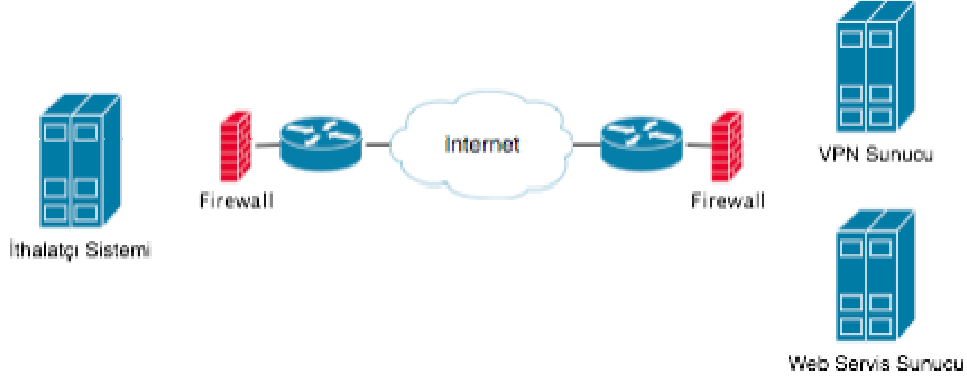


Web Servis-Web Sitesi Bağlantısı

MCKS İthalatçı web servisleri internet üzerinden güvenli şekilde erişime açılmıştır. Erişime ait ağ bağlantısı aşağıda şematik olarak gösterilmiştir.



Şekil - 1: MCKS-ithalatçı web servis ağ bağlantısı

Web servislerine erişmek için ithalatçı tarafından MCKS bünyesinde kullanılan VPN yazılımının istemcisinin kurulması gerekmektedir. Kurulumun tamamlanması ardından Telekomünikasyon Kurumu tarafından şu bilgiler sağlanacaktır.

- 1- VPN istemci güvenlik sertifikası
- 2- VPN istemci kullanıcı adı ve şifresi
- 3- VPN istemci IP adresi.
- 4- Web servis erişim anahtarı

VPN sistemi internet üzerinden gerçekleşen trafiği kriptolu hale getirerek transfer edilen veriye erişimi engellemektedir.

Ağ bağlantısının sağlanması ardından web servislerine standart SOAP yöntemi ve HTTPS protokolü üzerinden erişilir.

Her ithalatçı için bir adet VPN bağlantı seti sağlanmaktadır. Eğer ithalatçı bünyesinde birden fazla sunucu web servislere erişecek ise, VPN sunucusu yerel ağ üzerinde yönlendirme yapabilecek şekilde yapılandırılmalıdır. Yerel ağ kaynakları üzerinde VPN konfigürasyon dosyalarında yer alan IP adres grubuna yönlendirme (routing) yapılmalıdır. Bu konu ile ilgili bilgi-işlem departmanınıza veya ağ yöneticinize danışınız.

Microsoft Windows Kurulumu

MCKS VPN sistemine bağlantıda web servislerini kullanacak olan sunucunun tercihen UNIX/Linux olması önerilir. Ancak Windows platformu üzerinden de erişime olanak sağlanmıştır.

OpenVPN yazılımını windows üzerinde kullanılacak ise aşağıdaki linkten yazılımın indirilmesi ve kurulması gereklidir.

http://openvpn.se/files/install_packages/openvpn-2.0.9-gui-1.0.3-install.exe

Kurulum sonrasında TK tarafından sağlanan olan sertifikalar ve config dosyası

C:/Program Files/OpenVPN/config/

dizini altına kopyalanır. Dosyaların listesi aşağıda verilmiştir.

ca.crt	kök sertifika
ithalatci-adi.crt	ithalatciya ait sertifika
ithalatci-adi.key	ithalatciya ait sertifika key dosyası
mcks.conf	konfigürasyon dosyası (Bu dosya windows üzerinde kullanılacaksa adı mcks.ovpn olarak değiştirilmelidir)

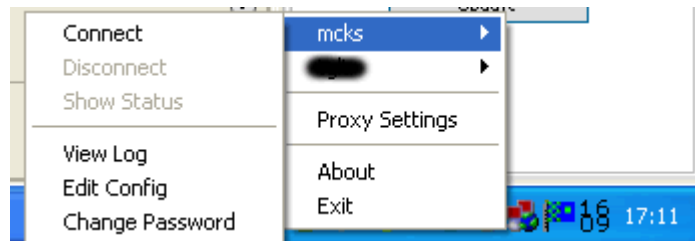
Dosyalar kopyalandıktan sonra mcks.conf dosyasında aşağıdaki parametreler TK tarafından sağlanan dosyaların isimlerine göre düzeltilerek konfigürasyon tamamlanır.

```
ca ca.crt  
cert ithalatci-adi.crt  
key ithalatci-adi.key
```

Programı çalıştırıp bağlanmak için araç çubuğundaki VPN simgesine sağ tıklanır. Bu simgeye sağ tıkladığında şekilde gösterildiği gibi bir menü çıkar.

