliyor.

The screenshot displays the configuration page for a Wireless Mobile Router. The page is titled "Konfigürasyon Yedekleme" (Configuration Backup) and includes a sidebar menu on the left with options like "Genel Ayarlar", "Kablosuz", "Servis", "VPN", "Güvenlik", "Erişim Kısıtlamaları", "NAT", "QoS Ayarları", "Uvculamalar", "Sistem Yönetimi", and "Durum". The "Sistem Yönetimi" menu is expanded, showing "Yonetim", "Canlı Tutma", "Komut", "Fabrika Ayarları", "Firmware Güncelleme", and "Konfigürasyon Yedekleme". The main content area is divided into three sections: "Konfigürasyon Yedekleme Ayarları", "Konfigürasyonu yükle", and "UYARI". The "Konfigürasyon Yedekleme Ayarları" section contains the text "Konfigürasyon dosyasını bilgisayarınıza yedeklemek için 'Yedekle' butonuna tıklayın." The "Konfigürasyonu yükle" section contains the text "Konfigürasyon Yükleme ayarları" and "Lütfen yükleme için dosya seçiniz" with a "Gözat..." button and "Dosya seçilmedi." text. The "UYARI" section contains a warning message: "Yalnızca aynı model Router'dan yedeklenen (Back up) dosyayı yükleyin. Bu şekilde oluşturulmayan hiçbir dosyayı yüklemeyiniz!" At the bottom of the page, there are two buttons: "Yedekle" and "Yükle". The top right corner of the page shows system information: "Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std", "Zaman: 00:09:44 up 9 min, load average: 0.10, 0.11, 0.06", and "WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0".

Şekil 5. Konfigürasyon Yedekleme ve Yükleme İşlemi

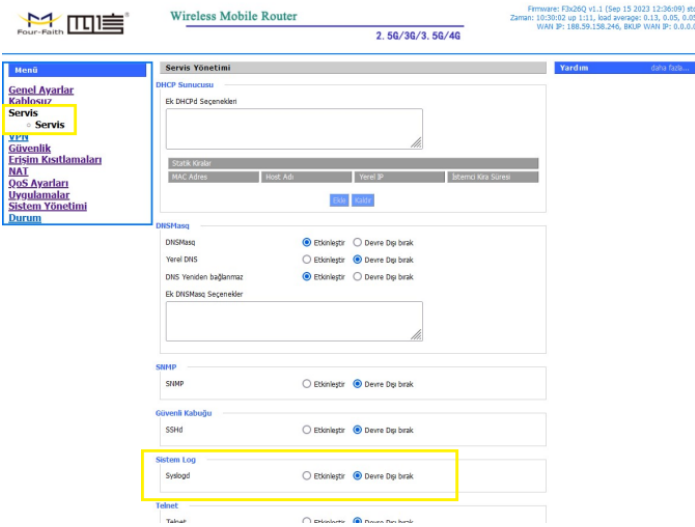
7. LOG Kaydı

7.1 Genel Açıklama

İnternet erişiminin sağlandığı projelerdeki en önemli konulardan biri güvenlidir. Söz konusu güvenliğin sağlanabilmesi, olası saldırı ve risklerin tespit edilebilmesi adına Four Faith F3x26Q modemlerde de log kaydı özelliği bulunmaktadır.

7.2 Log Kaydı Alma

Log kaydı uygulamasına başlamadan önce modeminize, ilgili firmware'yi yüklediğinizden emin olunuz. Daha sonra modeminize, log verilerinin kaydedilmesi için TF card veya SSD kartı takınız. İnternet erişimini sağladıktan sonra log kaydı ile ilgili ayarlara geçebilirsiniz. Her menüde yaptığınız ayarları tamamladıktan sonra sayfanın alt kısmından Save, ardından Apply Settings'e tıklayarak yapılan ayarları kaydetmeyi unutmayınız.



Şekil 1. Servis Syslogd

Uygulanacak Adımlar

1. "Servis" menüsünden "Servis" sekmesini seçin.
2. "Sistem Log" etkinleştiriyoruz.
3. "Durum" sekmesinden "net" , "konsol" ve "web" sekmelerini açıyoruz.

7.3 Net Log

Log verilerini uzaktaki bir server a kaydetmek için kullanılır.

The screenshot displays the configuration page for a Wireless Mobile Router. The interface is in Turkish and shows various settings for network management. The 'Servis Yönetimi' (Service Management) section is active, and the 'Net Log' application is highlighted with a yellow box. The 'Net Log' settings include:

- Sistem Log:** Etkinleştir Devre Dışı bırak
- Syslog Cihaz Modu:** Net Konsol Web
- Uzak Sunucu:** 188.59.158.246

Other settings visible in the interface include:

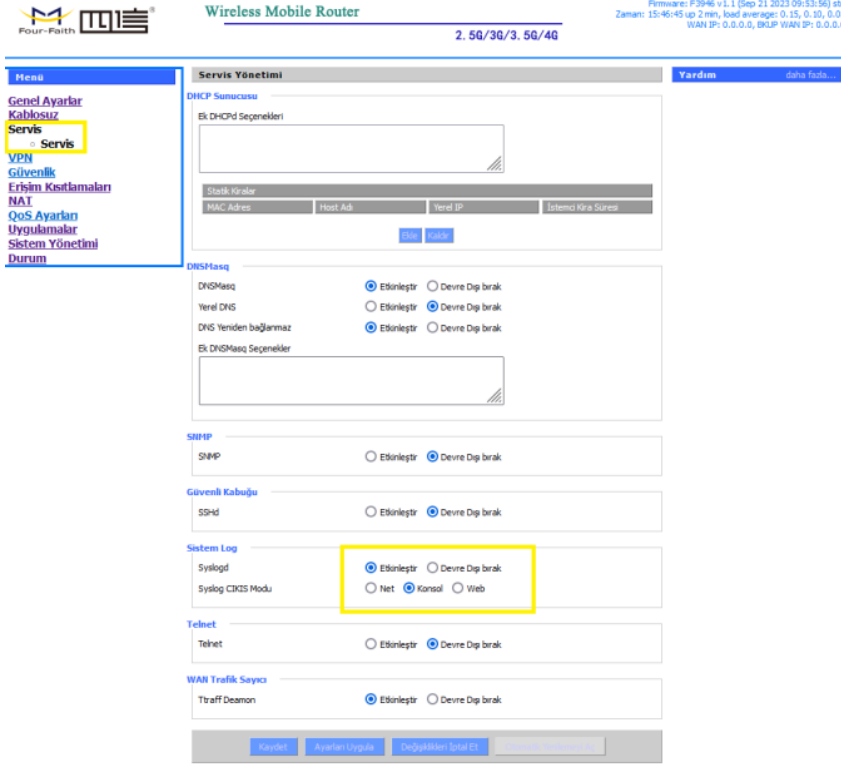
- DHCP Sunucusu:** Ek DHCPd Seçenekleri (empty text area), Statik Kiralar table (MAC Adres, Host Ad, Yerel IP, Etkinlik Süresi), Ekle, Kaldır buttons.
- DNSMasq:** Etkinleştir Devre Dışı bırak, Yerel DNS: Etkinleştir Devre Dışı bırak, DNS Yeriiden bağlanmaz: Etkinleştir Devre Dışı bırak, Ek DNSMasq Seçenekler (empty text area).
- SNMP:** Etkinleştir Devre Dışı bırak
- Güvenli Kabuğu:** Etkinleştir Devre Dışı bırak
- Telnet:** Etkinleştir Devre Dışı bırak
- WAN Trafik Sayıcı:** Etkinleştir Devre Dışı bırak

The interface also shows a sidebar menu with options like Genel Ayarlar, Kablosuz, Servis, VPN, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar, Sistem Yönetimi, and Durum. The top right corner displays firmware information: Firmware: F3946 v1.1 (Sep 21 2023 09:53:36) str, Zaman: 15:50:07 up 5 min, load average: 0.05, 0.06, 0.0, WAN IP: 0.0.0.0, BKIP WAN IP: 0.0.0.0.

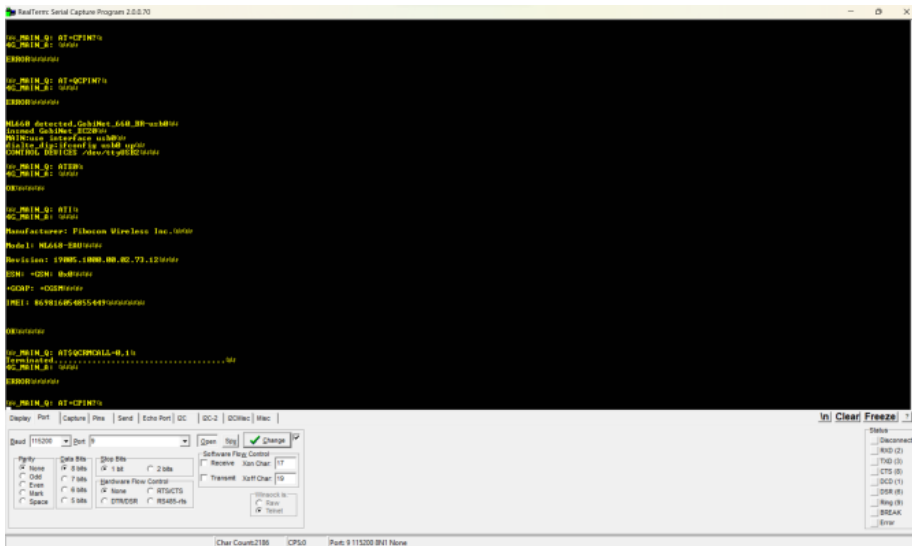
Şekil 2. Net Log Uygulaması

7.4 Konsol Log

Log verilerini konsol yardımı (RS232 veya RS485) bağlantısı ile Four Faith cihazlarda standart olan Baud 115200 8 None 1 ayarları ile pc üzerinden seri haberleşme programlarından herhangi birisiyle kaydedilebilir. (Örn: Realterm)



Şekil 3. Konsol Log Uygulaması 1



Şekil 4. Konsol Log Uygulaması 2

7.5 Web Log

Log verilerini "Web" arayüzünden anlık olarak takip edilebilir.

The screenshot shows the web interface of a Wireless Mobile Router. The top status bar displays the router's name, signal strength, and connection status (2.5G/3G/3.5G/4G). The firmware version is F3x26Q v1.1 (Sep 15 2023 12:36:09) std. The system time is 00:01:40 up 1 min, with a load average of 0.12, 0.04, 0.01. The WAN IP is 0.0.0.0, and the BKUP WAN IP is 0.0.0.0.

The left menu includes options such as Genel Ayarlar, Kablosuz, Servis, VPN, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar, Sistem Yönetimi, Durum, Router, WAN, LAN, WebLog (highlighted), Uzun Yönetimi, Akıllı Kapı Durumu, Bant Genişliği, and Sistem Bilgisi.

The main log window displays the following messages:

```
1970-01-01 00:01:10: 4G_MABN_A:
ERROR
1970-01-01 00:01:10: NL660 detected,GobNet_660-usb0
1970-01-01 00:01:10: nsm0d GobNet_660
1970-01-01 00:01:10: NABtuse pterface usb0
1970-01-01 00:01:10: dalte_dip/config usb0 up
1970-01-01 00:01:10: CONTROL DEVICES /dev/ttyUSB2
1970-01-01 00:01:10: 4G_MABN_Q: ATE0
1970-01-01 00:01:11: 4G_MABN_A:
OK
1970-01-01 00:01:11: 4G_MABN_Q: ATI
1970-01-01 00:01:11: 4G_MABN_A:
Manufacturer: Fibocom Wireless Inc.
Model: NL668-EAU
Revision: 1900S.1000.00.02.73.12
ESN: +GSM: 0x0
+GCAP: +CGSM
IMEI: 869816055584618
```

Şekil 5. Durum WebLog Uygulaması

8. VPN Uygulaması

8.1 IPSEC (Internet Protocol Security) Nedir?

Doğru bilginin doğru zamanda doğru kişinin eline geçmesi bugün olduğu gibi yüz yıllar önce de oldukça önemli bir konuydu. Yüzyıllar önce Kriptex adı verilen ve rivayete göre Leonardo Da Vinci tarafından icat edilen bir Mekanizma kullanılıyordu. İletilmesi istenen gizli bilgi papirüs kağıdına yazılarak/çizilerek bu mekanik cihazın içindeki sirke dolu cama sarılıyordu, cam da bu mekanik aksamın içine yerleştiriliyordu, eğer şifreyi biliyor iseniz mekanizmayı açabiliyordunuz; yok eğer zor kullanarak mekanizmayı açmaya çalışır iseniz Kriptex içerisindeki Cam kırılıyor ve içindeki sirke Papirüs kağıdına dökülüyor böylece belgedeki gizli bilgi siz okuyamadan siliniyordu.

Günümüzde ise TCP/IP protokolündeki bilgilerini şifreleme güvenlik hizmeti kullanılarak daha güvenli ve özel haberleşme sağlanması için IPSEC kullanılır. IPsec veriyi, şifreleyen/kriptolayan (encryption), bütünlüğünü sağlayan (integrity) , kimlik doğrulaması (authentication) ve verinin network üzerinde güvenli iletimini (Secure transmission) sağlayan bir standartdır.

8.1.1 Four Faith Routerlarda IPSEC Nasıl Uygulanır?

Router “WEB ARAYÜZÜ” ‘ne girerek “VPN” menüsü altında “IPSEC” seçeneğine tıklıyoruz. Ardından “Bağlantı Durumu ve Kontrolü” kısmında “Ekle” tuşuna basarak IPSEC bağlantımızı kurmaya başlıyoruz.

The screenshot shows the web interface of a Four Faith Wireless Mobile Router. The top navigation bar includes the Four Faith logo, the router model 'Wireless Mobile Router', and the status '2.5G/3G/3.5G/4G'. The firmware version is 'F3x26Q v1.1 (Sep 15 2023 12:36:09) stc' and the time is 'Zaman: 00:01:24 up 1 min, load average: 0.02, 0.01, 0.00'. The WAN IP is 'WAN IP: 0.0.0.0, BKUP WAN IP: 0.0.0.0'.

The main content area is divided into three sections:

- Genel Ayarlar**: Includes 'NAT-Geçiş Etkinleştir' (checked), 'Hata Ayıklama Seviyesi' (Hiçbiri), and 'IPSEC OVER LZTP' (Etkinleştir selected, Devre Dışı bırak unselected). A 'Kaydet' button is present.
- Bağlantı Durumu ve Kontrolü**: Contains a table for 'Bağlantı Durumu ve Kontrolü' with columns: Num, Adı, Tipi, Genel Adı, Durum, Eylem. A 'Ekle' button is highlighted in the 'Num' column.
- Sertifika Yönetimi**: Contains a table for 'Sertifika Yönetimi' with columns: CA Adı, Referans Sayısı, Eylem. A 'Ekle' button is present.

The left sidebar menu includes: Menü, Genel Ayarlar, Kablosuz, Servis, VPN (highlighted), PPTP, LZTP, OPENVPN, IPSEC (highlighted), IKE, Güvenlik, Erişim Kısıtlamaları, NAT, QoS Ayarları, Uygulamalar, Sistem Yönetimi, Durum. The right sidebar includes: Yardım, NAT-Geçiş (Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın), Log-Level (Hata ayıklamayı etkinleştirin yada devre dışı bırakın), Bağlantı Durumu (15 bağlantı oluşturulabilir).

Şekil 1.IPSEC Aktifleştirme

Daha sonra çıkan sayfayı projemiz doğrultusunda dolduruyoruz. Öncelikle dolduracağımız yerlerin ne anlama geldiğini bilmemiz gerekiyor.

