

Tahribat.Com @ renegadealien

Yeni Başlayanlar İçin VPN

V 1.0 – 30.03.2014

Tahribat.Com

İçindekiler

İçindekiler	2
Güncellemeler.....	3
Açıklamalar	4
Başlarken.....	4
Neden ?.....	5
Sebepler	6
Nasıl Olmalı	7
Ne Yapacağız.....	7
Gereksinimler.....	7
Başlıyoruz.....	8
1.Digitalocean.Com Hesap Açılması, İlk VPS'in Kurulması.....	8
2. Sunucuya Bağlanmak	14
3. SoftEther VPN Serverı Bulmak ve İndirmek.....	22
4. SoftEther VPN Management Tool'u Bulmak ve İndirmek	28
5. SoftEther VPN Management Tool ile SoftEther VPN Sunucusunun Konfigure Edilmesi.....	29
6. Windows7 / Windows 8 Üzerinden VPN'e Bağlanmak.....	43
7. Android, iPhone ve Diğer Cihazlar Üzerinden VPN'e Bağlanmak.....	51
8. Linux Üzerinden VPN'e Bağlanmak.....	52
9. Sonuç.....	53

Güncellemeler

Versiyon – Tarih	Sayfalar	Açıklamalar
V 0.9 – 28.09.2014	<ul style="list-style-type: none">-	İlk Versiyon
V 1.0 – 30.09.2014	<ul style="list-style-type: none">1,2,3-524	<ul style="list-style-type: none">Başlık, İçindekiler ve Güncelleme bölümleri eklendi.Görünmeyen bazı resimler düzeltildi.Linux Üzerinden VPN'e Bağlanmak kısmı eklendi.Açıklamalar bölümü güncellendi.

Açıklamalar

1. Dökümanın güncel hali için lütfen <http://www.tahribat.com/Forum-Toplanin-Millet-Kendi-Vpn-Sunucumuzu-Kendimiz-Kuruyoruz-Yeni-Baslayanlar-Icin-Vpn-192621/> adresini düzenli olarak takip ediniz.
2. Döküman ile ilgili sorulmuş sorular ve soracağınız sorular için aynı forum konusunu takip edebilirsiniz.
3. Bu döküman, Tahribat.Com müritlerini aşağıdaki maddelere karşı aydınlatmak amacını taşımaktadır.
 - Özellikle son günlerde çekilmez bir hal alan Türkiye Cumhuriyeti'nde meydana gelen internet yasaklarının dayanakları, sebepleri ve sonuçları.
 - 5651 sayılı İnternet ortamında yapılan yayınların düzenlenmesi ve bu yayınlar yoluyla yapılan suçların engellenmesi hakkındaki kanun aracılığı ile tüm vatandaşların tüm internet trafiğinin kaydedilmesi ile ilgili alınabilecek tedbirler.
 - Bu yasakları ve engellemeleri için devletin bunlarla mücadelesi sırasında aldığı tedbirler.
 - TOR ve firma bazlı VPN kullanımının avantajları, dezavantajları.
 - Kendi VPN sunucumuzun kurulması ve işletilmesi için yapılması gerekenler.
4. Döküman muhtemelen oldukça uzun olacak, sadece döküman değil, genel bilgilendirme, konu ile ilgili uzman görüşleri de(şu anda bir tek ben varım malesef :) yer almaktadır, bu sebeple, şimdiden kendinizi hazırlayın.
5. Kurulum için gerekenler ;
 - Beyin
 - Bilgisayar
 - İnternet
6. Dökümanı bulabildiğiniz, ulaşabildiğiniz ve paylaşabildiğiniz mecralarda paylaşırsanız sevinirim, kaç sene sonra oturdum döküman yazdım, olabildiğince fazla kişi yararlansın.
7. Dökümanımı kullanarak para kazanan her vatandaş, gelirin %30'unu bendeniz ile paylaşmak zorundadır, aksi taktirde haram zehir zikkım olsun.
8. Döküman Tahribat.Com için yazılmıştır. Kaynak belirtmeden paylaşmayın, bozuyoruz.
9. Dökümanın bir süre güncel hali çıkabilir, kelime tipografi ve ekran görüntülerinde hatalar olabilir, lütfen son halini www.tahribat.com üzerinden takip ediniz.

Başlarken

Öncelikle VPN kavramını kısaca açıklayalım. Açılımı Virtual Private Network - Sanal Özel Ağ. Kısacası, birbiri ile aynı ağda olmayan iki uzak sistemin, sanki aynı ağdaymış gibi davranması için kurulmuş bir bağlantı çeşitidir. Bu döküman çerçevesinde ve genelde duyduğunuz VPN'i şu şekilde örnekleyebiliriz.

Kendi bilgisayarımızı, internet üzerinden şifreli olarak dünyanın başka bir yerindeki bilgisayara bağlayıp, o uzaktaki bilgisayarın aracılığı ile internete çıkmak, bu sayede ülkemizde yer alan verilerin kaydedilmesi,

yasaklamalar, engellemeler gibi sıkıntılarla karşılaşmadan, özgür internete bağlanabilmek için kullanacağımız bir altyapı.

Ayrıntılı bilgi için bkz : http://tr.wikipedia.org/wiki/Virtual_Private_Network

Neden ?

Bildiğiniz gibi Türkiye'de Twitter yasaklandı. Bknz : <http://www.hurriyet.com.tr/teknoloji/26057641.asp>

Aslında bu yasaklamalara Türk vatandaşı olarak biz yabancı değiliz. Tahribat.Com olarak bile 3 kere yasaklandık! Bu istatistikleri tutan Engelliweb.com adresine göre, dökümanı yayınlandığı tarihte, 40733 web sitesi kapatılmış ! Bknz : <http://engelliweb.com/istatistikler/>

İşin daha enteresan boyutu şu; yasaklamaların tamamı hukuka aykırı!

Sitelerin kapatılması için kaynak gösterilen 5651 sayılı kanun oldukça açık! Bknz : <http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5651.pdf>

Erişimin engellenmesi, suçun işlendiği düşünülen URL üzerinden yapılır.

Yani, www.yasaksite.com/konu.asp?id=15 adresinde bir ihlal varsa, bu adresi kapatabilirsiniz, tüm siteyi değil!

Fakat, memlekette hukuk olmadığı için, bilgisayardan anlayan hukukçu da olmadığı için, teknik olarak, tüm internet trafiğinin URL bazlı filtrelenmesi mümkün olmadığı için, URL bazlı filtrelense bile, SSL trafiğinin içine filtre yapılamadığı için, tüm siteyi kapatıyorlar!

Peki kapatma nasıl yapılıyor? (aslında yapılıyor du olacak, çünkü Twitter kapatması sırasında yeni bir olay ile karşılaştık, okuyoruz) Oldukça amelece bir yöntemle :)

Türk Telekom ve diğer servis sağlayıcılar, kendi DNS Serverları üzerinde, yasaklanacak sitenin IP adresini, engelli sayfası bulunan bir web sunucusuna yönlendiriyor, standart bir ADSL kullanıcısı, IP ayarlarında bir değişiklik yapmadığı takdirde, TTNET tarafından, modemine atanmış olan, 195.175.39.39 ve 195.175.39.40 DNS sunucularına sorgu gönderiyor ve engelli sayfasını görüyorduk. (DNS nasıl çalışır bilmeyenler için, Bknz : <https://www.youtube.com/watch?v=F8xbHcfOu7s>)

Bunun üzerine, memleketteki herkez DNS değiştirmeyi öğrenmişti. Google DNS diye bildiğimiz 8.8.8.8 ve 8.8.4.4 adreslerini bilgisayarımızda ayarlıyor, bu sayede DNS sorgularımızı TTNET DNS yerine Google DNS adreslerine yönlendiriyor, yasaklı sitelere giriyorduk. (Bknz : <https://developers.google.com/speed/public-dns/?hl=tr>)

Ama durun bir dakika! Twitter engellenince, birşey daha oldu! Baktılar ki, devletle geyik yapıyoruz, 8.8.8.8 ve 8.8.4.4 adresine engellendi ! Bknz : <http://www.hurriyet.com.tr/teknoloji/26060179.asp>

YUUUUUUUUUUUHHHHH!

Hatta bununla kalmadılar, Yandex DNS'den engellendi !

YUUUUUUUUUUUHHHHH!

Bunun hemen ardından, millet VPN servislerine abanınca, VPN'de engellebilir tarzı yazılar haber sitelerinde dolaşmaya başladığında, tansiyonum düştü artık! Dedim böyle olmayacak, bir çözüm bulmalı.

Güncelleme : Bu dökümanı yazmaya başladığımın 2., yazmaya karar verdiğimin 4. günü Youtube.Com adreside Türkiye'den erişime kapatıldı.

YUUUUUUUUUUUUHHHHH!

Sebepler

Dikkat ! Bu kısım önemli!

1. Devamlı biryerler yasaklanıyor! Tahribat'tan Twitter'a hergün biryer yasaklanıyor! Sonra bunu yasakladıkları yetmiyormuş gibi, gidip DNS'leri bile yasaklayabiliyor, VPN servis sağlayıcılarını bile yasaklayacağız diyolarlar! Tekrar ediyorum,

YUUUUUUUUUUUUHHHHH!

2. 5651 üzerinde 6/2/2014 tarihinde yapılan güncelleme uyarınca, artık servis sağlayıcılar tüm erişim kayıtlarını kaydetmek ile yükümlüler! Bu demek oluyor ki, erişim kayıtlarımızı kaydedecek altyapı kurulacak, erişim kayıtlarımız ve istenildiği takdirde tüm iletişimimiz kaydedilecek!

Eşimle, dostumla, arkadaşım ile yazıştıklarım, maillerim, mesajlarım, girdiğim sitelerden devlete ne yahu!