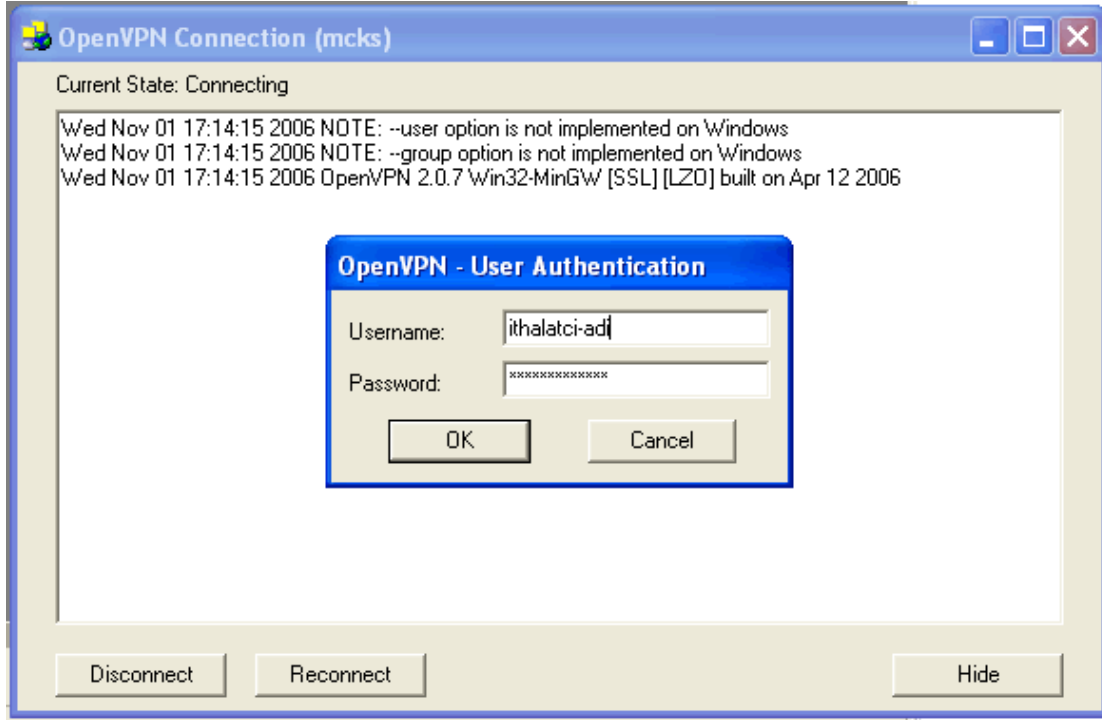


Şekil - 4: VPN araç çubuğu simgesi



Şekil - 5: VPN araç çubuğu simge menüsü

Yapılandırma dosyası “mcks” olarak adlandırılmıştır. Menüde üzerine gelince açılan menüden connect yazısına tıklanılarak bağlantı kurulumu başlatılır. Yazılım bağlantıyı kurmak için kullanıcı adı ve şifre soracaktır.



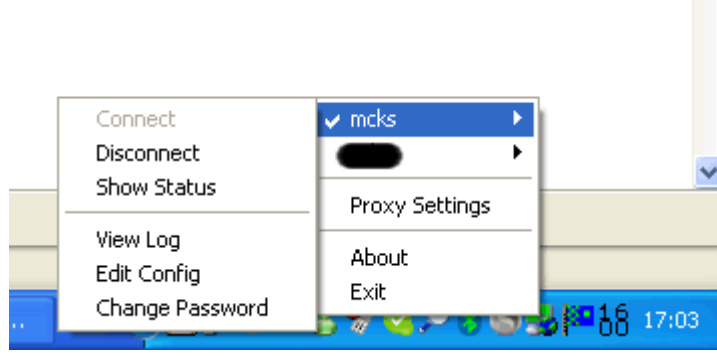
Şekil - 6: VPN kullanıcı ve şifre girişi

TK tarafından sağlanan kullanıcı adı ve şifre girildikten sonra bağlantı kurulacaktır. Bağlantı kurulduktan sonra araç çubuğundaki simge yeşil renge döner.