Menü

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
 - PPTP
 - L2TP
 - OPENVPN
 - IPSEC
 - GRE
- Güvenlik
- Erişim Kısıtlamaları
- NAI
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Tipi

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rol: İstemci

Bağlantı

Adı: [] Etkin:

Yerel WAN Arayüzü: WAN Uzak WAN adresi: []

Yerel Alt Ağ: [] Uzak Alt Ağ: []

Yerel ID: [] Uzak ID: []

Algılama

DPD Algılamayı Etkinleştir:

Zaman Aralığı: 60 (Sn) Zaman aşımı: 60 (Sn) Eylem: restart

Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir:

Phase 1

IKE Şifreleme: AES (256 bit) IKE Doğrulama: MD5 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 0 Saat

Phase 2

ESP Şifreleme: AES (256 bit) ESP Doğrulama: SHA2 (512) ESP Grup tipi: NULL

ESP Şifre Zamanı: 0 Saat

Enable IKEv2:

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak fedir!)

Perfect Forward Secrecy (PFS)

Doğrulama

Doğrulama: Paylaşılan şifreyi kullanın: []

X.509 sertifikası oluşturun ve kullanın

Not

sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

Tipi

IPsec tipini seçin,tünel ya da transport

Rol

IPsec rolünü seçin, istemci ya da sunucu

Bağlantının Adı

IPsec bağlantı adı 20 karaktere kadar olmalıdır

Yerel ve Uzak Ağ için ID

Yerel ve uzak ağ ID tanımlamak için IP adresi veya bağıntı @ işaretini ekleyerek domain adı girilebilir

PSK Değeri

PSK değerinin uzunluğu 30'dan fazla olamaz

IKEv2

undefined

Şekil 2.IPSEC Bağlantı Ayarları

Bu özellikleri tam olarak anladıktan sonra aşağıdaki resimlerde IPSEC uygulamasını yapabiliriz. Öncelikle istemci (client) tarafını aşağıdaki gibi yaptıktan sonra “Ayarları Kaydet” ‘i tıklıyoruz.

Menü

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
 - PPTP
 - L2TP
 - OPENVPN
 - IPSEC
 - GRE
- Güvenlik
- Erişim Kısıtlamaları
- NAI
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Tipi

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rol: İstemci Sunucu

Bağlantı

Bağlantı:

Adı: Zttest Etkin:

Yerel WAN Arayüzü: WAN Uzak WAN adresi: 81.6.111.88

Yerel Alt Ağ: 192.168.1.0/24 Uzak Alt Ağ: 192.168.1.0/24

Yerel ID: @zt2 Uzak ID: @zt1

Algılama

DPD Algılamayı Etkinleştir:

Zaman Aralığı: 60 (Sn) Zaman aşımı: 180 (Sn) Eylem: restart

Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir:

Phase 1

IKE Sifreleme: 3DES IKE Doğrulama: SHA1 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 24 Saat

Phase 2

ESP Sifreleme: 3DES ESP Doğrulama: SHA1 ESP Grup tipi: NULL

ESP Sifre Zamanı: 24 Saat

Enable IKEv2:

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletilir)

Perfect Forward Secrecy (PFS)

Doğrulama

Doğrulama:

Paylaşılan Sifreyi kullanın: 123456

X.509 sertifikası oluşturun ve kullanın

Yardım

Gözetim...

Not

sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

Tipi

IPsec tipini seçin, tünel ya da transport

Roller

IPsec rolünü seçin, istemci ya da sunucu

Bağlantının Adı

IPsec bağlantı adı 20 karaktere kadar olmalıdır

Yerel ve Uzak Ağ için ID

Yerel ve uzak ağa ID tanımlamak için IP adresi veya bağında @ işareti ekleyerek domain adı girilebilir

PSK Değeri

PSK değerinin uzunluğu 30'dan fazla olamaz

IKEv2

undefined

Şekil 3. IPSEC İstemci (Client)

Daha sonra sunucu (server) tarafı ayarlarını yaptıktan sonra aynı şekilde “Ayarları Kaydet” ‘i tıklıyoruz.

[Genel Ayarlar](#)

[Kablosuz Servis](#)

VPN

- o [PPTP](#)
- o [L2TP](#)
- o [OPENVPN](#)
- o [IPSEC](#)
- o [GRE](#)

[Güvenlik Erişim Kısıtlamaları](#)

[NAT](#)

[QoS Ayarları](#)

[Uygulamalar](#)

[Sistem Yönetimi](#)

[Durum](#)

Tipi

Tipi: Ağ'dan Ağ'a Sanal Özel Ağ

IPSEC rol: İstemci Sunucu

Bağlantı

Bağlantı:

Adı: Zttest	Etkin: <input checked="" type="checkbox"/>
Yerel WAN Arayüzü: WAN	Uzak WAN adresi:
Yerel Alt Ağ: 192.168.1.0/24	Uzak Alt Ağ: 192.168.1.0/24
Yerel ID: @zt1	Uzak ID: @zt2

Algoritma

Algoritma:

DPD Algoritmayı Etkinleştir:

Zaman Aralığı: 60 (Sn) Zaman aşımı: 180 (Sn) Eylem: restart

Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir:

Phase 1

IKE Şifreleme: 3DES IKE Doğrulama: SHA1 IKE Grup tipi: Grup2(1024)

IKE Ömrü: 24 Saat

Phase 2

ESP Şifreleme: 3DES ESP Doğrulama: SHA1 ESP Grup tipi: NULL

ESP Şifre Zamanı: 24 Saat

Enable IKEv2

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletir!)

Perfect Forward Secrecy (PFS)

Doğrulama

Doğrulama:

Paylaşılan Şifreyi kullanın: 123456

X.509 sertifikası oluşturun ve kullanın

Not

sunucu olarak davrandığında, yerel ID'si boş bırakılmaz

Tipi

IPsec tipini seçin, tünel ya da transport

Rol

IPsec rolünü seçin, istemci ya da sunucu

Bağlantının Adı

IPsec bağlantı adı 20 karaktere kadar olmalıdır

Yerel ve Uzak Ağ için ID

Yerel ve uzak ağ ID tanımlamak için IP adresi veya başında @ işareti ekleyerek domain adı girilebilir

PSK Değeri

PSK değerinin uzunluğu 30'dan fazla olamaz

IKEv2

undefined

Şekil 4.IPSEC Sunucu (SERVER)

Daha sonra router'ları yeniden başlatıyoruz ve ayarların yapıldığı sekmeden bağlantı durumunu gözlemleyebiliyoruz.

Menü

[Genel Ayarlar](#)

[Kablosuz](#)

[Servis](#)

VPN

- [PPTP](#)
- [L2TP](#)
- [OPENVPN](#)
- [IPSEC](#)
- [GRE](#)

[Güvenlik](#)

[Erişim Kısıtlamaları](#)

[NAT](#)

[QoS Ayarları](#)

[Uygulamalar](#)

[Sistem Yönetimi](#)

[Durum](#)

Genel Ayarlar

Genel Ayarlar

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi: Hiçbiri

IPSEC OVER L2TP: Etkinleştir Devre Dışı bırak

[Kaydet](#)

Bağlantı Durumu ve Kontrolü

Bağlantı Durumu ve Kontrolü

Num	Adı	Tipi	Genel Adı	Durum	Eylem
1	Zttest	Tünel-server	192.168.1.0/24-[WAN1] server-[192.168.1.0/24]	Erişlemiyor	Sil Düzenle Yenile Ekle

Sertifika Yönetimi

Sertifika Yönetimi

CA Adı	Referans Sayısı	Eylem
Ekle		

Yardım

NAT-Geçiş

Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

Log-Level

Hata ayıklamayı etkinleştirin yada devre dışı bırakın

Bağlantı Durumu

15 bağlantı oluşturulabilir

Şekil 5.IPSEC Sunucu(Server) Kurulmuş Bağlantı Örneği

Menü

[Genel Ayarlar](#)

[Kablosuz](#)

[Servis](#)

VPN

- [PPTP](#)
- [L2TP](#)
- [OPENVPN](#)
- [IPSEC](#)
- [GRE](#)

[Güvenlik](#)

[Erişim Kısıtlamaları](#)

[NAT](#)

[QoS Ayarları](#)

[Uygulamalar](#)

[Sistem Yönetimi](#)

[Durum](#)

Genel Ayarlar

Genel Ayarlar

NAT-Geçiş Etkinleştir

Hata Ayıklama Seviyesi: Hiçbiri

IPSEC OVER L2TP: Etkinleştir Devre Dışı bırak

[Kaydet](#)

Bağlantı Durumu ve Kontrolü

Bağlantı Durumu ve Kontrolü

Num	Adı	Tipi	Genel Adı	Durum	Eylem
1	Zttest	Tünel-client	192.168.1.0/24-[WAN1] 81.6.111.88-[192.168.1.0/24]	Erişlemiyor	Sil Düzenle Yenile Ekle

Sertifika Yönetimi

Sertifika Yönetimi

CA Adı	Referans Sayısı	Eylem
Ekle		

Yardım

NAT-Geçiş

Nat geçiş fonksiyonunu etkinleştirin veya devre dışı bırakın

Log-Level

Hata ayıklamayı etkinleştirin yada devre dışı bırakın

Bağlantı Durumu

15 bağlantı oluşturulabilir

Şekil 6.IPSEC İstemci(Client) Kurulmuş Bağlantı Örneği

NOT 1: Baęlantı durumunu gözlemlendięimiz sayfada “öp kutusu” ikonu ile baęlantıyı silebilir, “kalem” ikonu ile baęlantı ayarlarını deęiřtirebilir “yenile” ikonu ile baęlantı denemesini bařtan bařlatabilirsiniz. Bu kapsamda “kalem” ve “yenileme” ikonlarını sadece ihtiya duyduęumuzda kullanmamız gerekir. Aksi takdirde her seferinde iřlem yeniden bařlayacaęı için IPSEC baęlantının yapılması önlenir.

NOT 2: oęu uygulamada router modemlerin 4G’si BACKUP(yedekli) olarak kullanılmaktadır. Böyle uygulamalarda Router modemimizi internete ıkarmak için kullandıęımız cihazlar(ADSL Modem, Uydunet Modem gibi) ierisinde herhangi bir deęiřiklik yapmadan IPSEC tüneli kullanabiliriz. Bu řekilde olan uygulamalarda sadece IPSEC tünel kurmak istedięimiz uzak Aę’a hem 4G hem de yedek olarak kullandıęımız internetin IP’sini kaydetmemiz gerekmektedir.

8.2 MEDAŞ VPN Ayarları

The screenshot displays the 'Genel Ayarlar' (General Settings) section of the MEDAŞ VPN configuration. The 'Genel Ayarlar' tab is active, showing various settings. The 'Bağlantı Durumu ve Kontrolü' (Connection Status and Control) section is highlighted with a red box. It contains a table with the following data:

Num Adı	Tipi	Genel Adı	Durum	Eylem
1	medas	Tünel-client 10.123.11.0/27-[WAN1] vpn1.meramedas.com.tr-- [10.34.255.0/24,10.107.0.0/17]	Bağlantı Kuruldu	

Below the table, there is a red arrow pointing to the text: "Çift Altağı destekliyor. 2 Ayrık tünel birleştirilebiliyor".

Şekil 7. MEDAŞ VPN 1

The screenshot displays the 'Bağlantı' (Connection) and 'Gelişmiş Ayarlar' (Advanced Settings) sections of the MEDAŞ VPN configuration. The 'Bağlantı' section is highlighted with a red box. It contains the following fields:

Adı	Etkin
medas	<input checked="" type="checkbox"/>

Other fields include: Yerel WAN Arayüzü (WAN), Uzak WAN adresi (vpn1.meramedas.com), Yerel Alt Ağ (10.123.21.0/27), Uzak Alt Ağ (10.107.0.0/17,10.34.255.0/24), Yerel ID (10.123.21.1), and Uzak ID (88.255.44.70). A red arrow points to the 'Uzak Alt Ağ' field with the text: "iki ayrı alt ağı aralarında virgül koyarak "." boşluk bırakmadan yazabilir".

The 'Algilama' (Discovery) section is also highlighted with a red box. It contains the following fields:

DPD Algılamayı Etkinleştir	Zaman Aralığı	(Sn) Zaman aşımı	(Sn) Eylem
<input checked="" type="checkbox"/>	60	180	restart

The 'Gelişmiş Ayarlar' (Advanced Settings) section is also visible. It contains the following fields:

Phase 1	Phase 2
IKE Şifreleme: 3DES	ESP Şifreleme: 3DES
IKE Doğrulama: SHA1	ESP Doğrulama: SHA1
IKE Grup tipi: Grup2(1024)	ESP Grup tipi: NULL
IKE Ömrü: 24 Saat	ESP Şifre Zamanı: 24 Saat

There are also checkboxes for 'Enable IKEv2', 'IKE agresif moda izin ver', and 'Perfect Forward Secrecy (PFS)'.

Şekil 8. MEDAŞ VPN 2

bağlantı sorgulama

Algılama Periyodu: 300 Sn

Terah Edilen Sunucu IP: 8 8 8 8

Diğer Sunucu IP: 8 8 4 4

Bağlantı Hataları Restart: Etkinleştir Devre Dışı bırak (Default: 10 dakika)

Fixed WAN Netmask Address: Etkinleştir Devre Dışı bırak

STP: Etkinleştir Devre Dışı bırak

IPSEC Çevirini Devam et

Bağlantı Sorgulama: Ping

Algılama Periyodu: 3600 Sn

Terah Edilen Sunucu IP: 10 34 255 18

Özel Ayarlar

Router Adı: GENCBEGES

Host Adı:

Domain Adı:

MTU: Auto 1500

Force Net Card Mode: Auto

Ağ Ayarları

Router IP

Yerel IP Adresi: 10 123 11 1

Maksimum DHCP Kullanıcı:
Router'ınız dağıtmış olduğu adres sayısını sınırlayabilirsiniz. 0 (sıfır) sadece önceden tanımlanan statik adreslerin dağıtılacağı anlamına gelir.

Zaman Ayarı:
Bulunmuş olduğunuz zaman dilimini ve Yaz Saati Uygulama (YSU) dönemini seçiniz. Router yerel zamanı veya UTC zamanını kullanabilir.

Şekil 9. MEDAŞ VPN 3

Four-Faith Wireless Mobile Router 3G/4G/4G+

Firmware: R100 v1.0 (Sep 21 2023 14:18:51) sfd
Zaman: 19:43:52 up 15 min, load average: 0.02, 0.03, 0.03
WAN IP: 192.168.0.108, BKUP WAN IP: 0.0.0.0
Dil: Türkçe

Cron

Cron: Etkinleştir Devre Dışı bırak

Ek Cron Görevleri:

Dil Seçimi

Dil: Türkçe

Uzaktan Yönetim

Uzaktan Yönetim: Etkinleştir Devre Dışı bırak

Protokol: V1.0 V2.0

Sunucu IP'si: 47.88.21.65

Sunucu Portu: 9901 (Default: 44008, Aralık: 1 - 65535)

Canlılık Periyodu: 60 (Default: 60SnAralık: 1 - 999)

3G Veri Akışı Yükleme Periyodu: 300 (Default: 300SnAralık: 1 - 86400)

Aygıt Kodu: SN

Cihaz Tipi Tanımlama: F3x26Q

Özelleştirilmiş Yerel Domian: wifi.cn

Firmware Güncelleme

Firmware Güncelleme: Etkinleştir Devre Dışı bırak

Kaydet Ayarları Uygula Değişiklikleri İptal Et Router'ı Yeniden Başlat

Şekil 10. MEDAŞ Uzaktan Yönetim Ayarları

Komut Sayfası

Yardım daha fazla...

Komut Satırı

Komutlar

ping 10.34.255.18

```
PING 10.34.255.18 (10.34.255.18): 56 data bytes  
64 bytes from 10.34.255.18: seq=0 ttl=255 time=51.080 ms  
64 bytes from 10.34.255.18: seq=1 ttl=255 time=54.320 ms  
64 bytes from 10.34.255.18: seq=2 ttl=255 time=53.300 ms  
--- 10.34.255.18 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 51.080/52.900/54.320 ms
```

Komutu Çalıştır

Komutlar:

Komut satırını web arayüzünden çalıştırabilirsiniz. Metin alanına komutunuzu yazın ve göndermek için *Komutu Çalıştır* butonuna tıklayın.