3. Olayın farklı yönleride var aslında. Örneğin, wireless aracılığı ile bi alışveriş merkezinde internete girdiniz. Bu gün Google Play Store üzerinde, aynı ağa bağlı olduğunuz anda karşıldakinin Facebook ekranına giren uygulama dahil, envayi çeşit uygulama var, onun haricinde Man-In-The-Middle yöntemi ile verilerinizi kopyalayabilecek dünya kadar liseli var :)

Bu noktadan yola çıkarak yapılacaklar ile ilgili bazı alternatifler var.

- **TOR kullanmak.**

Alternatiflerden birisi TOR kullanmak. Fakat bazı dezavantajları var.

- Bağlantı oldukça yavaş.
- Tüm networkü secure etmediğimiz için, örneğin TOR Browserla girdiğimiz web siteleri ile aramızda olan trafik güvenli iken, PC üzerinde bulunan Google Chrome normal bağlantıyı kullanıyor.
- Tor sırasında her ne kadar, anonimlik sağlansa bile, TOR'un çıkış nodelarında var olan kullanıcılar unencrypt trafiğinizi loglayabilir.

- **ZenMate, HideMyAss, HotspotShield gibi uygulamaları kullanmak.**

Bu tarz uygulamaların tamamı, VPN kullanarak sizi yurtdışındaki bir sunucudan çıkartıyor, bu sayede hem yasaklara hem loglanmaya takılmıyorsunuz. Fakat bu sistminde bazı dezavantajları var.

- Bu hizmeti güvenli olarak alabileceğiniz, birkaç firma var. Bu firmalarda genellikle, yavaş ve sizi reklama boğan ücretsiz opsiyonu ve ortalama 7\$dan başlayan ücretli opsiyonları bulunmakta.
- Ülkemizde özellikle Twitter'ın yasaklanması sırasında oluşan yoğunluktan dolayı bu sunucuların performansları ve bağlantı hızları oldukça düştü.
- Büyük firmalarda olmak üzere, hemen hemen tamamı, bağlantılarımız üzerinden profil çıkartma hizmetleri sunuyorlar, resmi veya elaltından. Lan ben beni kimse loglamasın derken, paramla rezil mi olayım?

Nasıl Olmalı

1. Güvenli olmalı. Veri şifreli olmalı, bu sayede meraklı arkadaşlar erişmemeli.
2. Tüm cihazlarımda, bilgisayarım da, Laptop'um da, Cep telefonum da kullanılabilmeli.
3. Hızlı olmalı.
4. Benim kontrolümde olmalı.

Ne Yapacağız

Yurt dışında barınan, kendimize özel bir VPN sunucusu kuracağız. Tüm cihazlarımızı bu VPN'e bağlayacağız. İnternete çıkartacağız.

Gereksinimler

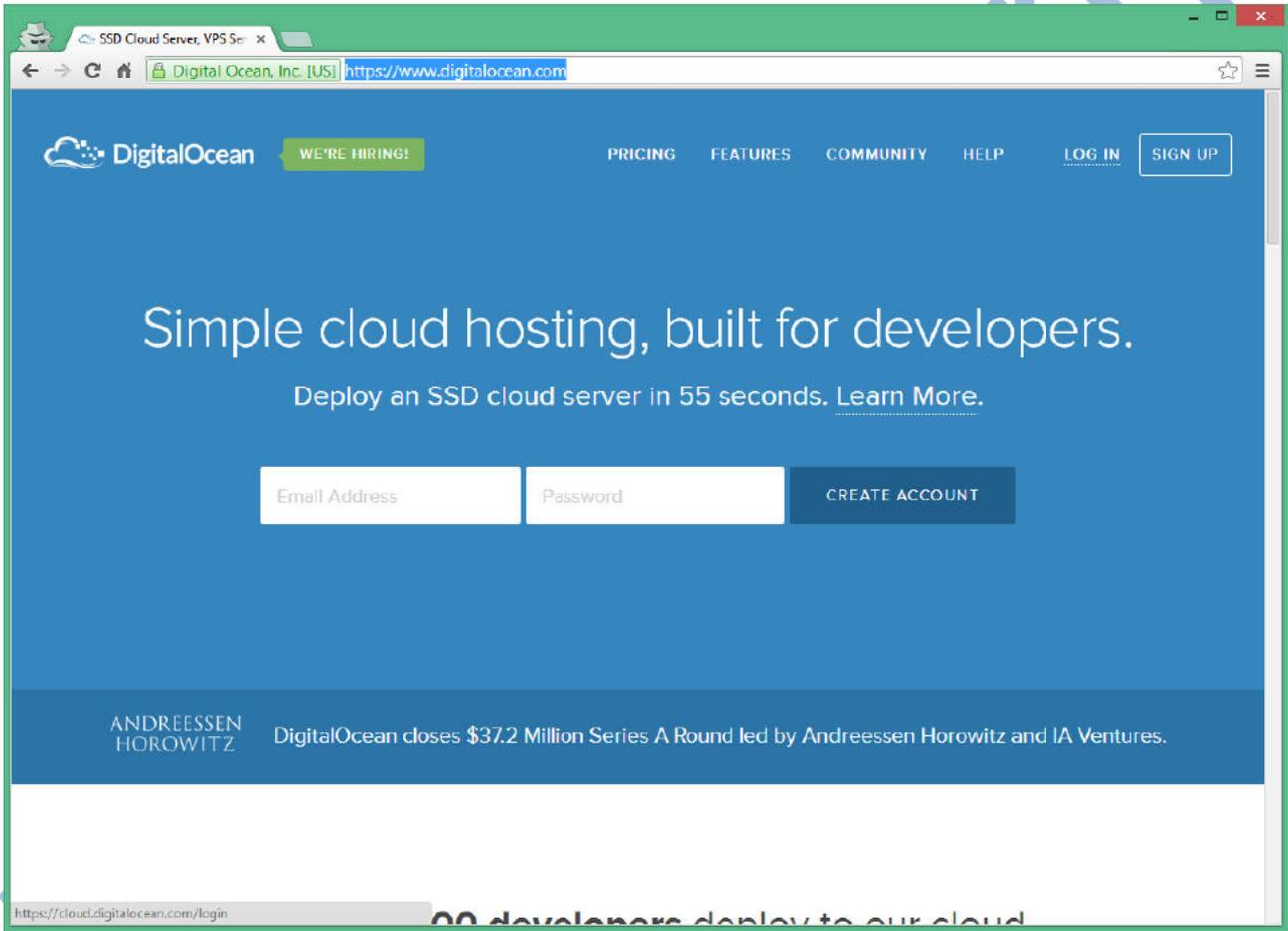
1. 1 adet yurt dışı lokasyonlu sunucu. Fiyatın ucuz olması oldukça avantaj. Aynı zamanda Türkiye'ye yakın olursa, bağlantımız daha hızlı olacaktır. Bu iş için ben www.digitalocean.com dan bir adet amsterdam lokasyonlu minimum konfigürasyonlu sunucu kullanacağım.
2. Sunucunun maliyeti aylık 5\$. Eğer sizin için yüksek geliyorsa, bir sunucu kurup aylık 5 liraya 5 arkadaşınıza kiralayabilirsiniz :)
3. VPN'i kuracağım sunucu CentOS 6'nın digitalocean üzerindeki son versiyonu. CentOS en sevdiğim Linux türevi olduğu için bunu kullanıyorum :)
4. VPN sunucusu olarak OpenSource SoftEther VPN Serveri kullanacağım. <https://www.softether.org/> adresinden inceleyebilirsiniz.
5. Sunucunun maliyeti aylık 5\$. Eğer sizin için yüksek geliyorsa, bir sunucu kurup aylık 5 liraya 5 arkadaşınıza kiralayabilirsiniz :)
6. Biraz kafayı çalıştırmamız, aşağıdaki adımları düzgün olarak takip etmeniz gerekli.

Başlıyoruz

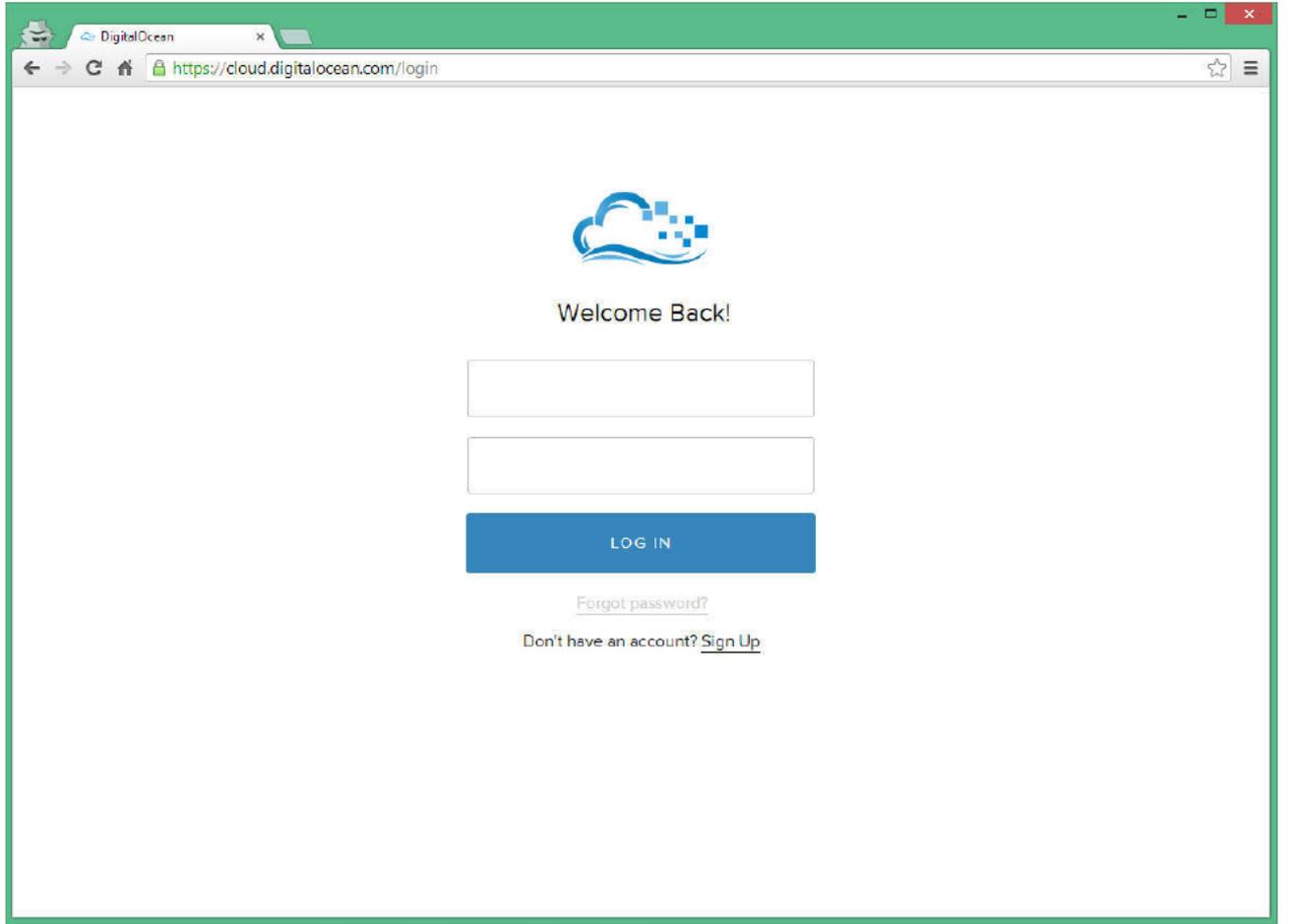
1. Digitalocean.Com Hesap Açılması, İlk VPS'in Kurulması