Şekil - 7: Bağlantı sonrası VPN araç çubuğu simgesi

Bağlantıyı kesmek için araç çubuğundaki VPN simgesine sağ tıklanarak açılan menüden mcks yazısına üzerine gelinir.



Şekil - 8: Bağlantı sonrası VPN araç çubuğu simge menüsü

Açılan menüden Disconnect yazısına tıklanarak bağlantı kesilir. Bağlantı kesildiğinde araç çubuğu üzerindeki simge tekrar kırmızı renge dönecektir.

UNIX/Linux Kurulumu

İthalat servislerine Linux / Unix işletim sistemi kullanılarak erişilecek ise aşağıdaki adresten openvpn yazılımı indirilerek içinden çıkan kurulum talimatlarına uygun olarak sisteme kurulur. Yazılımı kurmak ve çalıştırmak için “root” kullanıcısı olmak gerekmektedir.

<http://openvpn.net/release/openvpn-2.0.9.tar.gz>

Kurulum sonrasında TK tarafından sağlanan sertifikalar ve config dosyası **/etc/openvpn** dizini altına kopyalanır. Dosyaların listesi aşağıda verilmiştir.

ca.crt	kök sertifika
ithalatci-adi.crt	ithalatciya ait sertifika
ithalatci-adi.key	ithalatciya ait sertifika key dosyası
mcks.conf	konfigürasyon dosyası

Dosyalar kopyalandıktan sonra mcks.conf dosyasında aşağıdaki parametreler TK tarafından sağlanan dosyaların isimlerine göre düzeltilerek konfigürasyon tamamlanır.

```
ca ca.crt
cert ithalatci-adi.crt
key ithalatci-adi.key
```

Yukardaki işlemler tamamlandıktan sonra kullanılan Linux/Unix işletim sistemine bağlı olarak servis çalıştırılır.

Örneğin RedHat Linux işletim sistemi kullanılıyorsa;

```
# service openvpn start
```

Başka bir Linux dağıtımı kullanılıyorsa;

```
# /etc/init.d/openvpn start
```

Komutu ile OpenVPN yazılımı çalıştırılarak bağlantı kurulumu başlatılır. Bağlantı kurulması esnasında yazılım kullanıcı adı ve şifre soracaktır. TK tarafından sağlanan kullanıcı adı ve şifre girilerek bağlantı kurulur. Bağlantının kurulduğu

```
# ifconfig
```

komutu çalıştırıldığında tun0 isimli bir ağ adaptörünün var olduğu görülerek teyit edilir.

Bağlantıyı kesmek için ise

```
# service openvpn stop
```

veya;

```
# /etc/init.d/openvpn stop
```

komutu girilir. Bağlantı kesildiğinde “tun0” isimli ağ adaptörü artık görülmeyecektir.

UNIX/Linux üzerinde VPN, mesajlarını syslog aracılığıyla ek bir yapılandırma yapılmazsa mesaj loguna gönderir. Bağlantıda karşılaşılan sorunlar ile ilgili sisteminizin log dosyalarını incelemeniz gerekmektedir.

VPN Kullanımında Dikkat Edilecek Konular

VPN sistemi eş zamanlı olarak yüksek miktarda bağlantı yapılmasına uygun bir altyapı sağlamaktadır. Ancak, VPN istemci kullanımındaki **hatalar**, performans düşüklüğü, kopma ve bağlanamama gibi sorunlara neden olabilir.

VPN kullanımında aşağıdaki konulara özellikle **dikkat edilmesi gerekmektedir**.

1. Her VPN sertifikası ile aynı anda sadece ve sadece bir adet bağlantı gerçekleştirilebilir. Aynı sertifika ile aynı anda birden fazla bağlantı, trafik olduğunda her iki bağlantısında sürekli kopup yeniden bağlanmasına neden olacaktır. **Bu durum en çok karşılaşılan hataların başında gelmektedir.**
2. VPN erişiminin yapılabilmesi için bulunulan ağdan UDP 1194 numaralı portun geliş ve gidiş trafiğine, ve TCP 1194 portuna gidişin açılması ve gelecek yanıtlarında kabul edilmesini sağlayacak şekilde yerel güvenlik duvarı yapılandırılmalıdır.
3. VPN sistemi kullanıcı PC'leri yerine **tercihen** yerel ağ geçidi üzerinde yapılandırılmalıdır.
4. VPN sertifikaları **kesinlikle korunmalı** ve **paylaşılmamalıdır**.