Şekil 11. MEDAŞ VPN Testi

8.3 BEDAŞ VPN Ayarları

Wireless Mobile Router

2. 5G/3G/3. 5G/4G

Zamanı: 12:39:33 up 12:09, load average: 0.01, 0.03, 0.04
WAN IP: 5.24.231.92, BKUP WAN IP: 0.0.0.0

Menü

- Genel Ayarlar
- Kablosuz Servis
- VPN
 - PPTP
 - L2TP
 - OPENVPN
 - IPSEC
 - GRE
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Tipi

Tipi: Ağ'dan Ağ'a Senel Özel Ağ

IPSEC rol: İstemci Sunucu

Bağlantı

Bağlantı

Adı: VPN

Yerel WAN Arayüzü: WAN

Yerel Alt Ağ: 0.0.0.0/0

Yerel ID: 0.0.0.0/0

Etkin:

Uzak WAN adresi: 85.111.45.4

Uzak Alt Ağ: 0.0.0.0/0

Uzak ID: 0.0.0.0/0

Algılama

DPD Algılamayı Etkinleştir:

Zaman Aralığı: (null) (Sn) Zaman aşımı: (null) (Sn) Eylem:

Gelişmiş Ayarlar

Gelişmiş ayarları etkinleştir:

Phase 1

IKE Şifreleme: 3DES

IKE Doğrulama: MDS

IKE Grup tipi: Grup2(1024)

IKE Ömrü: 24 Saat

Phase 2

ESP Şifreleme: 3DES

ESP Doğrulama: MDS

ESP Grup tipi: NULL

ESP Şifre Zamanı: 4 Saat

Enable IKEv2:

IKE agresif moda izin ver. Mümkünse kullanmayın (paylaşılan şifre açık metin olarak iletir!)

Perfect Forward Secrecy (PFS)

Doğrulama

Doğrulama

Paylaşılan Şifreyi kullanın

X.509 sertifikası oluşturun ve kullanın

Ayarları Uygula Değişiklikleri İptal Et

Yardım

daha fazla...

Tipi

IPsec tipini seçin. tünel ya da transport

Rol

IPsec rolünü seçin. istemci ya da sunucu

Bağlantının Adı

IPsec bağlantı adı 20 karaktere kadar olmalıdır

Yerel ve Uzak Ağ için ID

Yerel ve uzak ağa ID tanımlamak için IP adresi veya bağında @ işaretini ekleyerek domain adı girilebilir

PSK Değeri

PSK değerinin uzunluğu 30'dan fazla olamaz

IKEv2

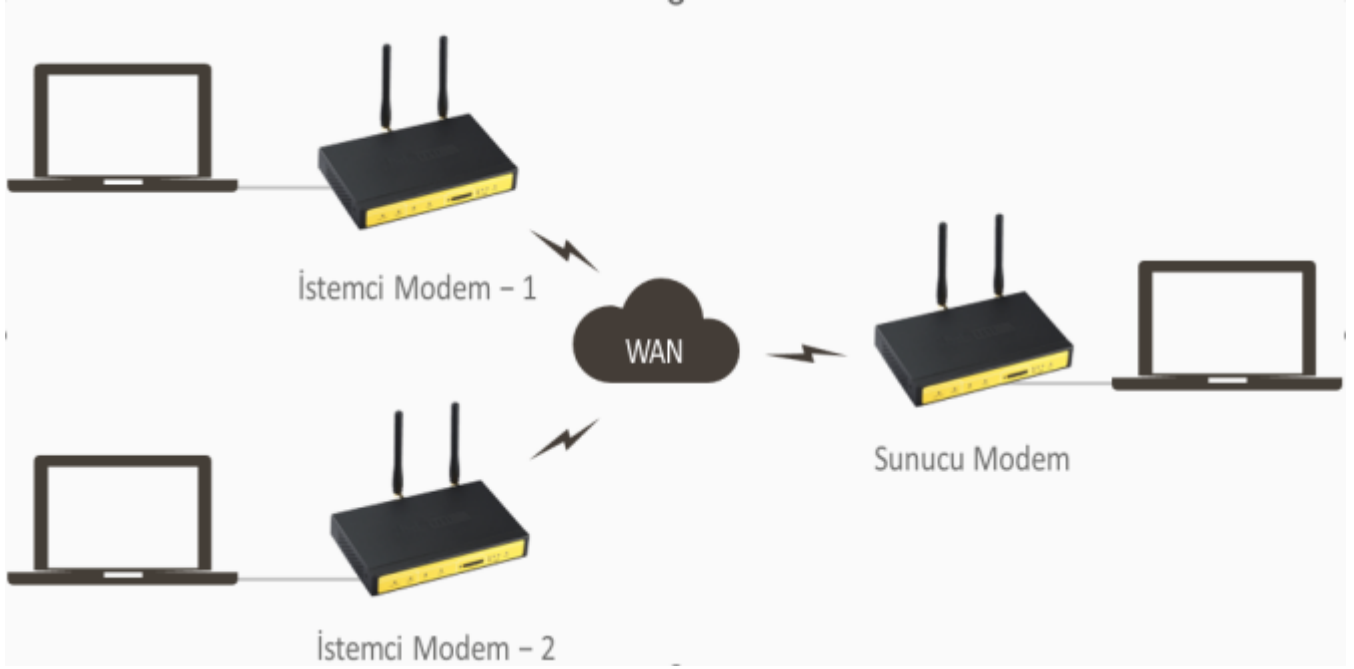
undefined

Şekil 12. BEDAŞ VPN Ayarları

NOT: BEDAS VPN IPSEC Kurulumu gerçekleştirildikten sonra modeme uzaktan erişim kapanır. Wan IP ile uzaktan 8088 portu ile erişemezsiniz. Ayrıca tüm yönlendirmeler VPN üzerine olduğu için açılan portlara da erişim olmayacaktır. Cihaz sadece local erişime açıktır.

8.4 OpenVPN Uygulması

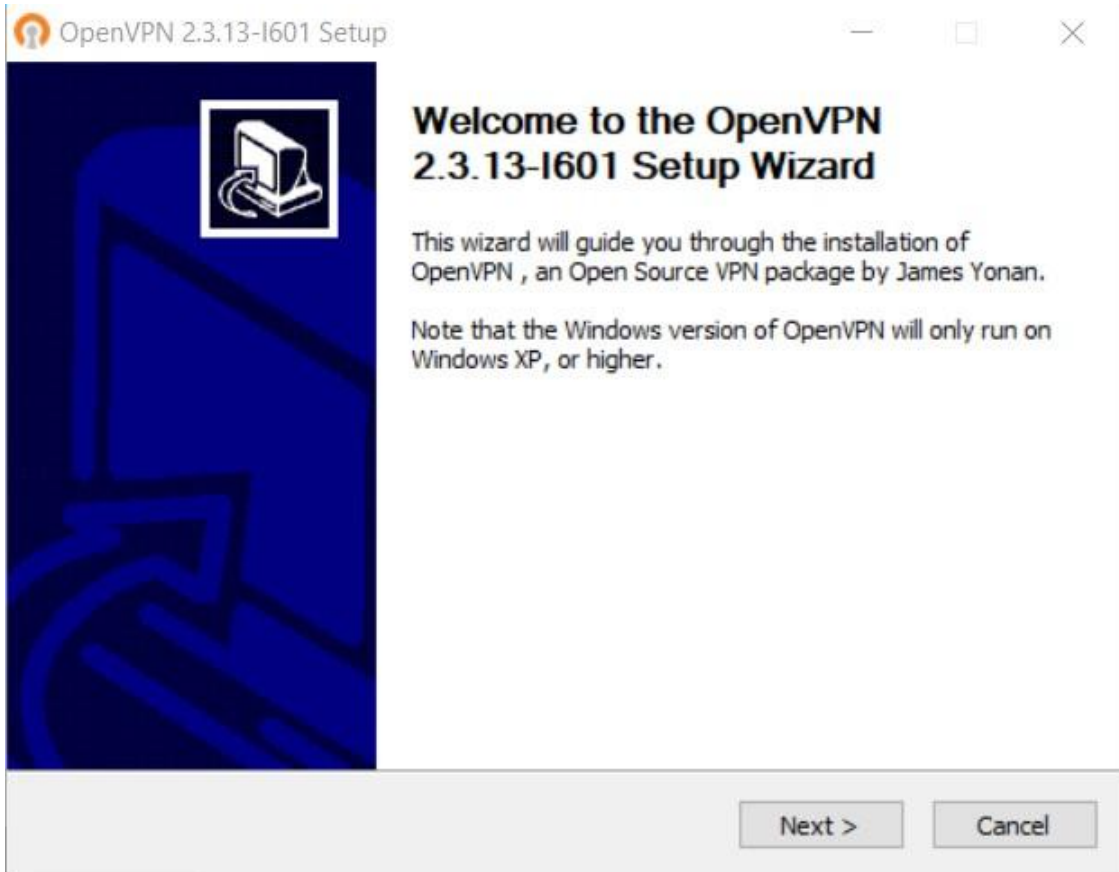
Four-Faith router modemler; PPTP, L2TP, IPSEC, GRE VPN türlerini desteklediği gibi OpenVPN'i de desteklemektedir. Kurulacak olan OpenVPN ağında bir sunucu ve birden çok istemci olmalıdır. Bu kılavuzda bir sunucu ve iki istemci olan örnek anlatılmıştır. Amaç, istemciler arasında VPN bağlantısının kurulması ve güvenli haberleşmenin sağlanmasıdır.



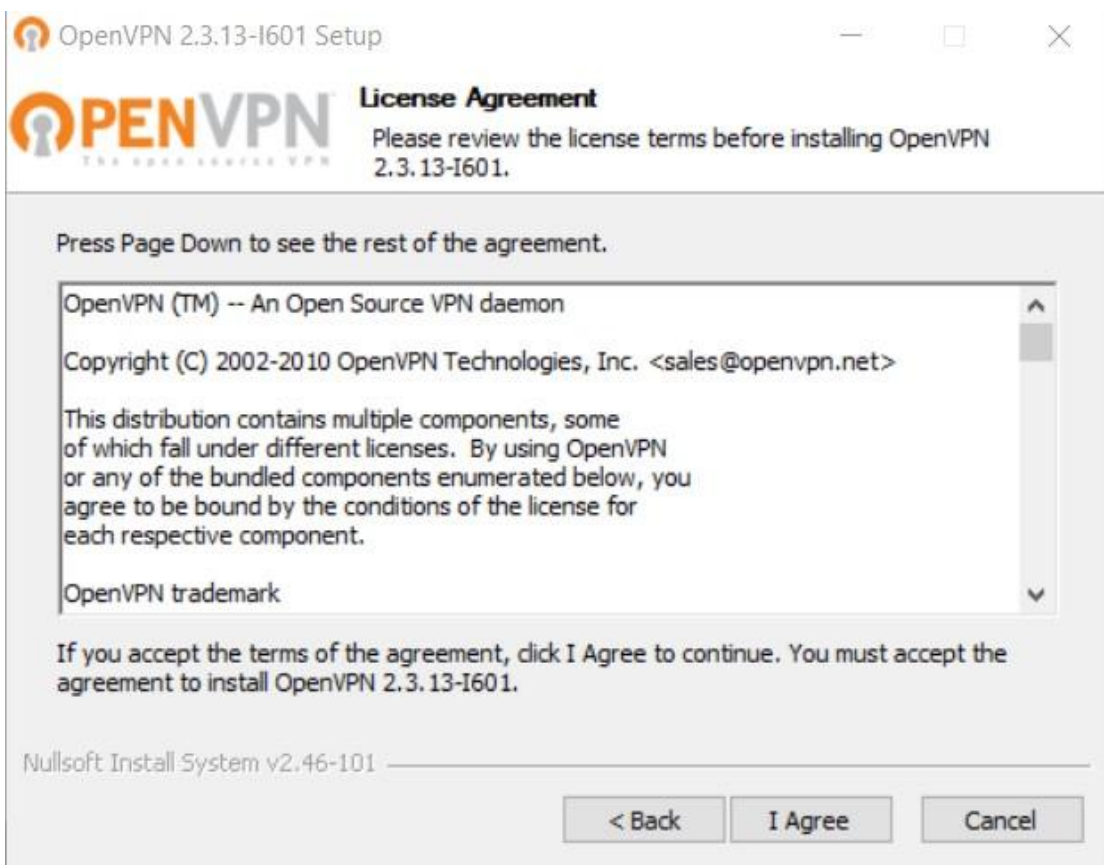
Şekil 1. Open VPN Uygulama Şeması

8.4.1 PC ile Modem Arasında OpenVPN Tünel Kurulumu

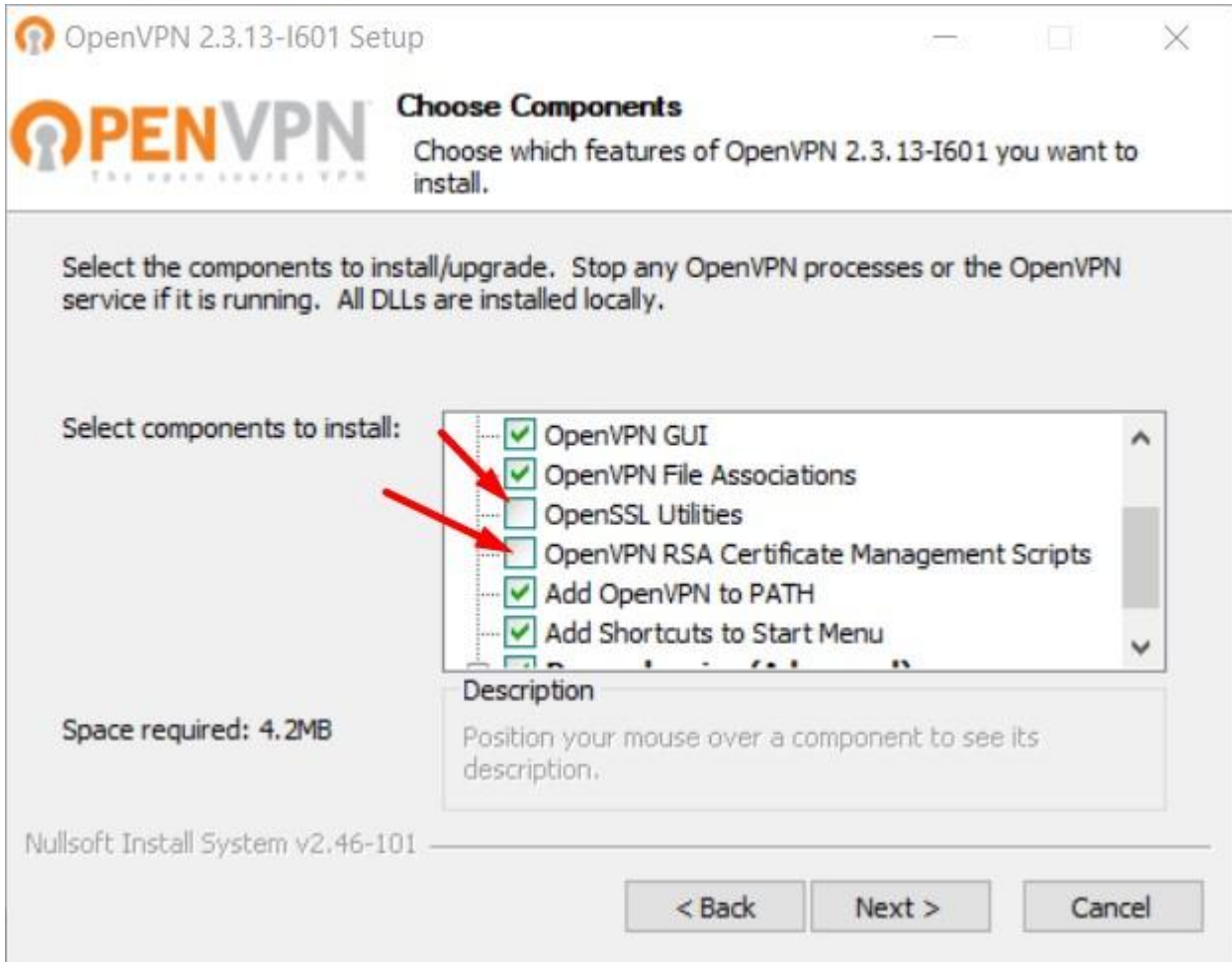
Öncelikli olarak OpenVPN programını PC'mize kuruyoruz. Aşağıdaki adımlar ile;



1. Adım



2. Adım



3. Adım

- Klasör içerisinde bulunan OpenVPN programını kurunuz. Kurulumu C:/ klasörüne yapacak kurulum dosyası içerisindeki easy-rsa klasörünü kopyalayıp D:/OpenVPN/easy-rsa uzantısı olacak şekilde kayıt edin. Aşağıda görselde olduğu gibi.