1. Digitalocean.com, dünyanın 6 değişik bölgesinde binlerce sunucusu olan, bizlere Cloud üzerinden VPS hizmeti veren bir web sitesi. Bu web sitesi aracılığı ile aylık 5\$'a 512 MB Ramli bir sunucu kiralayabiliyoruz, uygun olduğu için burayı kullanıyorum. VPS için Bknz : <http://www.sunucupark.com/vps-nedir.html>

<https://www.digitalocean.com> adresine giriyoruz, SignUp linkini kullanarak üye oluyoruz. Daha sonra Log In linkine tıklayarak giriş yapıyoruz.

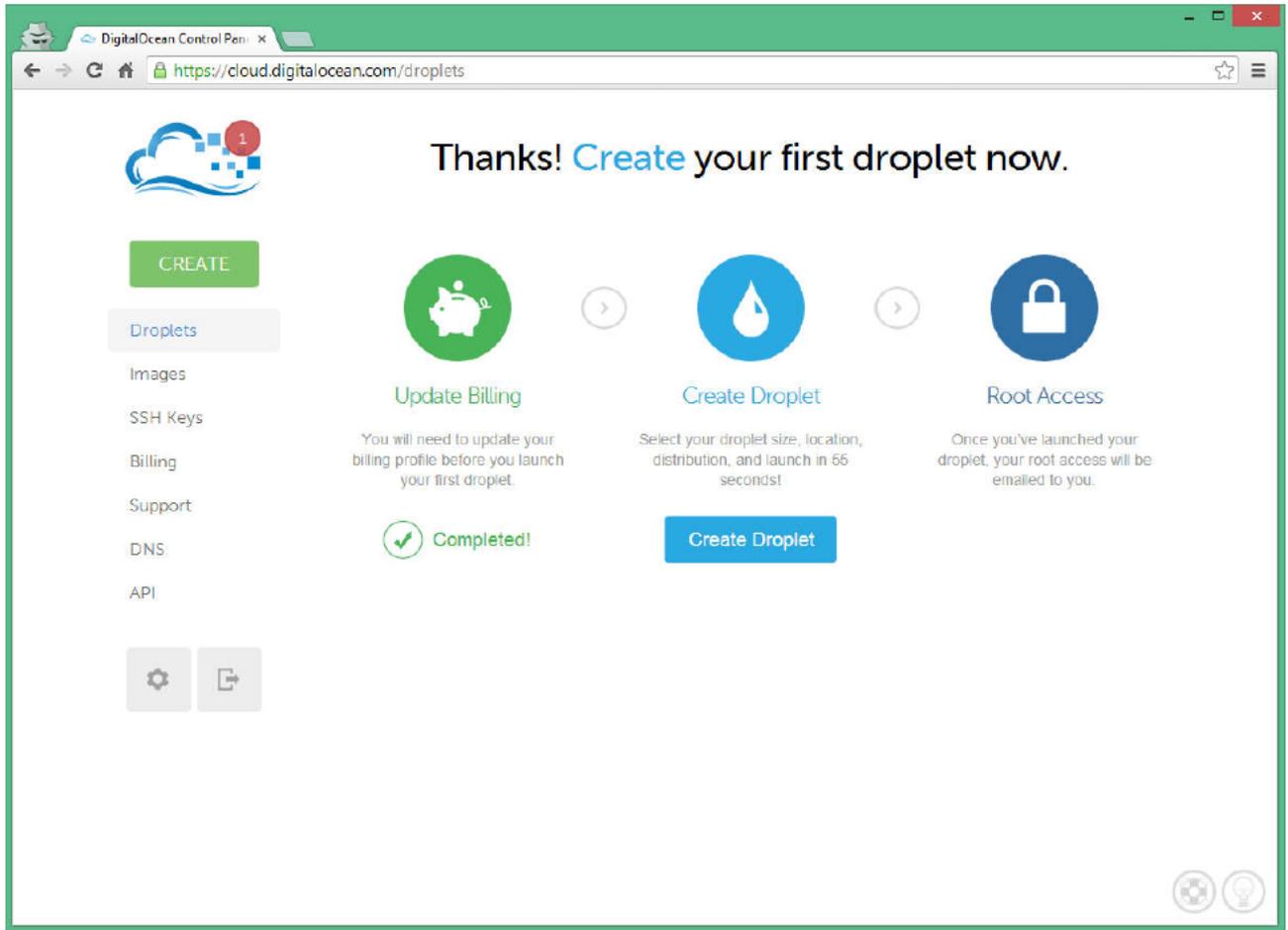


2. Açılan pencere aracılığı ile giriş yapıyoruz.



Gerekli ise, Billing kısmını kullanarak para yatırın, sanırım ilk açılışta 5\$ veriyordu. bu para ile 1 aylık sunucu kurulumunuzu bedavaya getirebilirsiniz.

3. Aşağıdaki pencerede Create Droplet sekmesine tıklayın.



4. Hostname olarak eğer, bir domaininiz var ise, vpn.domainname.com şeklinde yazabilirsiniz. aksi takdirde vpn yazıp geçebilirsiniz. ben vpn.kendidomainim.com yazıyorum, vpn.kendidomainim.com adresini buraya yönlendireceğim.

Select Size kısmından en küçük sunucuyu seçiyorum. tahmini 10 istemciye kadar bu sunucu kaldıracaktır. Daha fazla istemciyi sisteme bağlamak istiyor veya satış yapmak istiyorsanız, ilerde bir üst versiyon sunucuyu seçebilirsiniz.

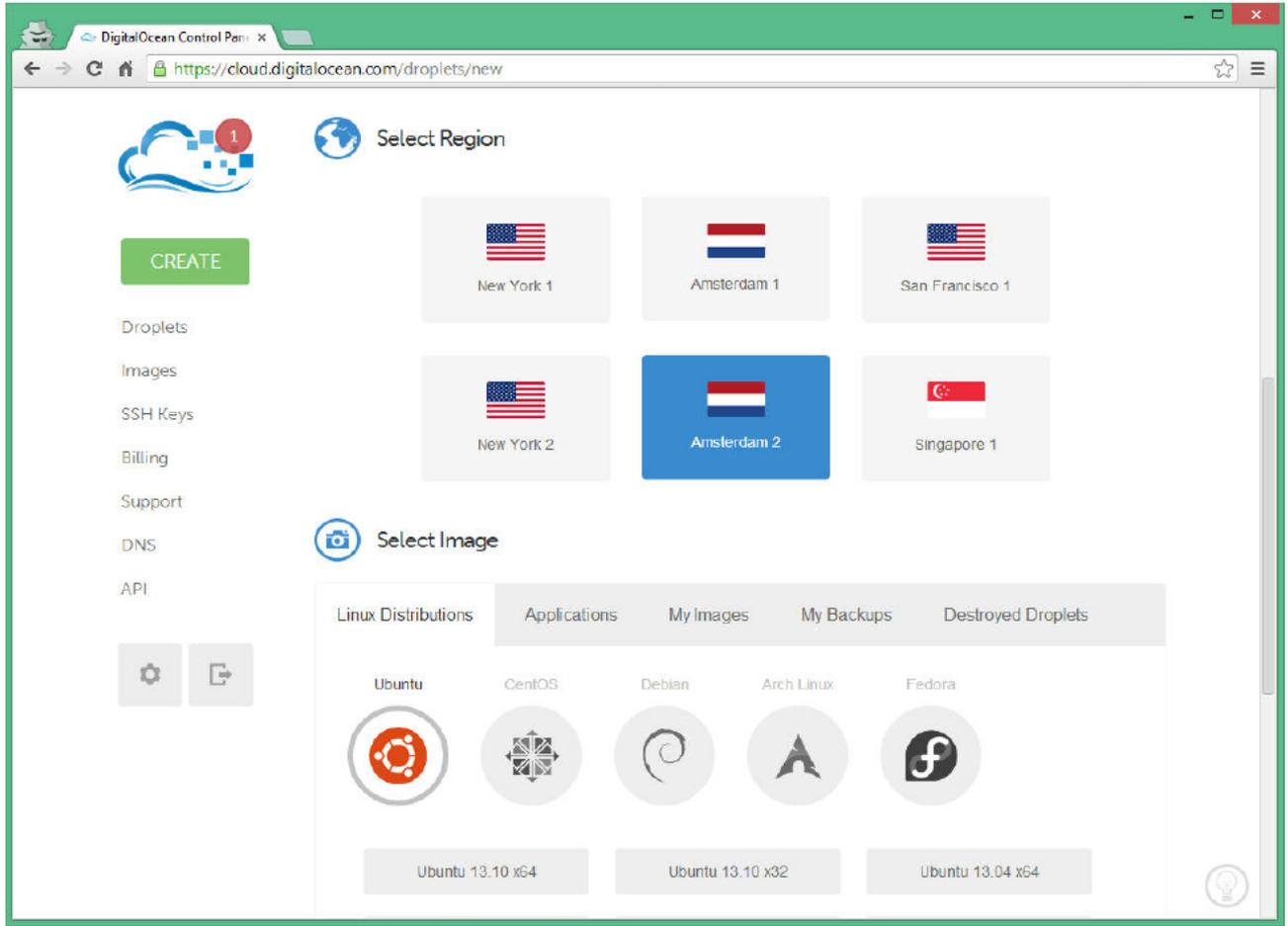
Şimdilik en düşük versiyonu seçiyorum.