This PC > YEDEK (D:) > OpenVPN > easy-rsa >

Name	Date modified	Type	Size
keys	12/16/2022 5:09 PM	File folder	
.rnd	12/16/2022 5:09 PM	RND File	1 KB
build-ca	11/3/2016 1:24 PM	Windows Batch File	1 KB
build-dh	11/3/2016 1:24 PM	Windows Batch File	1 KB
build-key	11/3/2016 1:24 PM	Windows Batch File	1 KB
build-key-pass	11/3/2016 1:24 PM	Windows Batch File	1 KB
build-key-pkcs12	11/3/2016 1:24 PM	Windows Batch File	1 KB
build-key-server	11/3/2016 1:24 PM	Windows Batch File	1 KB
clean-all	11/3/2016 1:24 PM	Windows Batch File	1 KB
index.txt.start	11/3/2016 1:24 PM	START File	0 KB
init-config	11/3/2016 1:24 PM	Windows Batch File	1 KB
openssl-1.0.0.cnf	11/3/2016 1:24 PM	CNF File	9 KB
README	11/3/2016 1:24 PM	Text Document	2 KB
revoke-full	11/3/2016 1:24 PM	Windows Batch File	1 KB
serial.start	11/3/2016 1:24 PM	START File	1 KB
vars	11/29/2022 4:59 PM	Windows Batch File	1 KB
vars.bat.sample	11/29/2022 4:59 PM	SAMPLE File	1 KB

Şekil 2. Easy-rsa Kayıt

Sırayla aşağıdaki adımları uygulayalım.

Name	Date modified	Type	Size
keys	12/16/2022 5:09 PM		
.rnd	12/16/2022 5:09 PM		
build-ca	11/3/2016 1:24 PM		
build-dh	11/3/2016 1:24 PM		
build-key	11/3/2016 1:24 PM		
build-key-pass	11/3/2016 1:24 PM		
build-key-pkcs12	11/3/2016 1:24 PM		
build-key-server	11/3/2016 1:24 PM		
clean-all	11/3/2016 1:24 PM		
index.txt.start	11/3/2016 1:24 PM		
init-config	11/3/2016 1:24 PM		
openssl-1.0.0.cnf	11/3/2016 1:24 PM		
README	11/3/2016 1:24 PM		
revoke-full	11/3/2016 1:24 PM		
serial.start	11/3/2016 1:24 PM		
vars	11/29/2022 4:59 PM	Windows Batch File	1 KB
vars.bat.sample	11/29/2022 4:59 PM	SAMPLE File	1 KB

How do you want to open this file?

Notepad

Look for an app in the Microsoft Store

[More apps ↓](#)

Always use this app to open .sample files

OK

4. Adım Vars Bat Open

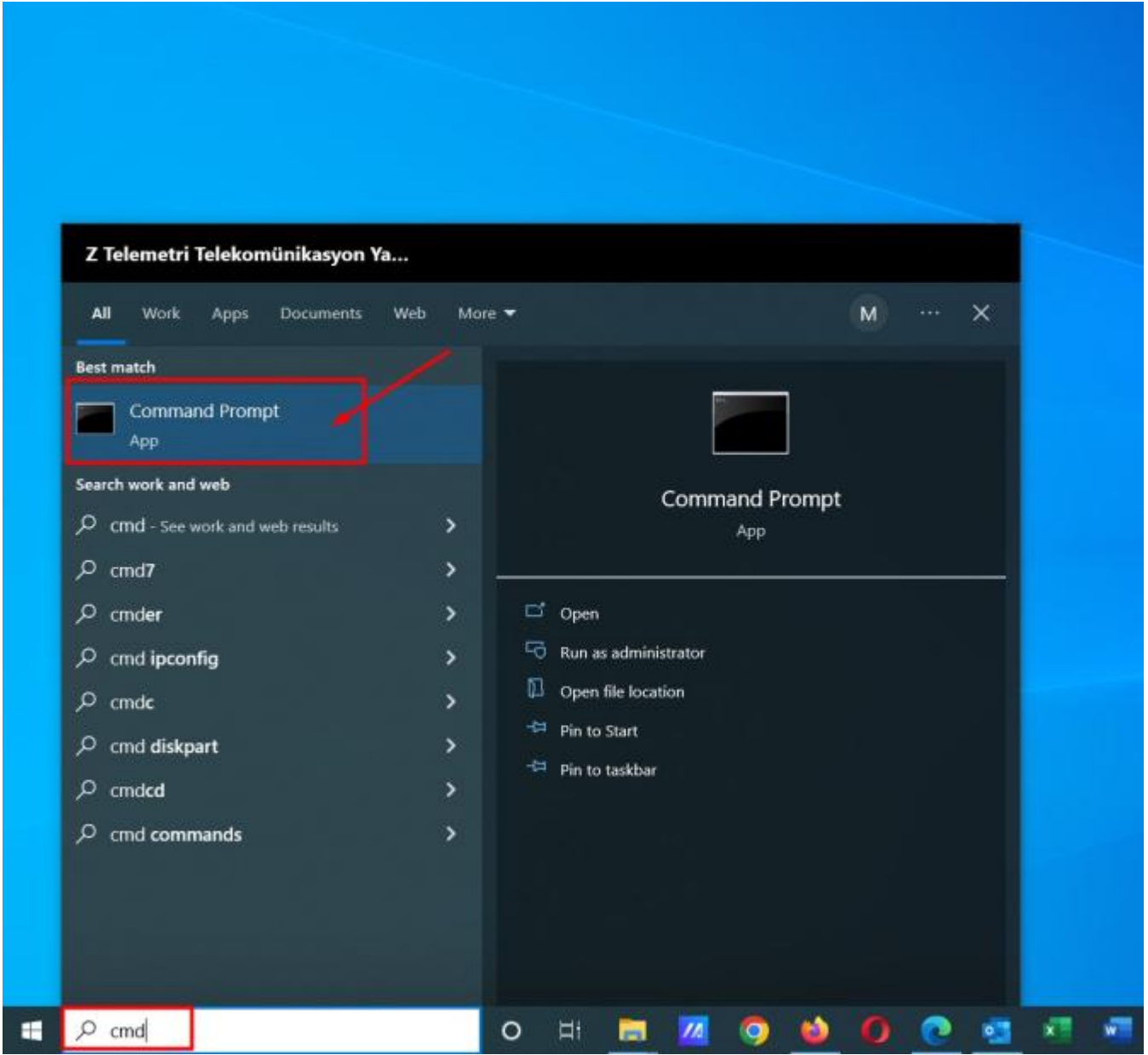
```
vars.bat.sample - Notepad
File Edit Format View Help
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.
set HOME=D:\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this to 2048 if you
rem are paranoid. This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set KEY_SIZE=1024
```

5. Adım Vars Bat Değişiklik

- PC mizde başlat menüsünden “cmd” yazarak Command Prompt açıyoruz. OpenVPN için Sertifikaları oluşturuyoruz kendimize ait aşağıdaki adımları izleyerek hepsini oluşturunuz.



6. Adım Cmd (Komut Sistemi) Açılması

- İlk aşamada gerekli dosyaya girerek Key klasörü oluşturuyoruz ve önceli sertifikaları temizliyoruz.

```
C:\> Command Prompt
Microsoft Windows [Version 10.0.19045.2251]
(c) Microsoft Corporation. All rights reserved.

C:\Users\Mustafa-Asus>d:

D:\>cd D:\OpenVPN\easy-rsa

D:\OpenVPN\easy-rsa>init-config

D:\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 file(s) copied.

D:\OpenVPN\easy-rsa>vars

D:\OpenVPN\easy-rsa>clean-all
1 file(s) copied.
1 file(s) copied.
```

7. Adım Commad 1

- **CA Cert Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.

```
Command Prompt
D:\OpenVPN\easy-rsa>build-ca
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:OPENVPN_CA
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com
```

8. Adım Command 2

- **Server Key Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.

```
Command Prompt
D:\OpenVPN\easy-rsa>build-key-server server
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:SERVER
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:ZT
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName          :PRINTABLE:'TR'
stateOrProvinceName :PRINTABLE:'TURKEY'
localityName         :PRINTABLE:'ANKARA'
organizationName     :PRINTABLE:'ZT'
organizationalUnitName:PRINTABLE:'MUSTAFA'
commonName           :PRINTABLE:'SERVER'
name                 :PRINTABLE:'MUSTAFA'
emailAddress         :IASSTRING:'mustafa.unsal@ztelemetry.com'
Certificate is to be certified until Dec 13 14:05:10 2032 GMT (3650 days)
Sign the certificate? [y/n]:Y

1 out of 1 certificate requests certified, commit? [y/n]Y
Write out database with 1 new entries
Data Base Updated
```

9. Adım Command 3

- **DH Key Oluşturmak İçin Komut Satırları**

Aşağıdaki bilgiler test amaçlı oluşturulmuştur. Siz kendi bilgilerinizi girerek oluşturmalısınız.


```
Command Prompt
D:\OpenVPN\easy-rsa>build-key client
WARNING: can't open config file: /etc/ssl/openssl.cnf
Loading 'screen' into random state - done
Generating a 1024 bit RSA private key
.....+++++
.....+++++
writing new private key to 'keys\client.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [US]:TR
State or Province Name (full name) [CA]:TURKEY
Locality Name (eg, city) [SanFrancisco]:ANKARA
Organization Name (eg, company) [OpenVPN]:ZT
Organizational Unit Name (eg, section) [changeme]:MUSTAFA
Common Name (eg, your name or your server's hostname) [changeme]:CLIENT
Name [changeme]:MUSTAFA
Email Address [mail@host.domain]:mustafa.unsal@ztelemetry.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:client_secret
An optional company name []:ZT
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Loading 'screen' into random state - done
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName       :PRINTABLE:'TR'
stateOrProvinceName :PRINTABLE:'TURKEY'
localityName      :PRINTABLE:'ANKARA'
organizationName  :PRINTABLE:'ZT'
organizationalUnitName:PRINTABLE:'MUSTAFA'
commonName        :PRINTABLE:'CLIENT'
name              :PRINTABLE:'MUSTAFA'
emailAddress       :IASSTRING:'mustafa.unsal@ztelemetry.com'
Certificate is to be certified until Dec 13 14:09:40 2032 GMT (3650 days)
Sign the certificate? [y/n]:Y

1 out of 1 certificate requests certified, commit? [y/n]Y
Write out database with 1 new entries
```

11. Adım Command 5

NOTE: Bir modeme bağlanacak Client PC sayısı 1 den fazla ise bu işlem tekrarlanır ve client2,client3...

Oluşturduğumuz tüm sertifikalar ve keyler bu klasörde bulunur.

Name	Date modified	Type	Size
01.pem	12/16/2022 5:05 PM	PEM File	5 KB
02.pem	12/16/2022 5:09 PM	PEM File	4 KB
ca	12/16/2022 5:02 PM	Security Certificate	2 KB
ca.key	12/16/2022 5:02 PM	KEY File	1 KB
client	12/16/2022 5:09 PM	Security Certificate	4 KB
client.csr	12/16/2022 5:09 PM	CSR File	1 KB
client.key	12/16/2022 5:09 PM	KEY File	1 KB
dh1024.pem	12/16/2022 5:05 PM	PEM File	1 KB
index	12/16/2022 5:09 PM	Text Document	1 KB
index.txt.attr	12/16/2022 5:09 PM	ATTR File	1 KB
serial	12/16/2022 5:09 PM	File	1 KB
server	12/16/2022 5:05 PM	Security Certificate	5 KB
server.csr	12/16/2022 5:05 PM	CSR File	1 KB
server.key	12/16/2022 5:05 PM	KEY File	1 KB

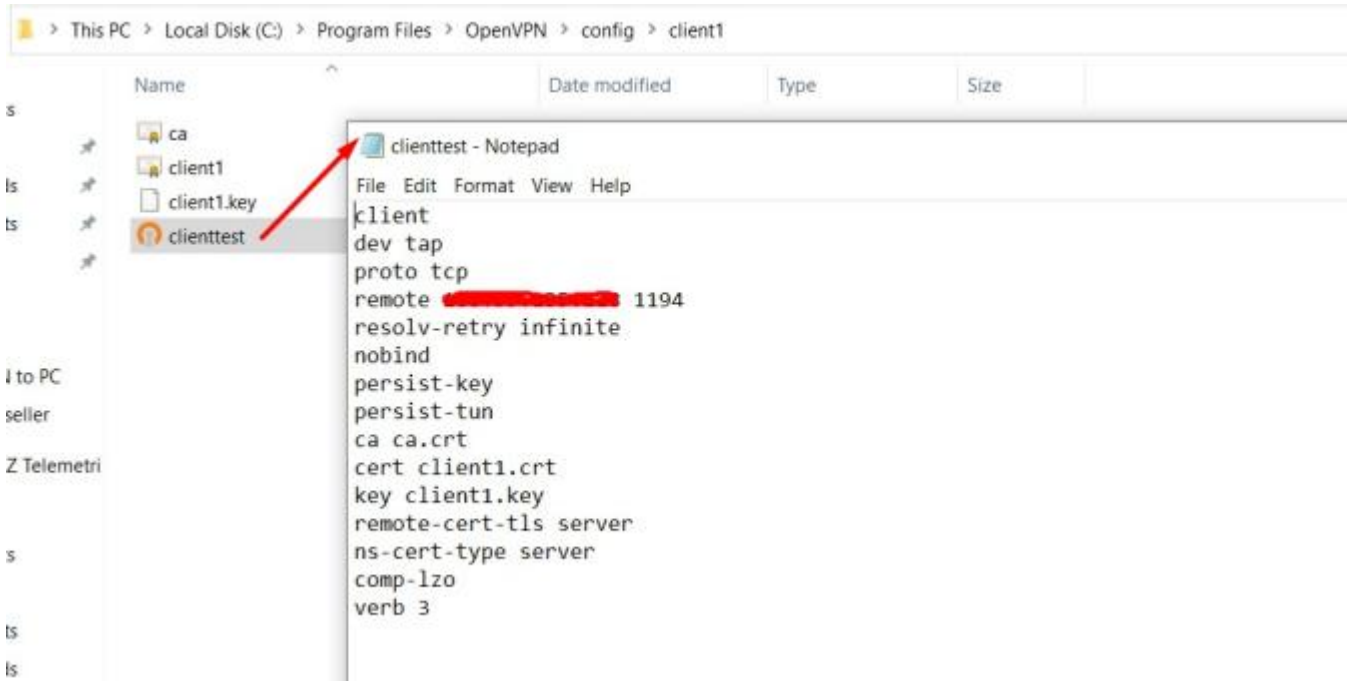
12. Adım Key Klasörü

- Config işlemlerini yapılandırmak için setifikalarımızı kopyalayıp aşağıdaki görselde bulunan dosya konumuna yapıştırıyoruz.