The screenshot shows the DigitalOcean 'Create Droplet' interface. The browser address bar is <https://cloud.digitalocean.com/droplets/new>. The page features a sidebar on the left with navigation links: Droplets, Images, SSH Keys, Billing, Support, DNS, and API. The main content area is titled 'Create Droplet' and includes a green 'CREATE' button. Below this, there is a 'Droplet Hostname' section with the text 'Hostname: vpn.mydomainname.com'. The 'Select Size' section displays six pricing options in a grid:

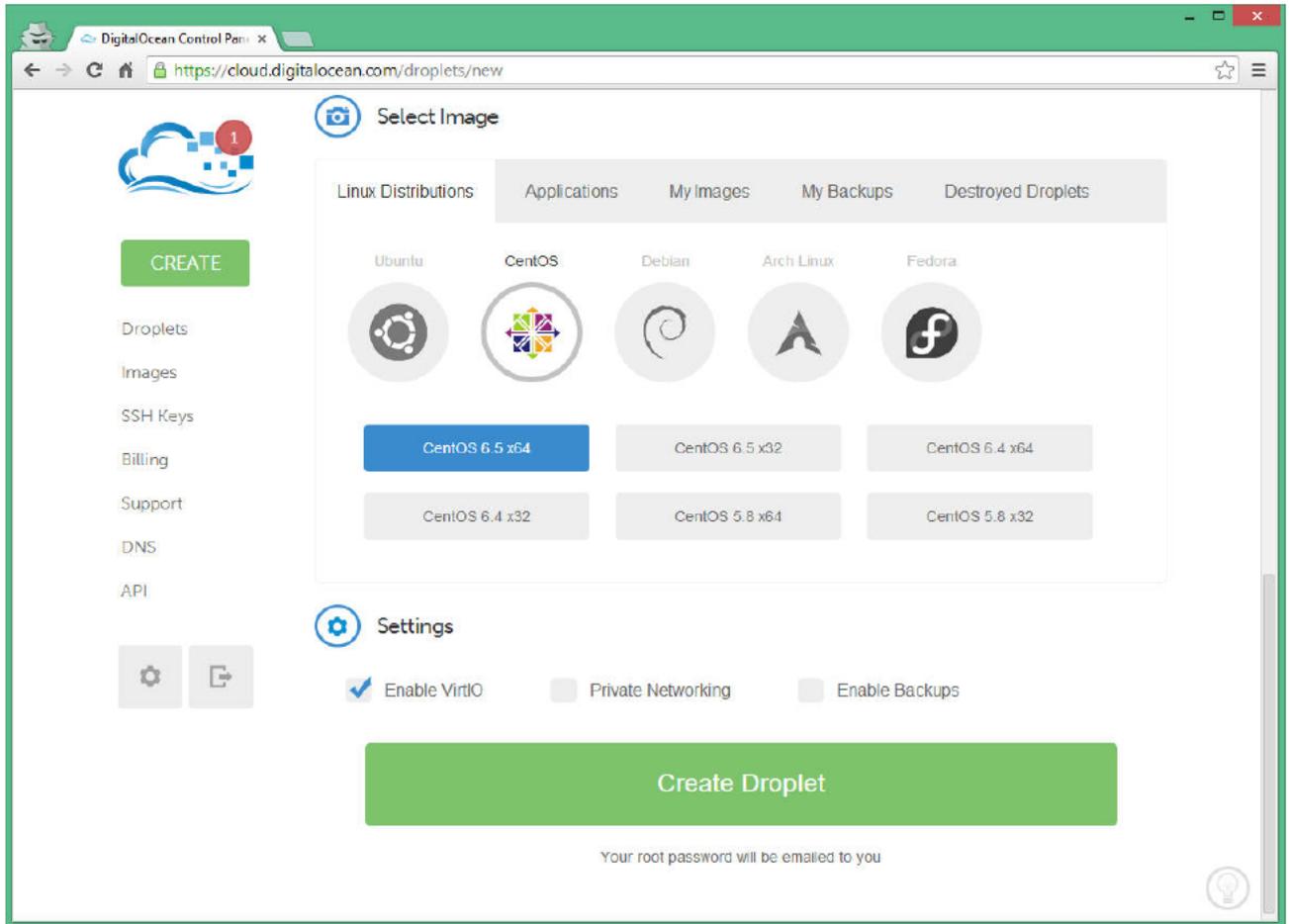
Size	Monthly Price	Hourly Price
512MB / 1 CPU 20GB SSD DISK 1TB TRANSFER	\$5.00	\$0.007
1GB / 1 CPU 30GB SSD DISK 2TB TRANSFER	\$10.00	\$0.015
2GB / 2 CPUS 40GB SSD DISK 3TB TRANSFER	\$20.00	\$0.030
4GB / 2 CPUS 60GB SSD DISK 4TB TRANSFER	\$40.00	\$0.060
8GB / 4 CPUS 80GB SSD DISK 5TB TRANSFER	\$80.00	\$0.119
16GB / 8 CPUS 160GB SSD DISK 6TB TRANSFER	\$160.00	\$0.238

At the bottom of the page, there is a 'Select Region' button with a globe icon.

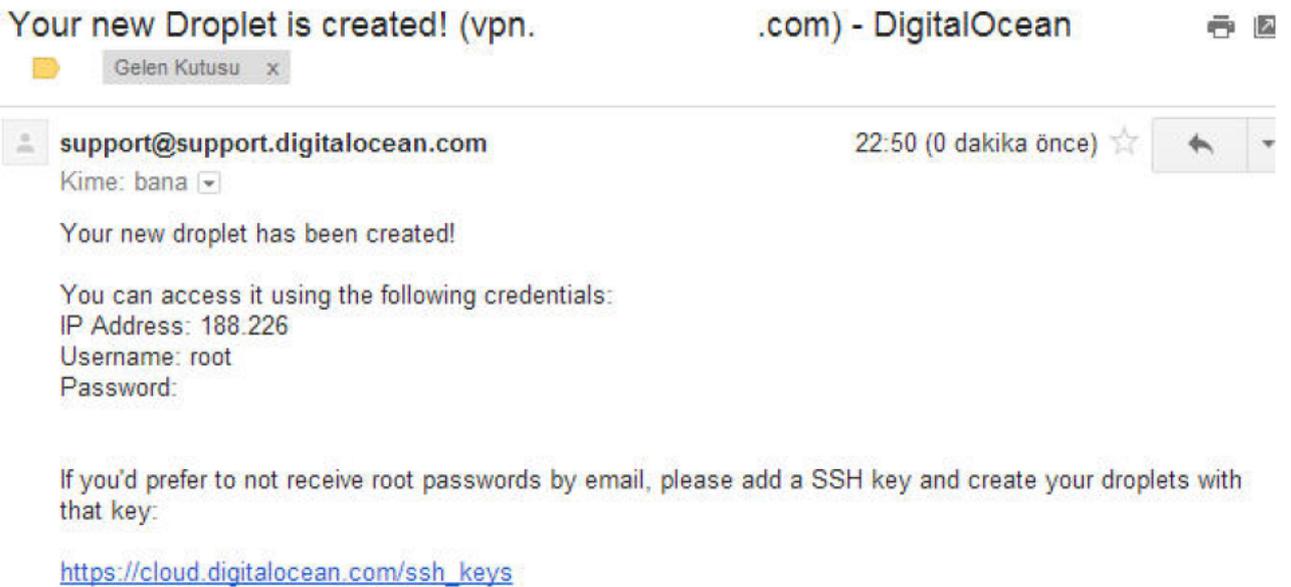
5. Select Region kısmında bölgeyi seçiyorum. Aynı kıtada olmamız Pingimizin düşük olması dolayısı ile bağlantımızın daha hızlı olmasını sağlayacaktır. Ben amstredam 2 lokasyonunu seçiyorum.



6. Select Image kısmından, CentOS'un 6.5 64Bit olanını seçiyorum.



7. Create Droplet'e tıklıyorum. Sunucum hazırlanıyor, yaklaşık 1 dakika içerisinde, sunucu bilgilerinin olduğu aşağıdaki gibi bir mail geldi.



8. Hesap alımı ve sunucu kurulumunun ilk adımı bitti.

2. Sunucuya Bağlanmak

1. Sunucumuz şu anda amsterdam'da kuruldu, açıldı ve bizim bağlanmamızı bekliyor. Bağlantı için <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html> adresinden PUTTY'yi indireceğiz.

PuTTY Download Page

[Home](#) | [Licence](#) | [FAQ](#) | [Docs](#) | [Download](#) | [Keys](#) | [Links](#)
[Mirrors](#) | [Updates](#) | [Feedback](#) | [Changes](#) | [Wishlist](#) | [Team](#)

Here are the PuTTY files themselves:

- PuTTY (the Telnet and SSH client itself)
- PSCP (an SCP client, i.e. command-line secure file copy)
- PSFTP (an SFTP client, i.e. general file transfer sessions much like FTP)
- PuTTYtel (a Telnet-only client)
- Plink (a command-line interface to the PuTTY back ends)
- Pageant (an SSH authentication agent for PuTTY, PSCP, PSFTP, and Plink)
- PuTTYgen (an RSA and DSA key generation utility).