Name	Date modified	Type	Size
bin	11/29/2022 4:52 PM	File folder	
config	12/14/2022 3:58 PM	File folder	
doc	11/29/2022 4:52 PM	File folder	
easy-rsa	11/29/2022 4:52 PM	File folder	
include	11/29/2022 3:35 PM	File folder	
log	12/14/2022 4:00 PM	File folder	
res	11/29/2022 3:35 PM	File folder	
sample-config	11/29/2022 4:52 PM	File folder	
icon	9/27/2016 11:12 AM	Icon	22 KB
license	12/15/2021 8:04 AM	Text Document	28 KB
Uninstall	11/29/2022 4:52 PM	Application	117 KB

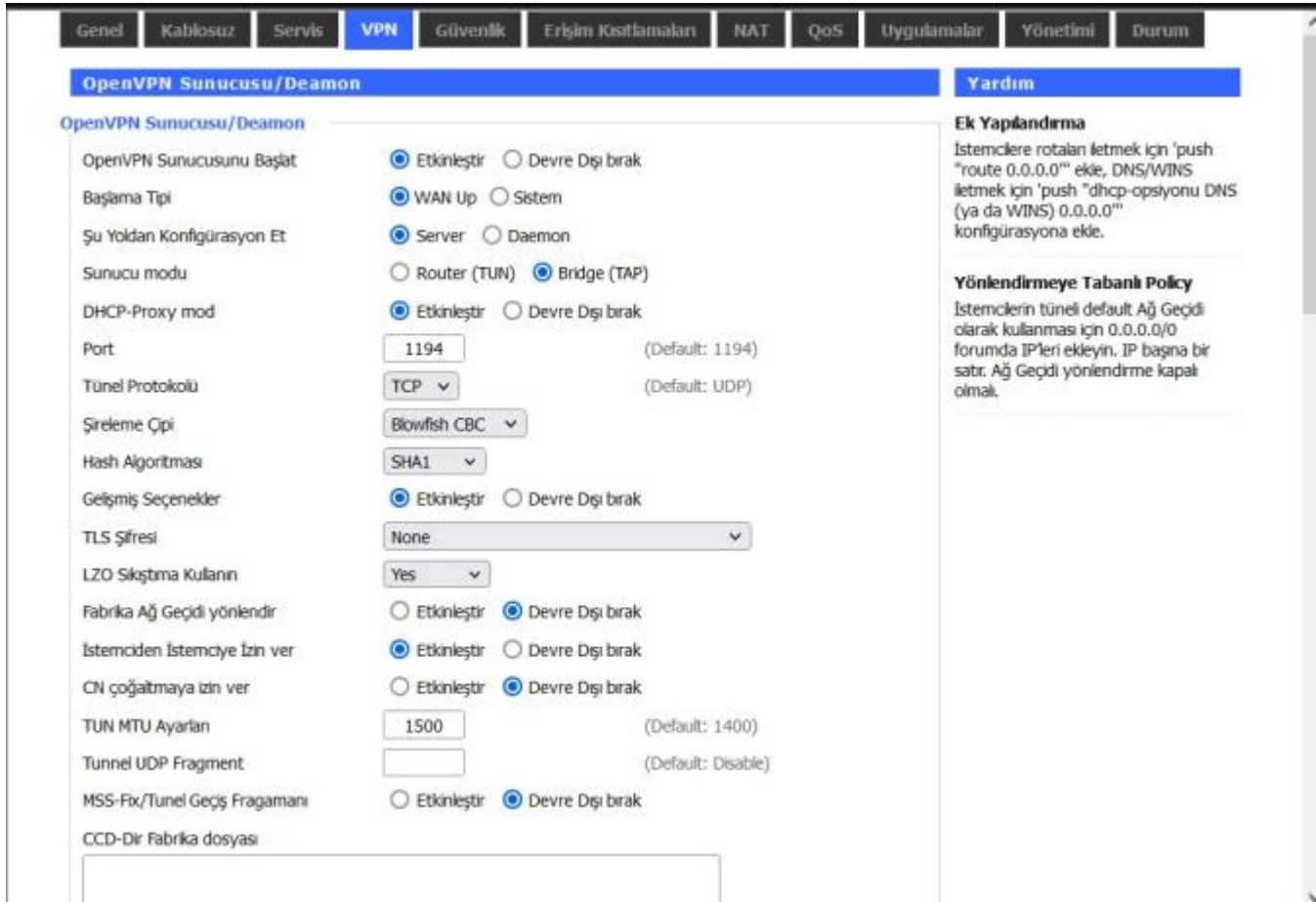
13. Adım Config Klasörü

- PC den modeme bağlantı için client dosyasını yapılandırıyoruz. Kırmızı çizgili kısma modeminize ait statik IP yazılmalıdır.



14. Adım Config Ayarı

- Modem ayarlarını yapılandırılm. OpenVPN Server olarak yapılandırıyoruz.



15. Adım Modem Ayarları-1

- Sertifikaların gerekli yerlerine eklenmesi, sertifikaları eklemek için dosyaları not defteri ile birlikte açıyoruz ve kopyalayıp yapıştırıyoruz.

Empty text input fields for TLS configuration:

- Kamu Sunucu Sertifikası
- CA Sertifikası
- Kişel Sunucu Key
- DH PEM
- Ek Yapılandırma

TLS Doğrulama Şifresi

16. Adım Modem Ayarları-2

File Explorer showing files and their corresponding fields in the modem configuration interface:

Name	Date modified	Type	Size
01.pem	12/16/2022 5:05 PM	PEM File	5 KB
02.pem	12/16/2022 5:09 PM	PEM File	4 KB
ca	12/16/2022 5:02 PM	Security Certificate	2 KB
ca.key	12/16/2022 5:02 PM	KEY File	1 KB
client	12/16/2022 5:09 PM	Security Certificate	4 KB
client.csr	12/16/2022 5:09 PM	CSR File	1 KB
client.key	12/16/2022 5:09 PM	KEY File	1 KB
dh1024.pem	12/16/2022 5:05 PM	PEM File	1 KB
index	12/16/2022 5:09 PM	Text Document	1 KB
index.txt.attr	12/16/2022 5:09 PM	ATTR File	1 KB
serial	12/16/2022 5:09 PM	File	1 KB
server	12/16/2022 5:05 PM	Security Certificate	5 KB
server.csr	12/16/2022 5:05 PM	CSR File	1 KB
server.key	12/16/2022 5:05 PM	KEY File	1 KB

Red arrows indicate the mapping of files to fields:

- ca → Kamu Sunucu Sertifikası
- ca.key → CA Sertifikası
- client.key → Kişel Sunucu Key
- dh1024.pem → DH PEM

17. Adım Sertifika Yazma İşlemi-1

- Sertifikaların modem de yerlerine yazılmış hali.

Static Key

PKCS12 Key

Public Server Cert

```
-----BEGIN CERTIFICATE-----
MIIDxTCCAy6gAwIBAgIBATANBgkqhkiG9w0BAQFADBMQswCQYDVQQG
```

CA Cert

```
-----BEGIN CERTIFICATE-----
MIIDYDCCAsmgAwIBAgIJAPv5J6Hlmag1MA0GC5qGS1b3DQEBBQUAMH4xC
```

Private Server Key

```
-----BEGIN PRIVATE KEY-----
MIICeAIBADANBgkqhkiG9w0BAQEFAASCAmIwggJeAgEAAoGBANLEdMb4E
```

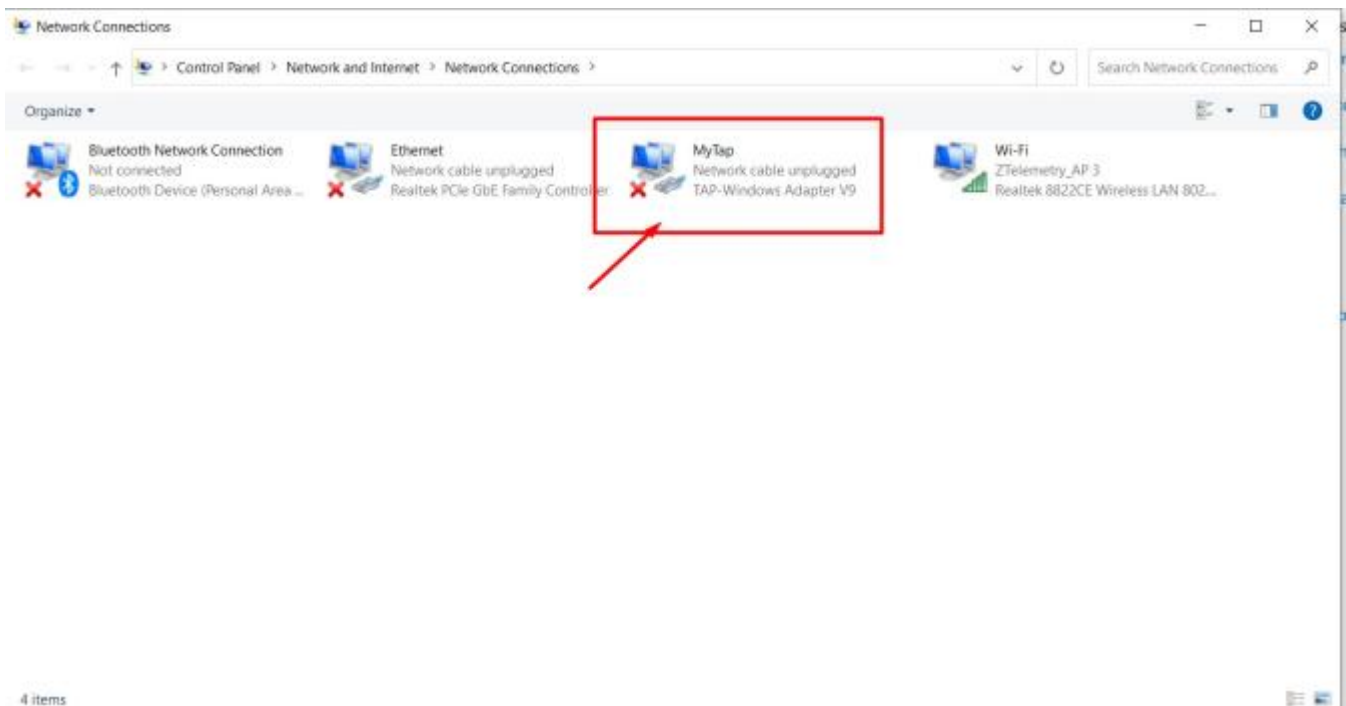
DH PEM

```
-----BEGIN DH PARAMETERS-----
MIGHAoGBAIFDvucSwx/Ruch+12Y1y0+O9H4unCYBVK+kE1B+sqP9VkwrtI0/
```

Additional Config

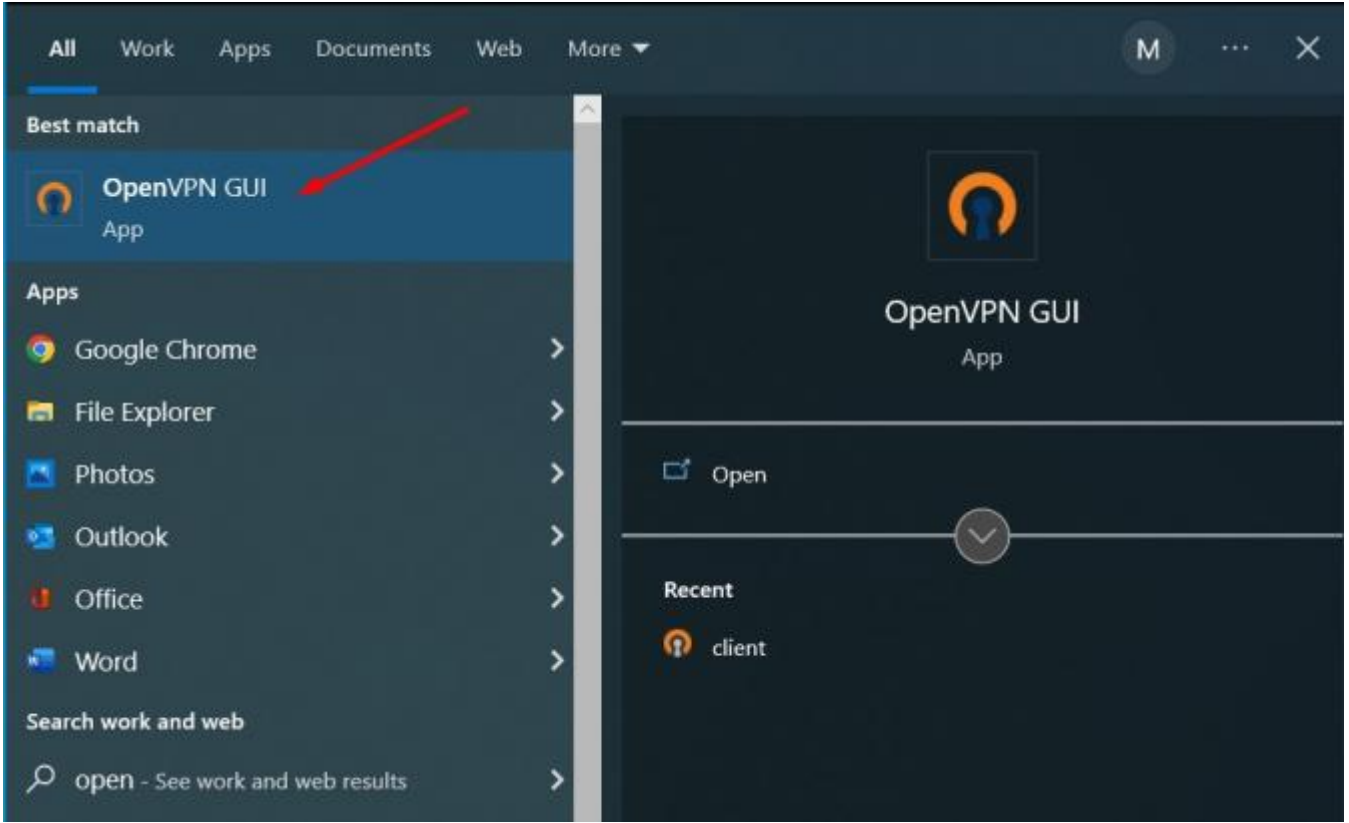
18. Adım Sertifika Yazma İşlemi-2

- PC tarafında OpenVPN bağlantısı için TAP kurulumu yapmalıyız sanal ağ bağdaştırıcısı
“tap-windows-9.21.2”