LEGAL WARNING: Use of PuTTY, PSCP, PSFTP and Plink is illegal in countries where encryption is outlawed. I believe it is legal to use PuTTY, PSCP, PSFTP and Plink in England and Wales and in many other countries, but I am not a lawyer and so if in doubt you should seek legal advice before downloading it. You may find [this site](#) useful (it's a survey of cryptography laws in many countries) but I can't vouch for its correctness.

Use of the Telnet-only binary (PuTTYtel) is unrestricted by any cryptography laws.

There are cryptographic signatures available for all the files we offer below. We also supply cryptographically signed lists of checksums. To download our public keys and find out more about our signature policy, visit the [Keys page](#). If you need a Windows program to compute MD5 checksums, you could try the one at [this site](#). (This MD5 program is also cryptographically signed by its author.)

Binaries

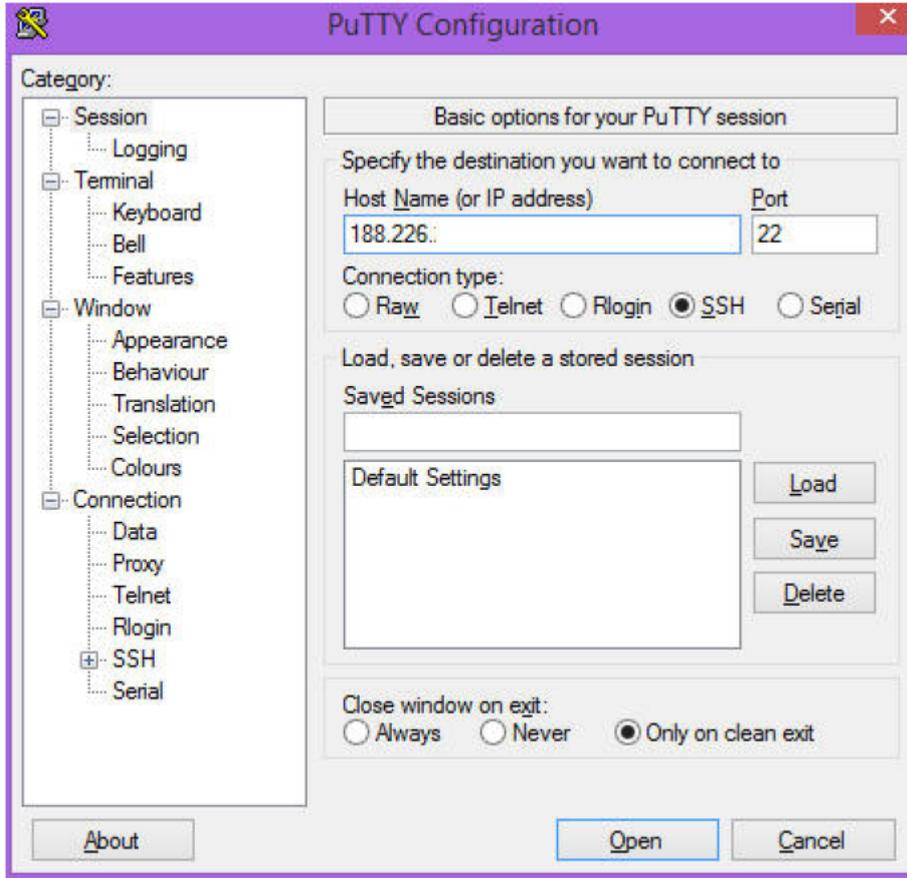
The latest release version (beta 0.63). This will generally be a version I think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if I've already fixed the bug, before reporting it to me.

For Windows on Intel x86

PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink:	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)
Pageant:	pageant.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYgen:	puttygen.exe	(or by FTP)	(RSA sig)	(DSA sig)

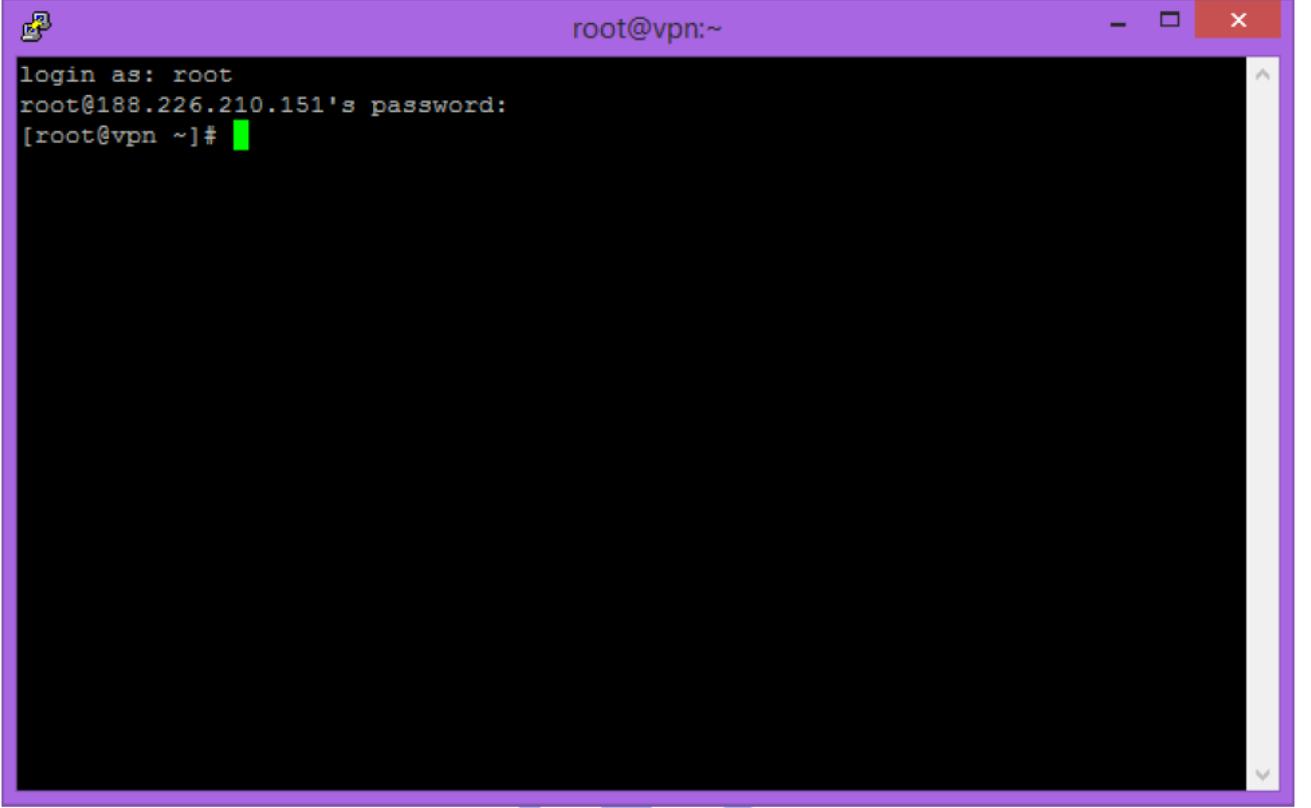
the.earth.li/~sgtatham/putty/latest/x86/putty.exe

2. Putty indirildikten sonra, Mail'de gelen IP adresini yazarak SSH aracılığı ile 22. porttan sunucuya bağlanıyoruz.



3. Cihazın SSL bağlantısı için kullanacağı KEY'i YES'e tıklayacak bilgisayarımıza yüklüyoruz.

4. Sunucunun konsolu önümüze geldi. Kullanıcı adı olarak root yazıyor şifre olarak mail'de gelen şifreyi yazıyor ve entera basıyoruz.



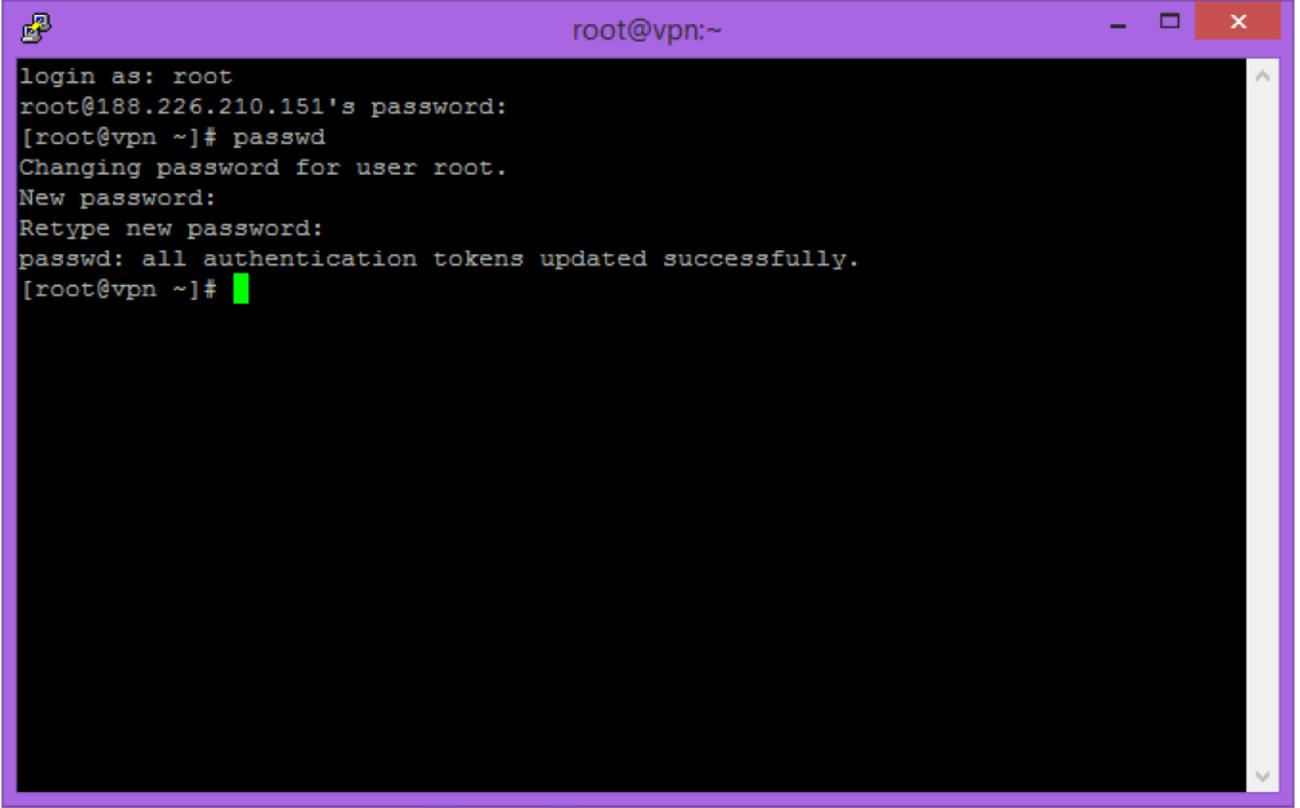
```
root@vpn:~  
login as: root  
root@188.226.210.151's password:  
[root@vpn ~]#
```