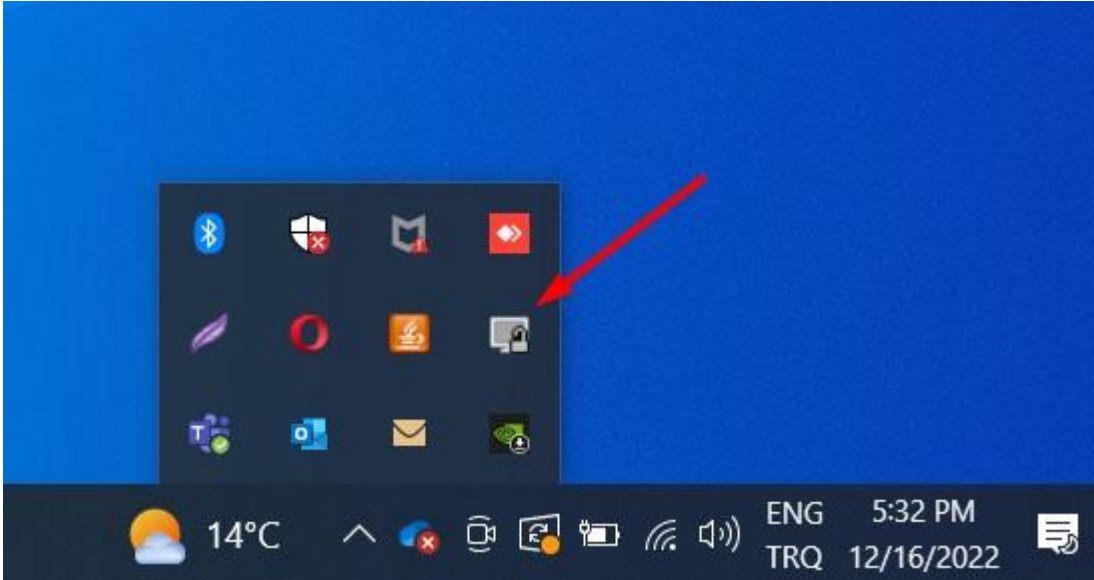


19. Adım Tap Kurulumu

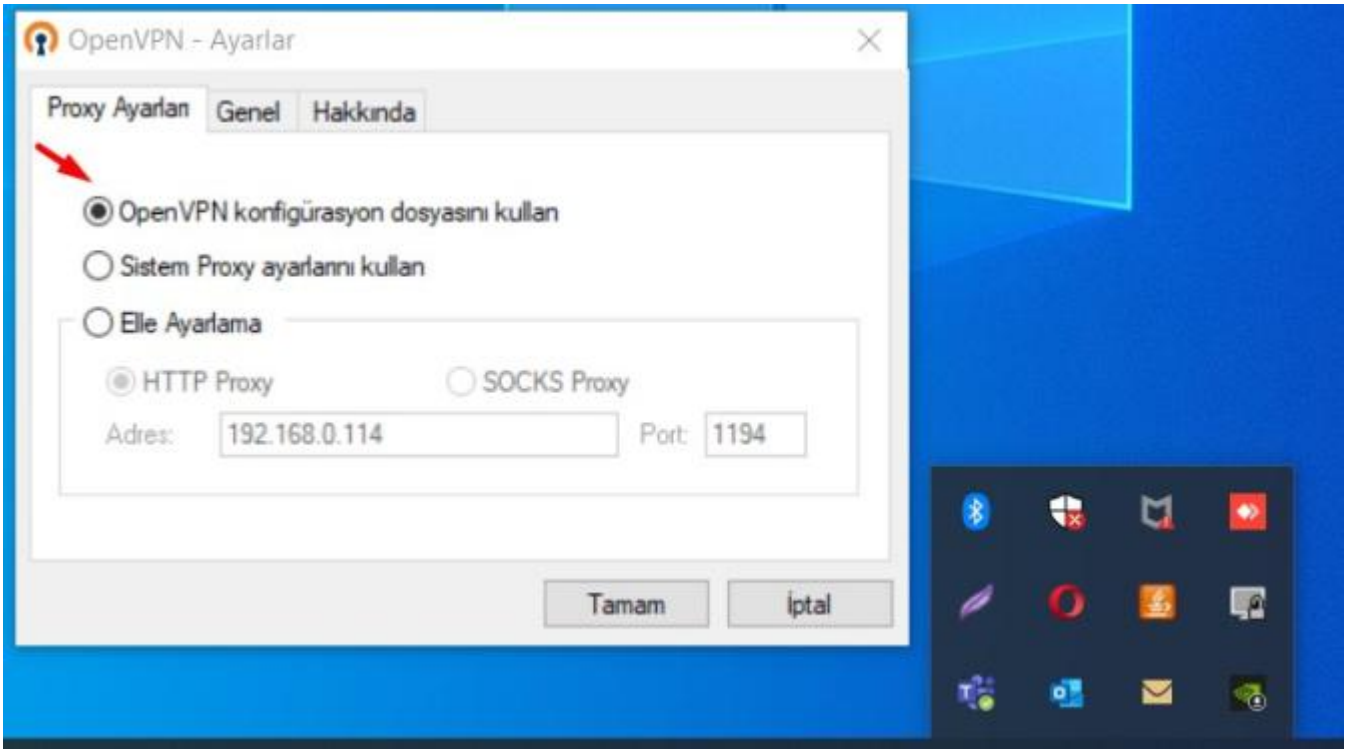
- Tüm ayarlarımız bittikten sonra PC den OpenVPN programını açarak modemimize bağlantı sağlayacağız.



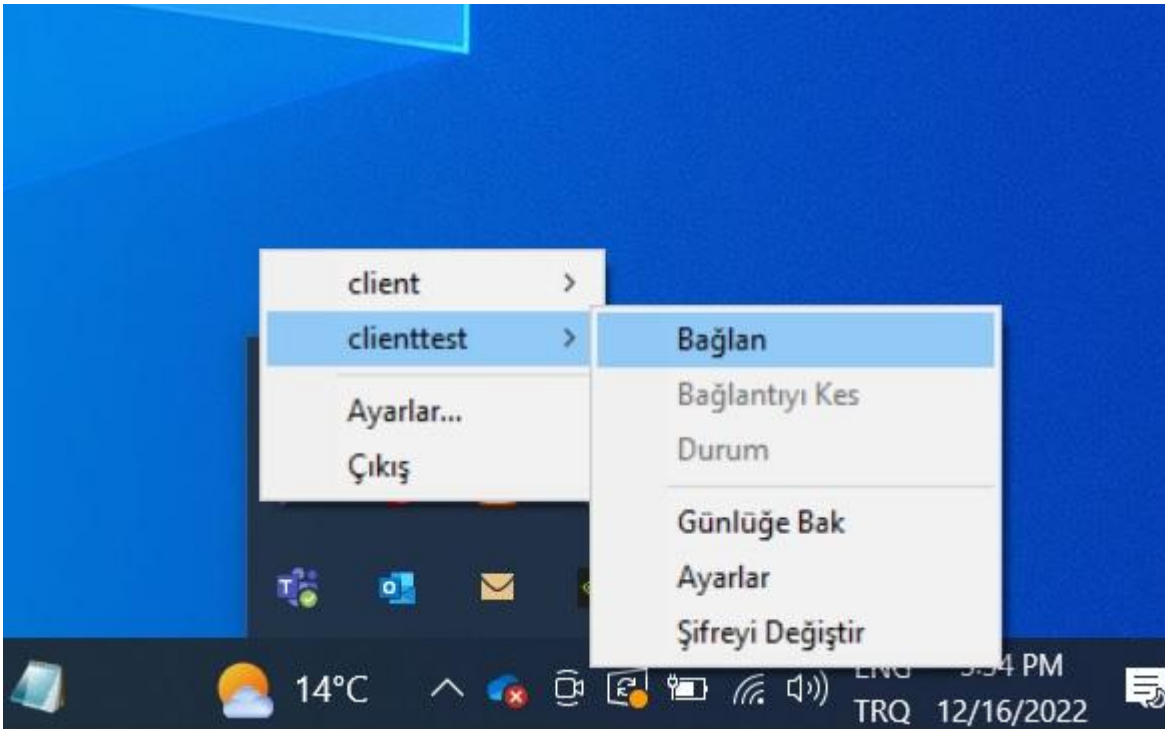
20. Adım OpenVPN Uygulaması Açılması-1



21. Adım OpenVPN Uygulaması Açılması-2



22. Adım OpenVPN Uygulaması Açılması-3



23. Adım OpenVPN Bağlatı Başlatılması

8.5 PPTP Uygulaması

Noktadan noktaya güvenli haberleşme için en yaygın VPN güvenli haberleşme metodlarından biri PPTP olup günümüzde birçok işletim sisteminde yaygın olarak kullanılmaktadır. Şirketimizin sunmuş olduğu Four Faith marka modemler de bu tip, güvenli haberleşme çözümlerini desteklemektedir.

8.5.1 Sunucu Modem Ayarları

Bu uygulamada, biri sunucu biri istemci olmak üzere iki adet F3x26Q Router Modem kullanılmıştır. İhtiyaca göre istemci modem sayısı artırılabilir.

The screenshot displays the configuration page for a Wireless Mobile Router. The page title is "Wireless Mobile Router" and the status bar shows "2. 5G/3G/3. 5G/4G". The firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) stc" with a time of "Zaman: 00:02:56 up 2 min, load average: 0.09, 0.04, 0.01" and WAN IP: "0.0.0.0, BKUP WAN IP: 0.0.0.0".

The main configuration area is titled "PPTP Sunucusu" (PPTP Server). It includes the following settings:

- PPTP Sunucusu: Etkinleştir Devre Dışı bırak
- Yayın Desteği: Etkinleştir Devre Dışı bırak
- MPPE Şifrelemeye Zorla: Etkinleştir Devre Dışı bırak
- DNS1:
- DNS2:
- WINS1:
- WINS2:
- Sunucu IP:
- İstemci IP:
- CHAP-Parola:

Below the PPTP Sunucusu section is the "PPTP İstemcisi" (PPTP Client) section, which has the following setting:

- PPTP İstemci Seçenekleri: Etkinleştir Devre Dışı bırak

At the bottom of the configuration area, there are three buttons: "Kaydet" (Save), "Ayarları Uygula" (Apply Settings), and "Değişiklikleri İptal Et" (Cancel Changes).

Şekil 1. Sunucu Ayarları

Uygulanacak Adımlar

1. "PPTP Sunucu", "Yayın Desteğini" ve "MPPE Şifrelemeye Zorla" etkinleştirin.
2. Sunucu tünel IP'sini belirleyiniz.
3. İstemcilerin IP aralığını belirleyiniz.
4. CHAP Parola kutucuğuna, satır satıra sırasıyla istemcilerin ismi ve şifresini aralara "*" işareti ve birer boşluk koyarak giriniz.

Menü

- Genel Ayarlar
 - Sistem Ayarları
 - DDNS
 - MAC Adres Kopyalama
 - Gelişmiş Yönlendirme
 - Ağ Oluşturma
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Gelişmiş Routing

Çalıştırma Modu

Çalıştırma Modu: Ağ Geçidi

Statik Routing

Set değeri seçin: 1 (İstemci 1) 34

Router Adı: istemci 1

Metrik: 3

Hedef LAN NET: 192, 168, 2, 0

Alt Ağ Maskesi: 255, 255, 255, 0

Ağ Geçidi: 200, 200, 200, 2

Arayüz: ANY

[Routing Tablosunu Göster](#)

[Kaydet](#) [Ayarları Uygula](#) [Değişiklikleri İptal Et](#)

Yardım daha fazla...

Çalıştırma Modu:
Eğer Router sizin internet bağlantınıza yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

Set değeri seçin:
Ekleme yapmayan Router sayıdır, en fazla 50 ayarlanabilir.

Router Adı:
Router'a vermek istediğiniz adı giriniz.

Hedef LAN NET:
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.

Alt Ağ Maskesi:
Ağ ve Host bölümlerini belirler.

Şekil 2. Sunucu Gelişmiş Yönlendirme Ayarları

Uygulanacak Adımlar

1. Sunucu modem Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modemin adını giriniz.
3. İstemci modemin sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modemin tünel IP adresini giriniz.

Sunucu modem ayarlarını tamamladıktan sonra istemci modem ayarlarına geçebilirsiniz.

8.5.2 İstemci Modem Ayarları

İstemci modem ayarlarını VPN menüsü altından PPTP seçeneğinden yapabilirsiniz. Kutucuklarda belirtilen ayarlar uygulamanıza özel olup diğer ayarları şekildeki gibi giriniz.



The screenshot displays the configuration interface for a Wireless Mobile Router. The page title is "Wireless Mobile Router" and the firmware version is "F3x26Q v1.1 (Sep 15 2023 12:36:09) std". The current time is "Zaman: 15:25:18 up 15 min, load average: 0.00, 0.01, 0.03" and the WAN IP is "WAN IP: 192.168.0.116, BKUP WAN IP: 0.0.0.0". The page is divided into a left sidebar menu and a main content area. The sidebar menu includes "Genel Ayarlar", "Kablosuz", "Servis", "VPN", "Güvenlik", "Erişim Kısıtlamaları", "NAT", "QoS Ayarları", "Uygulamalar", "Sistem Yönetimi", and "Durum". The main content area is titled "PPTP Sunucusu" and "PPTP İstemcisi". The "PPTP Sunucusu" section has a "PPTP Sunucusu" field and two radio buttons: "Etkinleştir" (selected) and "Devre Dışı bırak". The "PPTP İstemcisi" section has a "PPTP İstemci Seçenekleri" field with two radio buttons: "Etkinleştir" (selected) and "Devre Dışı bırak". Below this are several input fields: "Sunucu IP'si ya da DNS Adı" (188.59.158.246), "Uzak Subnet" (192, 168, 1, 1), "Uzak Alt Ağ Maskesi" (255, 255, 255, 0), "MPPE Şifreleme" (mppe stateless), "MTU" (1450, Default: 1450), "MRU" (1450, Default: 1450), "NAT" (Etkinleştir selected), "Sabit IP" (Devre Dışı bırak selected), "Kullanıcı Adı" (istemci1), and "Şifre" (masked with asterisks). There is a "Göster" checkbox next to the password field. At the bottom of the page, there are three buttons: "Kaydet", "Ayarları Uygula", and "Değişiklikleri İptal Et".

Şekil 3. İstemci Ayarları

Uygulanacak Adımlar

1. PPTP istemci ayarlarını enable ediniz.
2. Sırasıyla sunucu modem WAN IP'si, sunucu modem LAN IP'si ve subnet mask'ını giriniz.
3. İstemci modem ismi ve şifresini giriniz.

192.168.2.1/Routing.asp

Four-Faith Wireless Mobile Router 2.5G/3G/3.5G/4G

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) std
Zaman: 15:25:01 up 15 min, load average: 0.00, 0.01, 0.03
WAN IP: 192.168.0.116, BKUP WAN IP: 0.0.0.0

Menü

- Genel Ayarlar
 - Sistem Ayarları
 - DDNS
 - MAC Adres Kopyalama
 - Gelişmiş Yönlendirme
 - Ağ Oluşturma
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum

Gelişmiş Routing

Çalıştırma Modu

Çalıştırma Modu: Ağ Geçidi

Statik Routing

Set değeri seçin: 1 (sunucu1) Sil

Router Adı: sunucu1

Metrik: 0

Hedef LAN NET: 192.168.1.0

Alt Ağ Maskesi: 255.255.255.0

Ağ Geçidi: 200.200.200.1

Arayüz: ANY

Routing Tablosunu Göster

Kaydet Ayarları Uygula Değişiklikleri İptal Et

Yardım daha fazla...

Çalıştırma Modu:
Eğer Router sizin internet bağlantınızı yönetiyorsa, Ağ Geçidi modunu seçin. Eğer ağınızda başka router varsa, Router modunu seçin.

Set değeri seçin:
Eşleşmeyen Router sayıdır, en fazla 50 ayarlanabilir.

Router Adı:
Router'a vermek istediğiniz adı giriniz.

Hedef LAN NET:
Statik Route yapmak istediğiniz ağın lokal IP bloğudur.

Alt Ağ Maskesi:
Ağ ve Host bölümlerini belirler.

Şekil 4. İstemci Gelişmiş Yönlendirme Ayarları

Uygulanacak Adımlar

1. Sunucu modemini Gelişmiş Routing ayarlarında Çalıştırma Modu için "Ağ Geçidi" seçiniz.
2. Advance routing yapacağınız birinci istemci modemini adını giriniz.
3. İstemci modemini sırasıyla LAN IP'si, Alt Ağ Maskesi ve istemci modemini tünel IP adresini giriniz.

8.5.3 Bağlantı Testi

Sunucu ve istemci ayarlarını tamamladıktan sonra bağlantı testine geçebilirsiniz.

Four-Faith  Wireless Mobile Router

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) str
Zaman: 14:42:50 up 3 min, load average: 0.01, 0.03, 0.01
WAN IP: 188.59.158.246, BKUP WAN IP: 0.0.0.0

2. 5G/3G/3. 5G/4G

Menü

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
- Durum**
- Router
- WAN
- LAN
- Kablosuz
- Cihaz Yönetimi
- Akıllı Kapı Durumu
- Bant Genişliği
- Sistem Bilgisi

Yerel Ağ

LAN Durumu

MAC Adres	54:D0:B4:37:CC:8E
Yerel IP	192.168.1.1
Alt Ağ Maskesi	255.255.255.0
Ağ Geçidi	0.0.0.0
Yerel DNS	0.0.0.0

Aktif İstemciler

Host Adı	Yerel IP	MAC Adres	Bağl. Sayım	Oran [16384]
- Hiçbiri -				

Dynamic Host Configuration Protocol (DHCP)


DHCP Durumu

DHCP Sunucusu	ETKİN
DHCP Daemon	DNSMasq
Başlangıç IP Adresi	192.168.1.100
Bitiş IP Adresi	192.168.1.149
İstemci Kira Süresi	1440 dakika

DHCP İstemcileri

Host Adı	Yerel IP	MAC Adres	İstemci Kira Süresi	Sil
- Hiçbiri -				

PPTP İstemcileri Bağlandı

Arayüz	Kullanıcı Adı	Uzak Tünel IP	Uzak IP	Sil
ppp0	istemci1	200.200.200.2	78.175.54.236	

[Yeni İstemci Ekle](#)

Yardım daha fazla...