Tahribat

5. Öncelikle

passwd

komutunu kullanarak şifremizi deęiştiriyoruz.

A terminal window with a purple title bar containing the text 'root@vpn:~'. The terminal output shows the following sequence of commands and responses: 'login as: root', 'root@188.226.210.151's password:', '[root@vpn ~]# passwd', 'Changing password for user root.', 'New password:', 'Retype new password:', 'passwd: all authentication tokens updated successfully.', and '[root@vpn ~]#'. A green cursor is visible at the end of the last line.

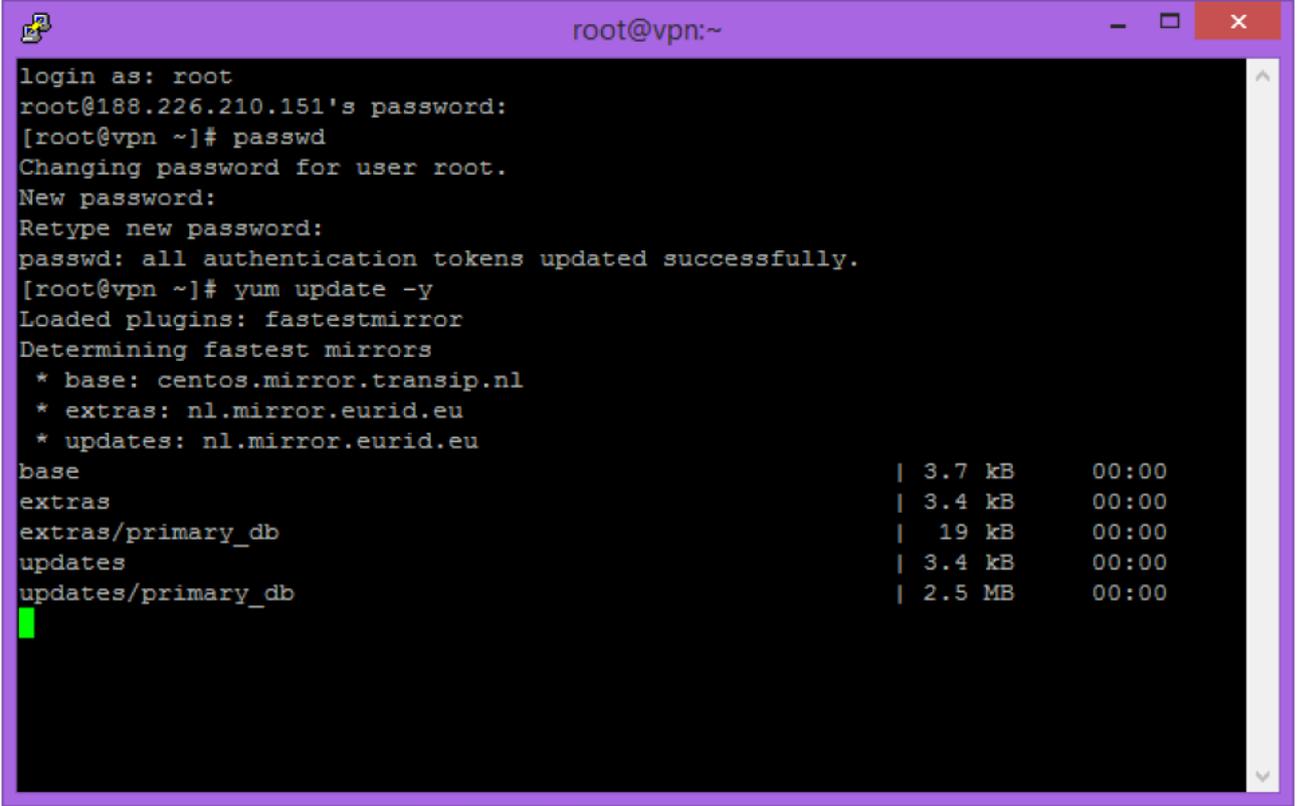
```
root@vpn:~
login as: root
root@188.226.210.151's password:
[root@vpn ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@vpn ~]#
```

Tahribat

6. Sunucu güncellemeleri için

yum update -y

komutunu kullanıyoruz.



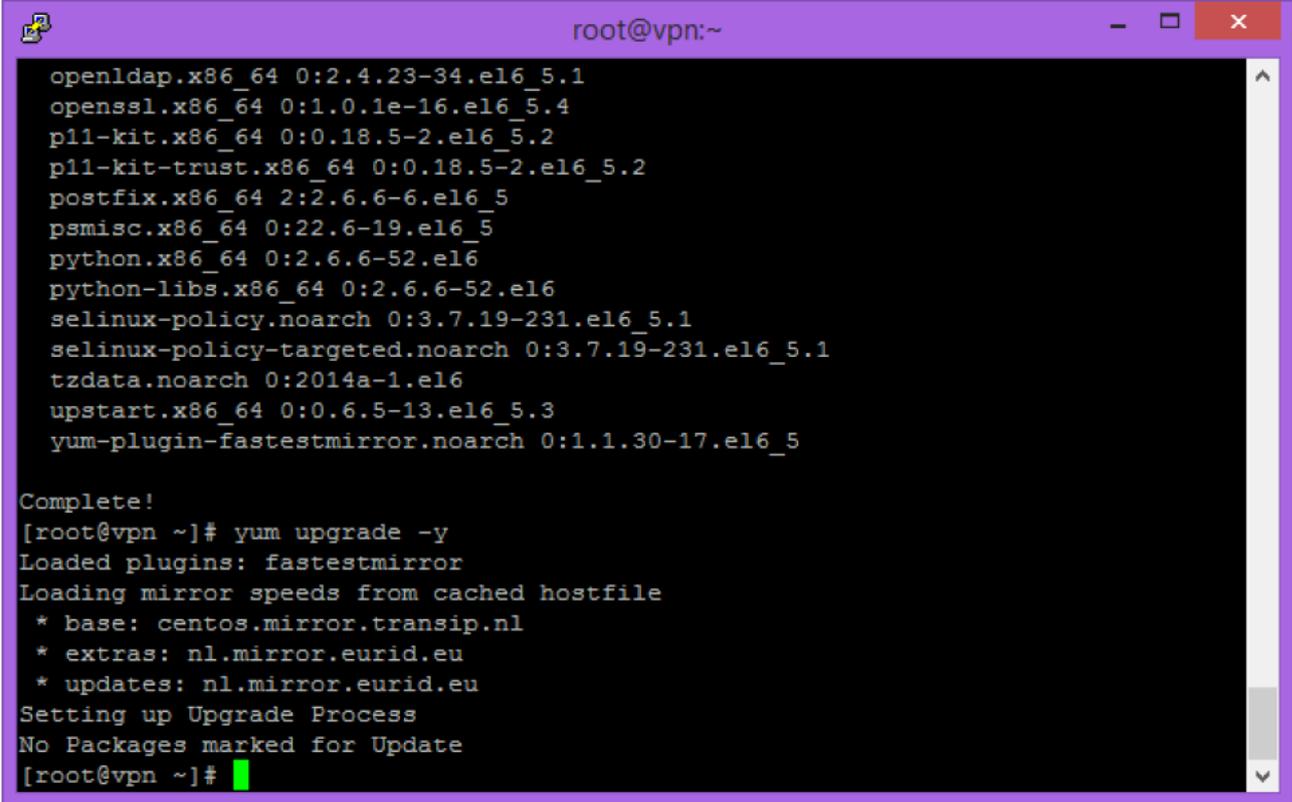
```
root@vpn:~
login as: root
root@188.226.210.151's password:
[root@vpn ~]# passwd
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
[root@vpn ~]# yum update -y
Loaded plugins: fastestmirror
Determining fastest mirrors
 * base: centos.mirror.transip.nl
 * extras: nl.mirror.eurid.eu
 * updates: nl.mirror.eurid.eu
base | 3.7 kB | 00:00
extras | 3.4 kB | 00:00
extras/primary_db | 19 kB | 00:00
updates | 3.4 kB | 00:00
updates/primary_db | 2.5 MB | 00:00
█
```

Tahribat

7. Eğer varsa, upgrade için işaretlenmiş güncellemeler var ise, yüklemek için

`yum upgrade -y`

komutunu kullanıyoruz.