MAC Adresi:
Yerel, Ethernet ağında görüldüğü gibi bu Router'in MAC adresidir.

Yerel IP:
Yerel, Ethernet ağında görüldüğü gibi bu Router'in IP adresini gösterir.

Alt Ağ Maskesi:
Router bir Alt Ağ Maskesi kullandığında, o burda gösterilir.

DHCP Sunucusu:
Eğer Router'i DHCP sunucusu olarak kullanıyorsanız, burada görüntülenir.

OUI Search:
Herhangi bir MAC adresine tıklayarak, ağ arayüzünün Organizationally Unique Identifier (OUI) sini göreceksiniz. (IEEE Standards OUI database search).

Şekil 5. Bağlantı Testi

Sunucu modemini istemci modemle ve sunucu modemle olan PPTP bağlantısını "PPTP İstemcileri Bağlandı" sekmesinden kontrol edebilirsiniz.

Son olarak sunucu ve istemci modemleri iki taraflı olarak LAN IP adreslerinden pingleyerek güvenli PPTP bağlantısının kurulduğunu doğrulayabilirsiniz

192.168.2.1/apply.cgi

Four-Faith Wireless Mobile Router 2.5G/3G/3.5G/4G

Firmware: F3x26Q v1.1 (Sep 15 2023 12:36:09) stc
Zaman: 15:14:12 up 4 min, load average: 0.00, 0.01, 0.01
WAN IP: 192.168.0.116, BKUP WAN IP: 0.0.0.0

Menü

- Genel Ayarlar
- Kablosuz
- Servis
- VPN
- Güvenlik
- Erişim Kısıtlamaları
- NAT
- QoS Ayarları
- Uygulamalar
- Sistem Yönetimi
 - Yönetim
 - Canlı Tutma
 - Komut
 - Fabrika Ayarları
 - Firmware Güncelleme
 - Konfigürasyon
 - Yedekleme
- Durum

Komut Sayfası

Komut Satırı

Komutlar

```
ping 192.168.1.1
```

```
PING 192.168.1.1 (192.168.1.1): 56 data bytes  
64 bytes from 192.168.1.1: seq=0 ttl=64 time=303.841 ms  
64 bytes from 192.168.1.1: seq=1 ttl=64 time=55.040 ms  
64 bytes from 192.168.1.1: seq=2 ttl=64 time=52.921 ms  
--- 192.168.1.1 ping statistics ---  
3 packets transmitted, 3 packets received, 0% packet loss  
round-trip min/avg/max = 52.921/137.067/303.841 ms
```

Yardım daha fazla...

Komutlar:
Komut satırlarını web arayüzünden çalıştırabilirsiniz. Metin alanına komutunuzu yazın ve göndermek için Komutu Çalıştır butonuna tıklayın.

Komutu Çalıştır

Şekil 6. Ping Testi

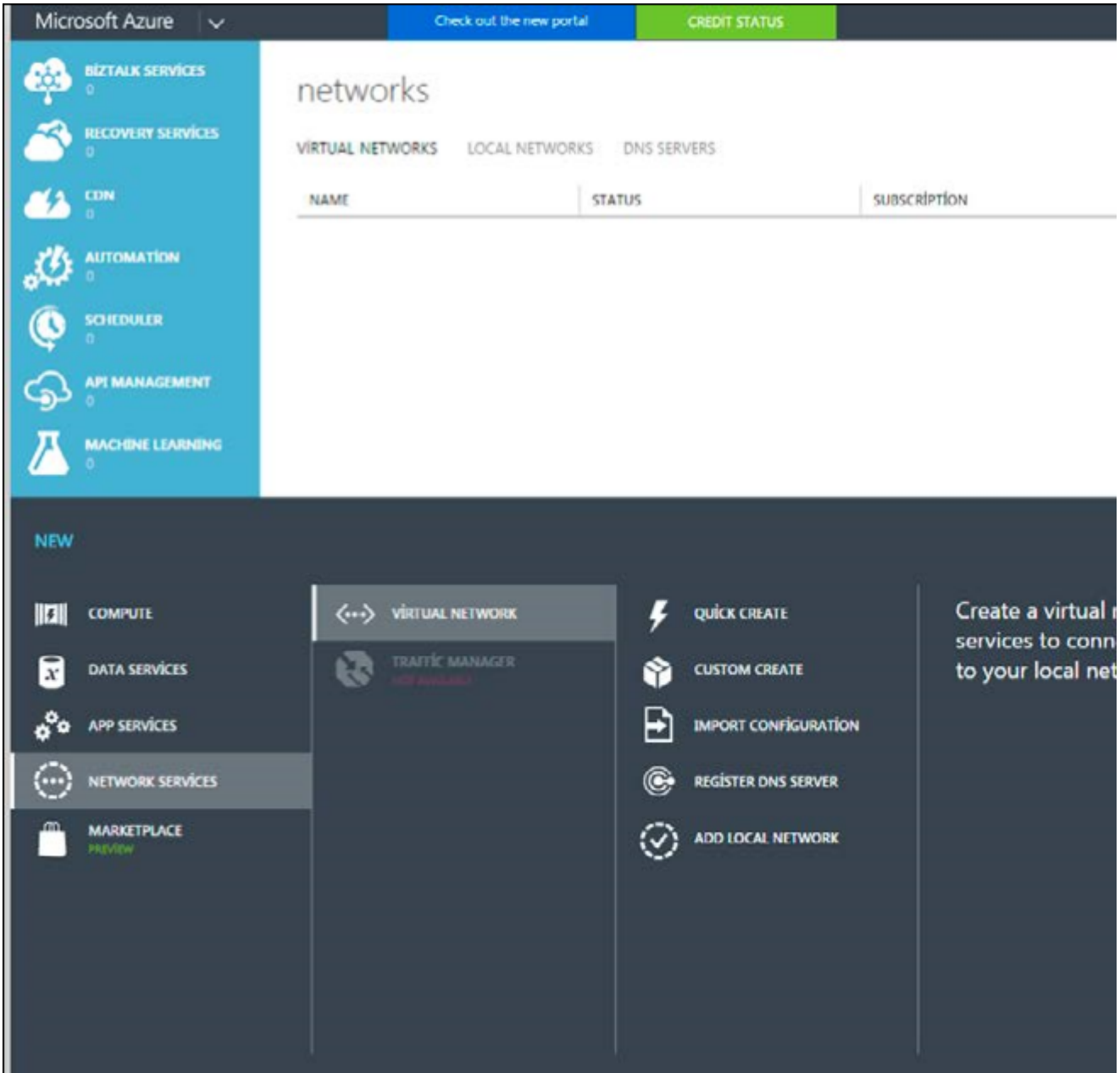
8.6 Azure VPN Uygulaması

8.6.1 Açıklama

Bulut tabanlı sistemlerin yaygınlaşması ile çeşitli halka açık ve ücretsiz profesyonel platformlar hizmete girmiştir. Microsoft Azure da bu konuda en uygun çözümlerden biridir. Microsoft Azure ile siteden siteye ve noktadan siteye güvenli bağlantı kurmak için şirketimizin sunmuş olduğu Four Faith marka Router ve Modemler bu tip güvenli haberleşme çözümlerinde, VPN istemci tarafında ilgili ihtiyacı rahatlıkla karşılamaktadır.

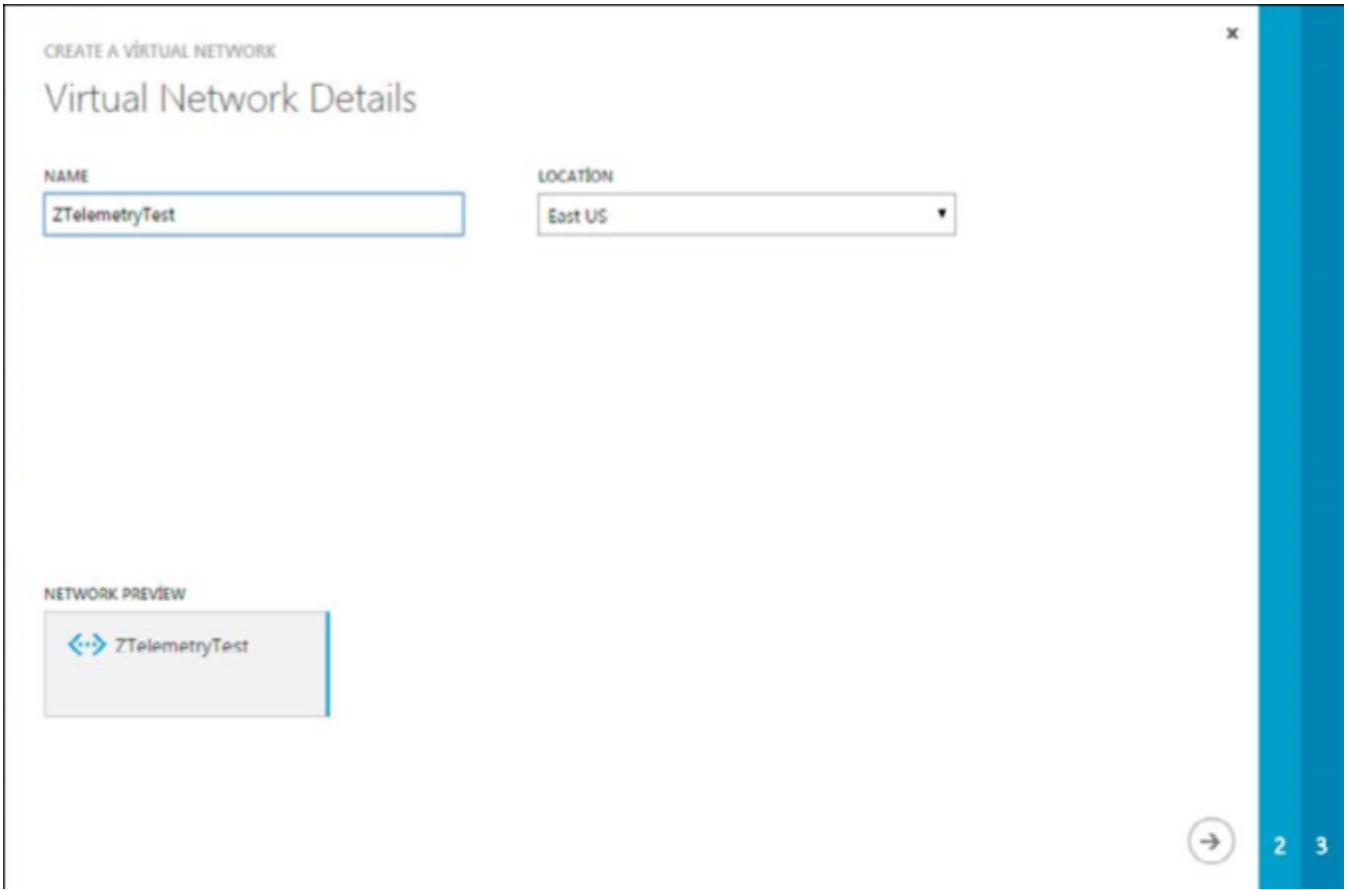
8.6.2 MS Azure Ayarları

<https://manage.windowsazure.com/> adresine gidip Microsoft Azure hesabınıza giriş yaptıktan sonra Azure VPN ayarlarını yapmaya başlayabilirsiniz. Bu uygulamada Azure tarafı VPN Sunucu, Four Faith Router tarafı ise VPN İstemci olarak belirlenmiştir.



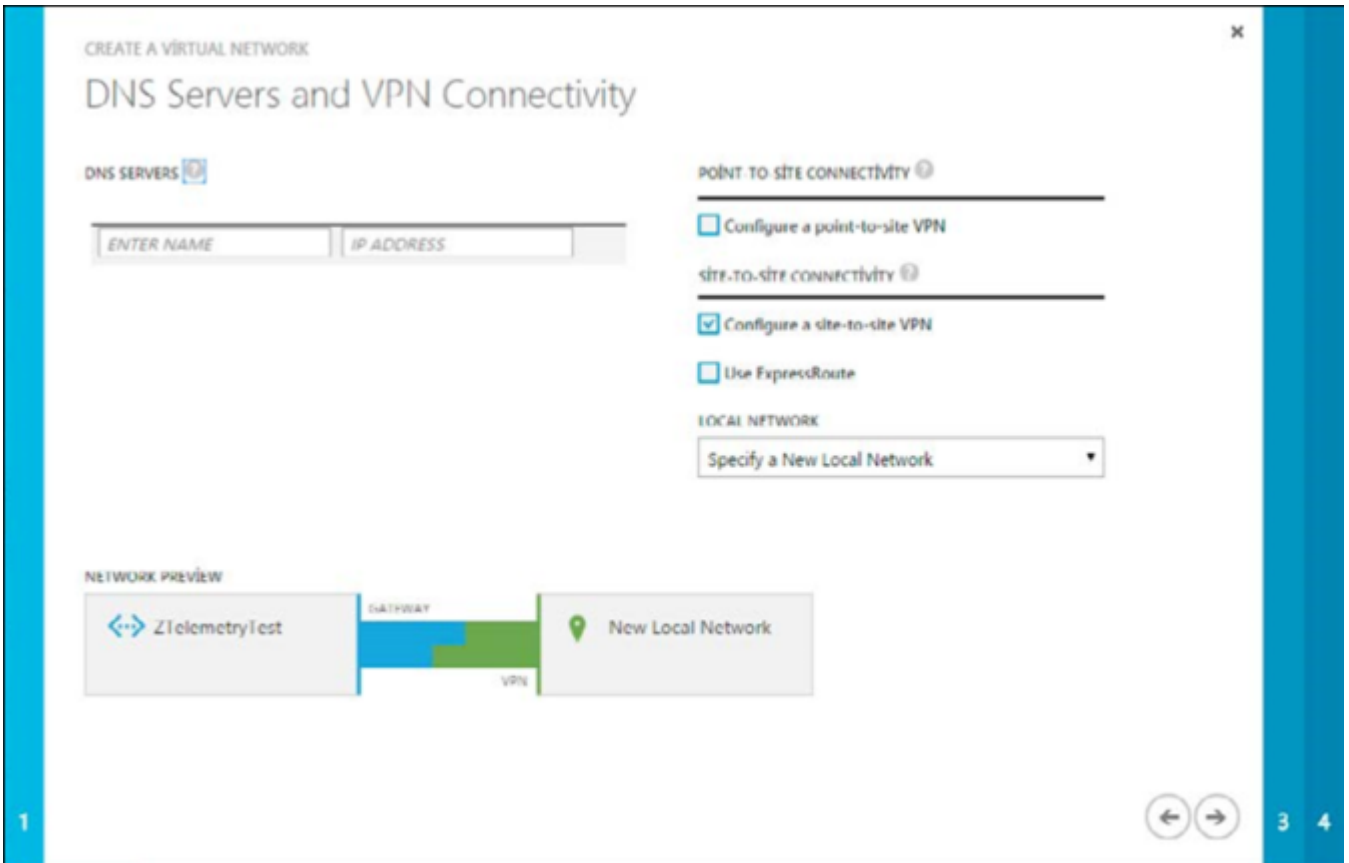
Şekil 1. Azure VPN Giriş Ekranı

- Sırasıyla; Network Services, Virtual Network ve Custom Create seçeneklerine tıklayarak sanal ağınıza yaratınız.