A terminal window with a purple title bar showing the output of the 'yum upgrade -y' command. The window title is 'root@vpn:~'. The output lists several packages to be updated, followed by 'Complete!' and the execution of the 'yum upgrade -y' command. The command output shows 'Loaded plugins: fastestmirror', 'Loading mirror speeds from cached hostfile', and 'Setting up Upgrade Process'. Finally, it states 'No Packages marked for Update' and returns to the shell prompt.

```
root@vpn:~  
openldap.x86_64 0:2.4.23-34.el6_5.1  
openssl.x86_64 0:1.0.1e-16.el6_5.4  
p11-kit.x86_64 0:0.18.5-2.el6_5.2  
p11-kit-trust.x86_64 0:0.18.5-2.el6_5.2  
postfix.x86_64 2:2.6.6-6.el6_5  
psmisc.x86_64 0:22.6-19.el6_5  
python.x86_64 0:2.6.6-52.el6  
python-libs.x86_64 0:2.6.6-52.el6  
selinux-policy.noarch 0:3.7.19-231.el6_5.1  
selinux-policy-targeted.noarch 0:3.7.19-231.el6_5.1  
tzdata.noarch 0:2014a-1.el6  
upstart.x86_64 0:0.6.5-13.el6_5.3  
yum-plugin-fastestmirror.noarch 0:1.1.30-17.el6_5  
  
Complete!  
[root@vpn ~]# yum upgrade -y  
Loaded plugins: fastestmirror  
Loading mirror speeds from cached hostfile  
* base: centos.mirror.transip.nl  
* extras: nl.mirror.eurid.eu  
* updates: nl.mirror.eurid.eu  
Setting up Upgrade Process  
No Packages marked for Update  
[root@vpn ~]#
```

Tahribat

8. Kullanacağımız uygulamaları yüklemek için

yum install wget ftp gcc make nano -y

komutunu kullanıyoruz. Komutları kısaca açıklayım.

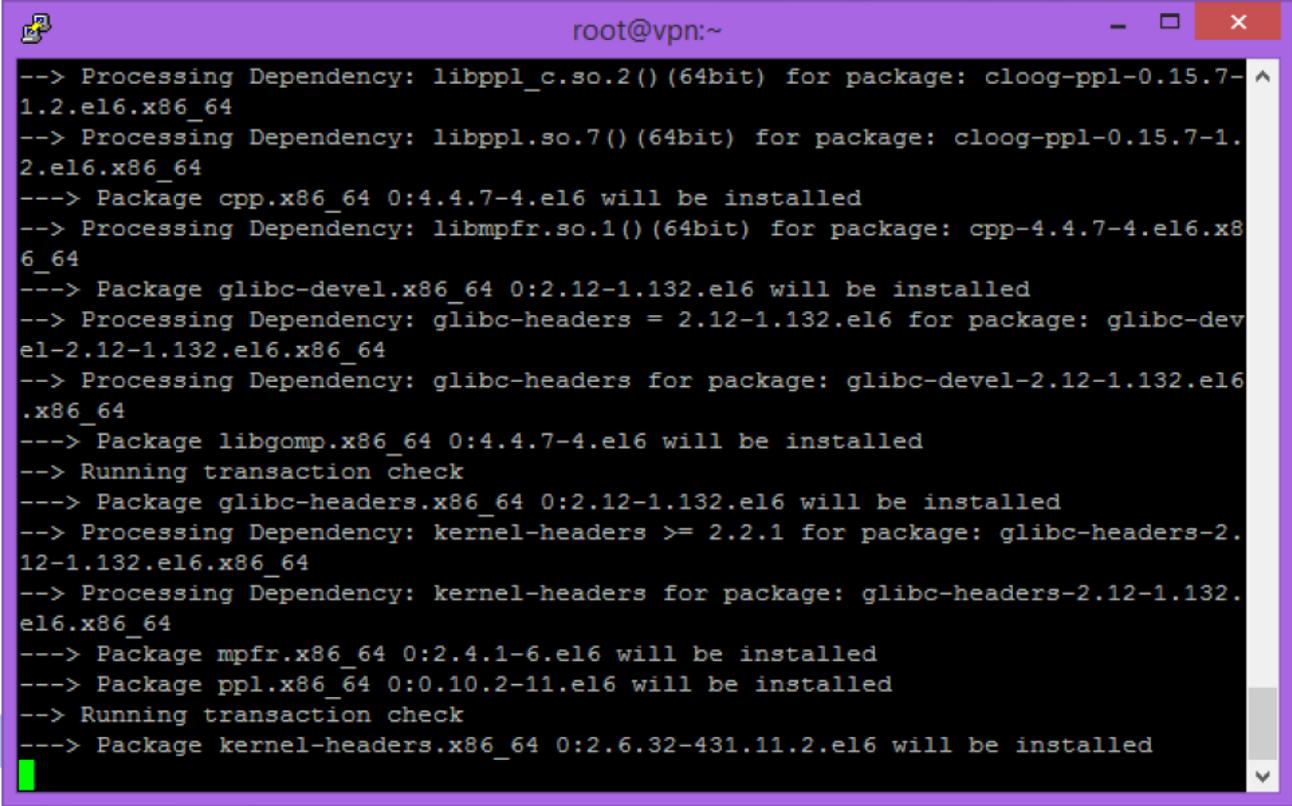
wget : HTTP protokolü kullanarak dosya indirmek için kullanacağız.

ftp : FTP protokolü kullanırsam diye yükledim.

gcc : İndirdiğimiz dosyaların derlenmesi için gerekecektir.

make : İndirdiğimiz dosyaların installerlarının çalışması için gerekecektir.

nano : Favori text ediyorum, illa işe yarar diye yükledim :)



```
root@vpn:~
--> Processing Dependency: libpppl_c.so.2 () (64bit) for package: cloog-pppl-0.15.7-1.2.el6.x86_64
--> Processing Dependency: libpppl.so.7 () (64bit) for package: cloog-pppl-0.15.7-1.2.el6.x86_64
--> Package cpp.x86_64 0:4.4.7-4.el6 will be installed
--> Processing Dependency: libmpfr.so.1 () (64bit) for package: cpp-4.4.7-4.el6.x86_64
--> Package glibc-devel.x86_64 0:2.12-1.132.el6 will be installed
--> Processing Dependency: glibc-headers = 2.12-1.132.el6 for package: glibc-devel-2.12-1.132.el6.x86_64
--> Processing Dependency: glibc-headers for package: glibc-devel-2.12-1.132.el6.x86_64
--> Package libgomp.x86_64 0:4.4.7-4.el6 will be installed
--> Running transaction check
--> Package glibc-headers.x86_64 0:2.12-1.132.el6 will be installed
--> Processing Dependency: kernel-headers >= 2.2.1 for package: glibc-headers-2.12-1.132.el6.x86_64
--> Processing Dependency: kernel-headers for package: glibc-headers-2.12-1.132.el6.x86_64
--> Package mpfr.x86_64 0:2.4.1-6.el6 will be installed
--> Package ppl.x86_64 0:0.10.2-11.el6 will be installed
--> Running transaction check
--> Package kernel-headers.x86_64 0:2.6.32-431.11.2.el6 will be installed
```

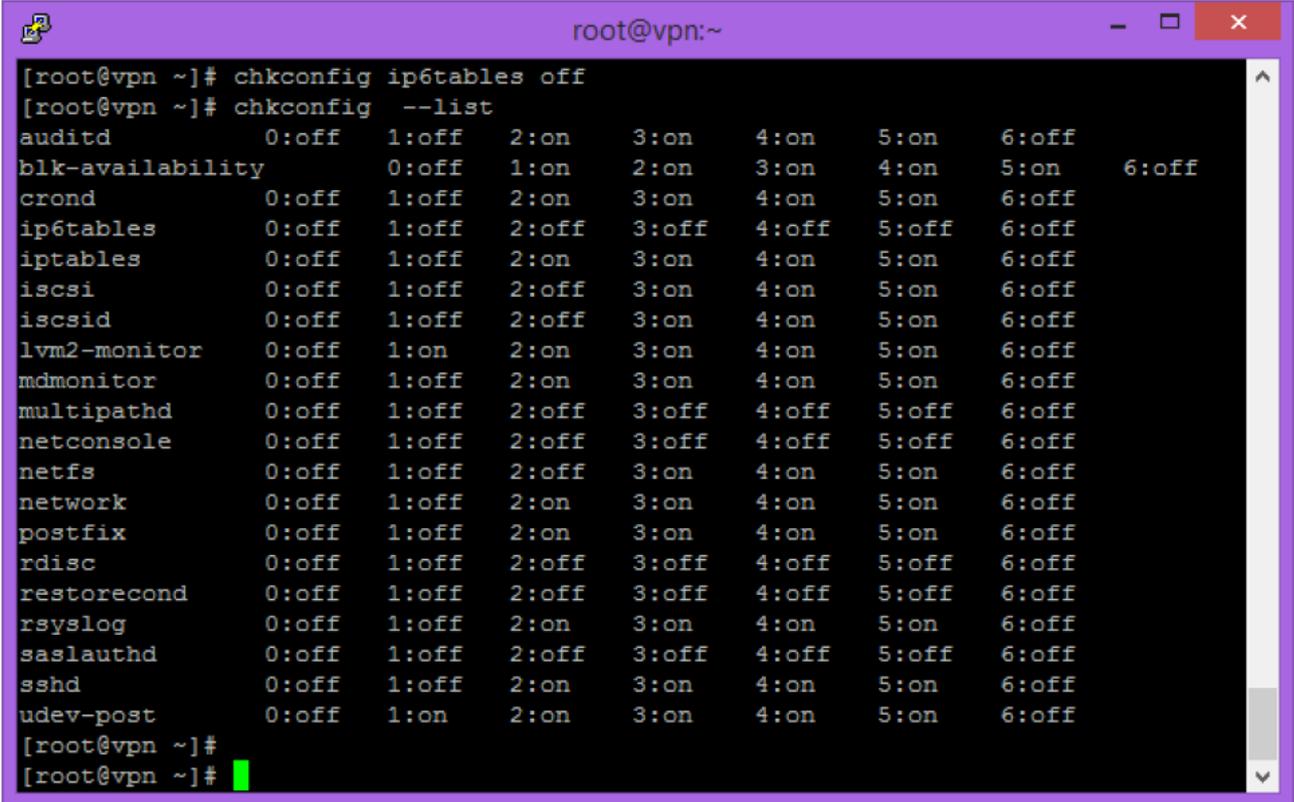
9. Servisleri

chkconfig --list

ile kontrol ettim. ip6tables, IPv6 Firewallı, kullanamayacağımız için

chkconfig ip6tables off

ile kapattım.