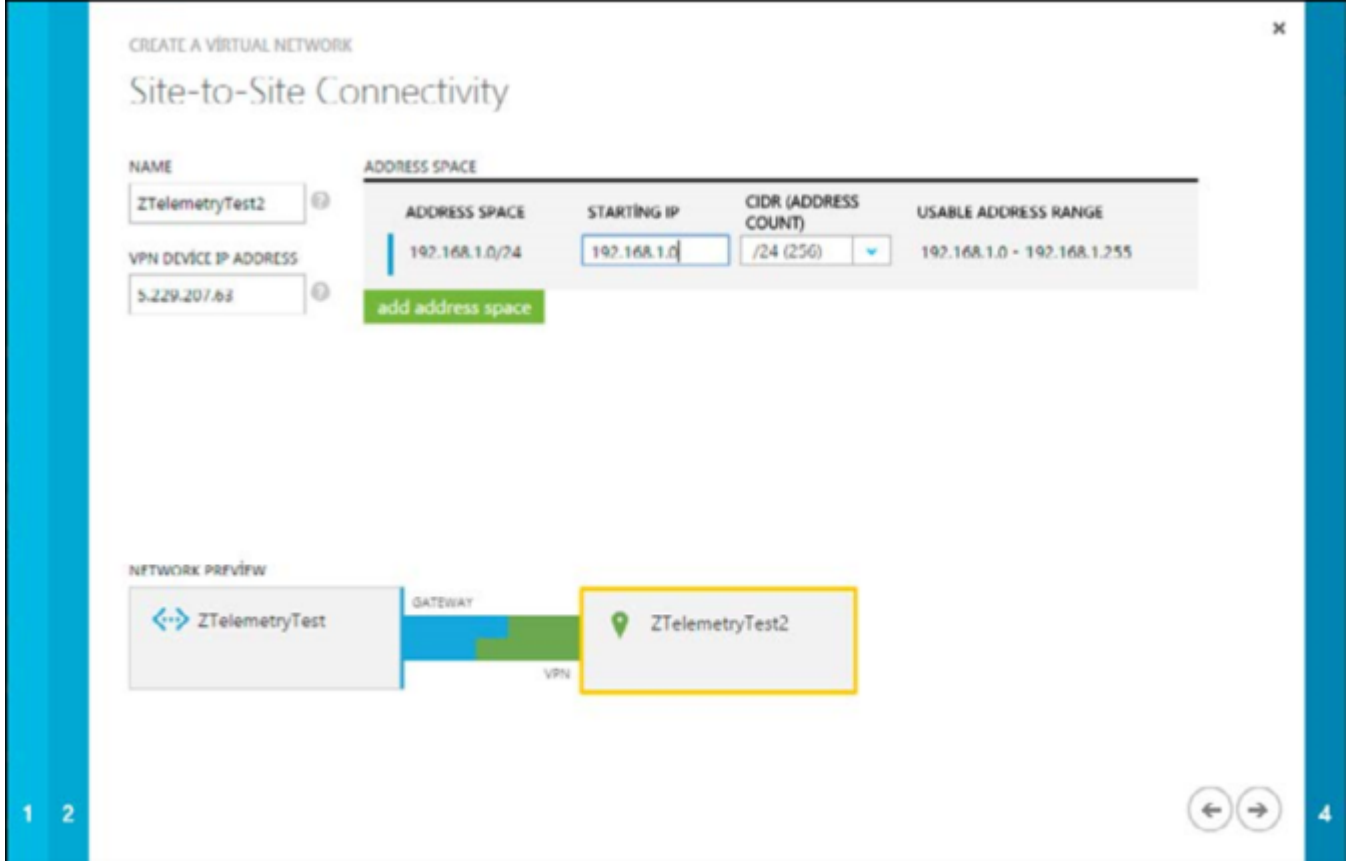
Şekil 2. Azure VPN Ayarları 1

- Yarattığınız sanal ağın ismini giriniz.
- Bulduğunuz bölgeyi seçiniz.
- Bu sayfadaki ayarları tamamladıktan sonra ileri butonuna basınız.



Şekil 3. Azure VPN Ayarları 2

- Yeni bir yerel ağ belirlemek için ilgili seçeneği seçiniz.
- Bu sayfadaki ayarları tamamladıktan sonra ileri butonuna basınız.



Şekil 4. Azure VPN Ayarları 3

- Bağlantı için bir isim belirleyiniz.
- Four Faith modem, yani VPN istemci tarafın WAN IP'sini giriniz.
- Four Faith modem, yani VPN istemci tarafın LAN subnet adresini giriniz.
- Bu sayfadaki ayarları tamamladıktan sonra ileri butonuna basınız.

CREATE A VIRTUAL NETWORK

Virtual Network Address Spaces

ADDRESS SPACE	STARTING IP	CIDR (ADDRESS COUNT)	USABLE ADDRESS RANGE
10.4.0.0/16	10.4.0.0	/16 (65536)	10.4.0.0 - 10.4.255.255

SUBNETS

Subnet-1	10.4.2.0	/24 (256)	10.4.2.0 - 10.4.2.255
Subnet-2	10.4.3.0	/24 (256)	10.4.2.0 - 10.4.3.255
Gateway	10.4.1.0	/24 (256)	10.4.1.0 - 10.4.1.255

add subnet add gateway subnet

add address space

NETWORK PREVIEW

The network preview shows a connection between ZTelemetryTest and ZTelemetryTest2. A Gateway is connected to ZTelemetryTest, and a VPN is connected to ZTelemetryTest2. The Gateway and VPN are connected to each other.

Şekil 5. Azure VPN Ayarları 4

- Azure tarafı subnet adresini giriniz.
- Birden çok subnet adresi girebilirsiniz. Azure için ilgili gateway adresini giriniz.
- Bu sayfadaki ayarları tamamladıktan sonra ilgili buton ile sanal ağ ayarlarını tamamlayınız.

Microsoft Azure

Check out the new portal. CREDIT STATUS delphsonic@outlook.com

ztelemetrytest

DASHBOARD CONFIGURE CERTIFICATES

virtual network

ZTelemetryTest

ZTelemetryTest2

GATEWAY VPN

THE GATEWAY WAS NOT CREATED.

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME	
------	------	------------	-------------	--

quick glance

Download VPN Device Script

STATUS
Created

SUBSCRIPTION ID
73111f13-3a07-434e-aeed-d4562eb90c1

VIRTUAL NETWORK ID
02f39606-d371-48c4-a40e-e395d6dd540d

LOCATION
East US.

+ NEW

CREATE GATEWAY EXPORT DELETE

1 1 ?

Şekil 6. Azure VPN Ayarları 5

- Gateway yaratmak için ilgili butona basınız.
- Gateway için Static Routing'i seçip işleme başlayınız. Bu işlem yaklaşık 15 dakika sürecektir.

Microsoft Azure | Check out the new portal | CREDIT STATUS | delphionic@outlook.com

ztelemetrytest

DASHBOARD CONFIGURE CERTIFICATES

virtual network

ZTelemetryTest

ZTelemetryTest2

DATA IN: 0B | DATA OUT: 0B | GATEWAY IP ADDRESS: 13.68.208.239

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
------	------	------------	-------------

quick glance

Download VPN Device Script

STATUS: Created

SUBSCRIPTION ID: 73111f13-3b97-434c-aeed-04562eb9f2c1

VIRTUAL NETWORK ID: 02f396f6-d371-46c4-a40e-e305d6dd540d

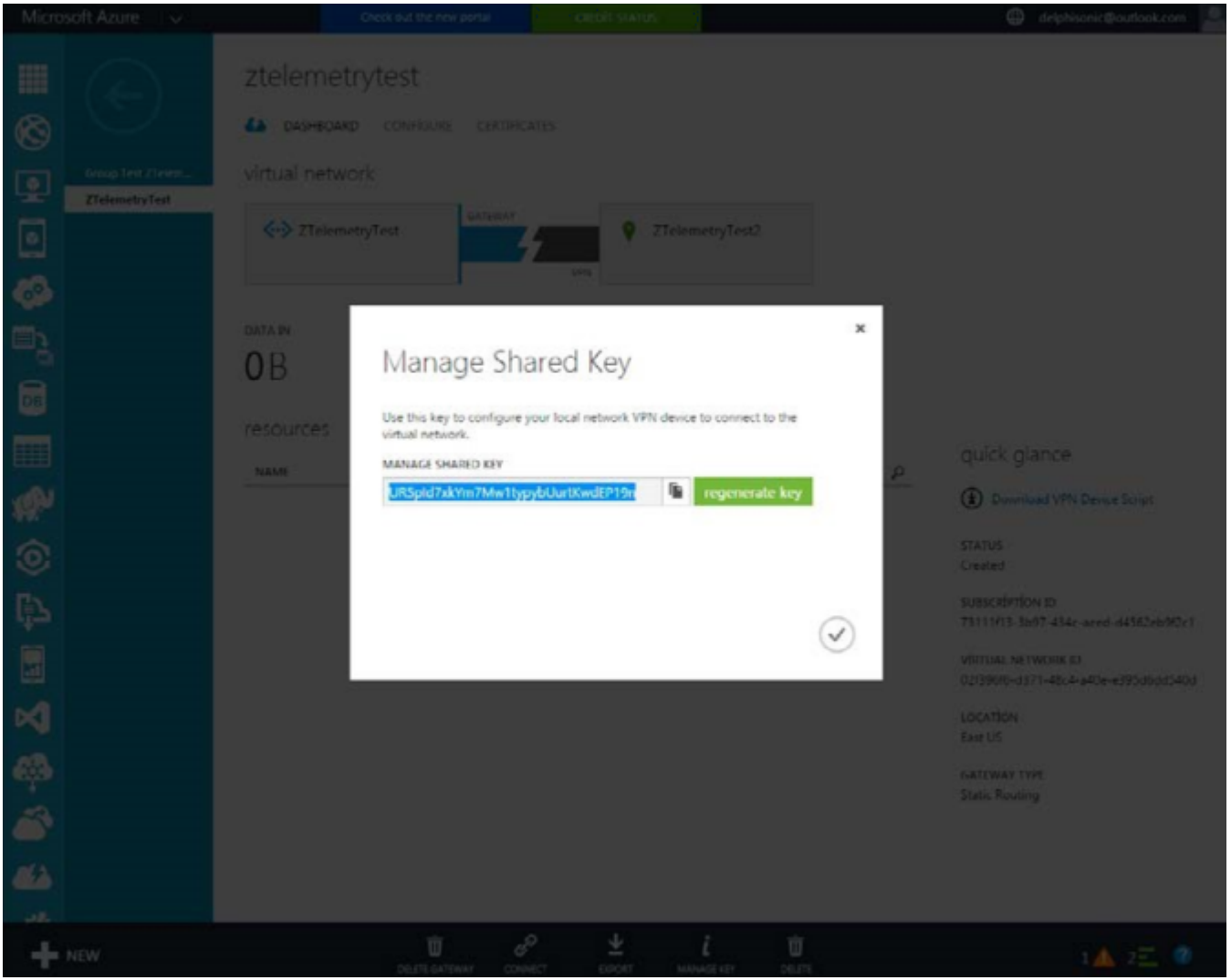
LOCATION: East US

GATEWAY TYPE: Static Routing

+ NEW | DELETE GATEWAY | CONNECT | EXPORT | MANAGE KEY | DELETE

Şekil 7. Azure VPN Ayarları 6

- Gateway yaratma işlemini tamamladıktan sonra önceden belirlenmiş Pre-Shared Key'e erişmek için ilgili butona tıklayınız.



Şekil 8. Azure VPN Ayarları 7

- Pre-Shared Key'i kaydediniz.

8.6.3 İstemci Ayarları

Azure ayarlarını tamamladıktan sonra VPN istemci tarafı olan Four Faith Router ayarlarına geçebilirsiniz. Ayarları yapmaya başlamadan önce Four Faith marka Routerınıza uygun firmware'i yüklediğinizden ve internet bağlantı ayarlarını yaptığınızdan emin olunuz.

Menu

- Setup
- Wireless
- Services
- VPN
- Security
 - Firewall
- Access Restrictions
- NAI
- QoS Setting
- Applications
- Administration
- Status

Security

Firewall Protection

SP1 Firewall Enable Disable

Additional Filters

- Filter Proxy
- Filter Cookies
- Filter Java Applets
- Filter ActiveX

Block WAN Requests

- Block Anonymous WAN Requests (ping)
- Filter IDENT (Port 113)
- Block WAN SNMP access

Impede WAN DoS/Brute-force

- Limit SSH Access
- Limit Telnet Access
- Limit PPTP Server Access
- Limit L2TP Server Access

Log Management

Log

Log Enable Disable

Save Apply Settings Cancel Changes

Help

Firewall Protection:
Enable or disable the SP1 fir

Şekil 9. İstemci VPN Ayarları 1

- Güvenlik duvarını disable ediniz.

Menu

- Setup
- Wireless
- Services
- VPN**
 - o PPTP
 - o L2TP
 - o OPENVPN
 - o IPSEC
 - o GRE
- Security
- Access Restrictions
- NAT
- QoS Setting
- Applications
- Administration
- Status

Type

Type: Net-to-Net Virtual Private Network

IPSEC role: Client Server

Connection

Connection: Azure

Name: Azure	Enabled: <input checked="" type="checkbox"/>
Local WAN Interface: WAN	Peer WAN address: 13.68.208.239
Local Subnet: 192.168.1.0/24	Peer subnet: 10.4.0.0/16
Local Id: 5.229.207.63	Peer ID: 13.68.208.239

Detection

Detection

Enable DPD Detection:

Time Interval: 60 (s) Timeout: 60 (s) Action: restart

Advanced Settings

Advanced Settings

Enable advanced settings:

Phase 1

IKE Encryption: 3DES IKE Integrity: SHA1 IKE Group type: Group2(1024)

IKE Lifetime: 0 hours

Phase 2

ESP Encryption: 3DES ESP Integrity: SHA1 ESP Group type: NULL

ESP Key life: 1 hours

IKE aggressive mode allowed. Avoid if possible (pre-shared key is transmitted in clear text)

Perfect Forward Secrecy (PFS)

Authentication

Authentication

Use a Pre-Shared Key: URSpId7xkYm7Hw1tYpYb

Generate and use the X.509 certificate

Help more...

Type
Select the type of ipsec, tunnel or transport

Role
Select the role of ipsec, client or server

Name of the connection
the name of the ipsec connection, up to 20 characters

ID for local and remote endpoint
Can be an IP address (in any ipsec_idname(3) syntax) or a fully-qualified domain name preceded by @

PSK Value
The length of Psk Value can not be more than 30

Şekil 10. İstemci VPN Ayarları 2

- Kullanacağınız bağlantı tipini Net-to-Net Virtual Private Network olarak belirleyiniz ve router'istemci olarak ayarlayınız.
- IPSEC bağlantı ismini giriniz.
- İstemci lokal ağ adresini yazınız.
- Lokal ağı simgeleyen bir IP adresi yazabilirsiniz.
- Sunucunun WAN adresini giriniz.
- Sunucu lokal ağ adresini yazınız.
- Sunucunun ağını simgeleyen bir IP adresi yazabilirsiniz.
- Faz-1 ve Faz-2 ayarlarını giriniz.
- Azure ayarlarında kaydettiğiniz Pre-Shared Key'i belirtilen kısma giriniz.


8.6.4 Bağlantı Testi

Four Faith Router ve Azure tarafındaki VPN ayarlarını tamamladıktan sonra iki tarafta da güvenli IPSEC bağlantısının başarıyla sağlandığını görebilirsiniz.

ztelemetrytest

DASHBOARD CONFIGURE CERTIFICATES

virtual network



DATA IN: 0B
DATA OUT: 280B
GATEWAY IP ADDRESS: 13.68.208.239

resources

NAME	ROLE	IP ADDRESS	SUBNET NAME
------	------	------------	-------------

Global settings

Global settings





Enable NAT-Traversal

Debug Level: None

Save

Connection status and control

Connection status and control

Num	Name	Type	Common Name	Status	Action
1	Azure	Tunnel-client	192.168.1.6/24-[WAN] 13.68.208.239-[10.4.0.0/16]	ESTABLISHED	   

add

Şekil 11. Bağlantı Testi