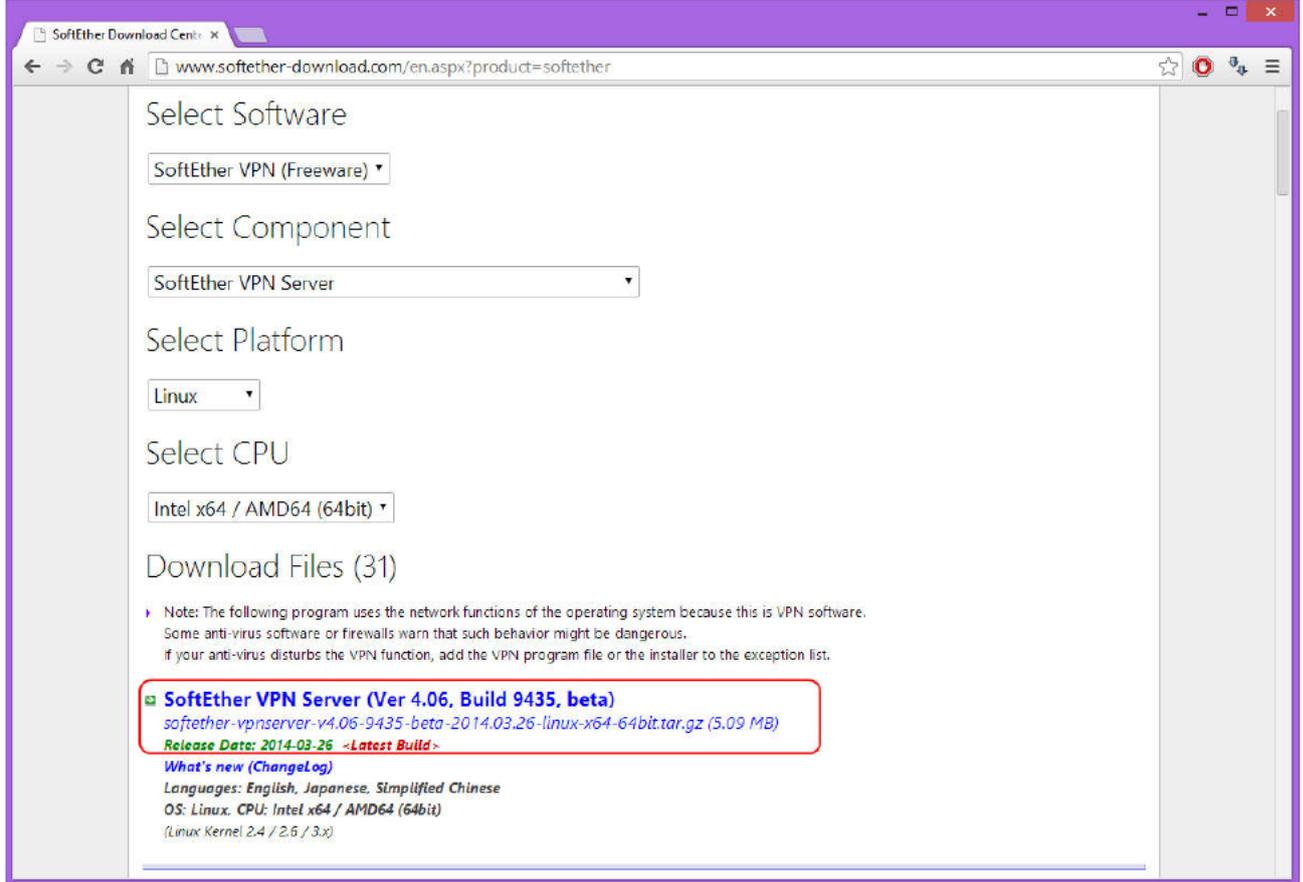
```
root@vpn:~  
[root@vpn ~]# chkconfig ip6tables off  
[root@vpn ~]# chkconfig --list  
auditd          0:off  1:off  2:on   3:on   4:on   5:on   6:off  
blk-availability 0:off  1:on   2:on   3:on   4:on   5:on   6:off  6:off  
crond           0:off  1:off  2:on   3:on   4:on   5:on   6:off  
ip6tables       0:off  1:off  2:off  3:off  4:off  5:off  6:off  
iptables       0:off  1:off  2:on   3:on   4:on   5:on   6:off  
iscsi           0:off  1:off  2:off  3:on   4:on   5:on   6:off  
iscsid          0:off  1:off  2:off  3:on   4:on   5:on   6:off  
lvm2-monitor    0:off  1:on   2:on   3:on   4:on   5:on   6:off  
mdmmonitor     0:off  1:off  2:on   3:on   4:on   5:on   6:off  
multipathd     0:off  1:off  2:off  3:off  4:off  5:off  6:off  
netconsole     0:off  1:off  2:off  3:off  4:off  5:off  6:off  
netfs           0:off  1:off  2:off  3:on   4:on   5:on   6:off  
network        0:off  1:off  2:on   3:on   4:on   5:on   6:off  
postfix        0:off  1:off  2:on   3:on   4:on   5:on   6:off  
rdisc          0:off  1:off  2:off  3:off  4:off  5:off  6:off  
restorecond    0:off  1:off  2:off  3:off  4:off  5:off  6:off  
rsyslog        0:off  1:off  2:on   3:on   4:on   5:on   6:off  
saslauthd      0:off  1:off  2:off  3:off  4:off  5:off  6:off  
sshd           0:off  1:off  2:on   3:on   4:on   5:on   6:off  
udev-post      0:off  1:on   2:on   3:on   4:on   5:on   6:off  
[root@vpn ~]#  
[root@vpn ~]#
```

10. Sunucudaki genel kurulumum bitti. Şimdi VPN Serverı bulacağız.

3. SoftEther VPN Serveri Bulmak ve Indirmek

1. <https://www.softether.org> adresine girdim. Download linkine tıkladım. Download SoftEther VPN linkine tıkladım.

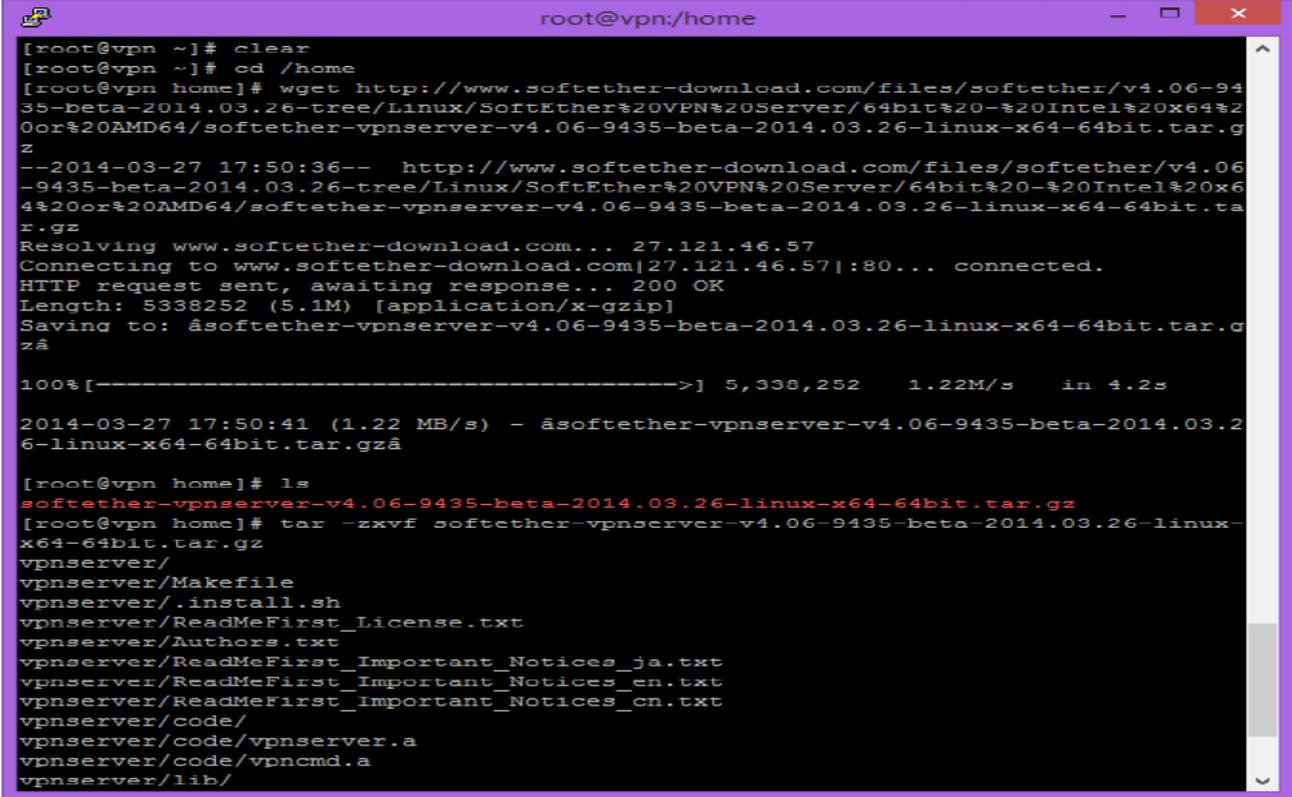
Aşağıdaki seçenekleri seçerek Linux 64 Bit SoftEther VPN Serverın en son versiyonun linkini buldum ve sağ tuş ile kopyaladım.



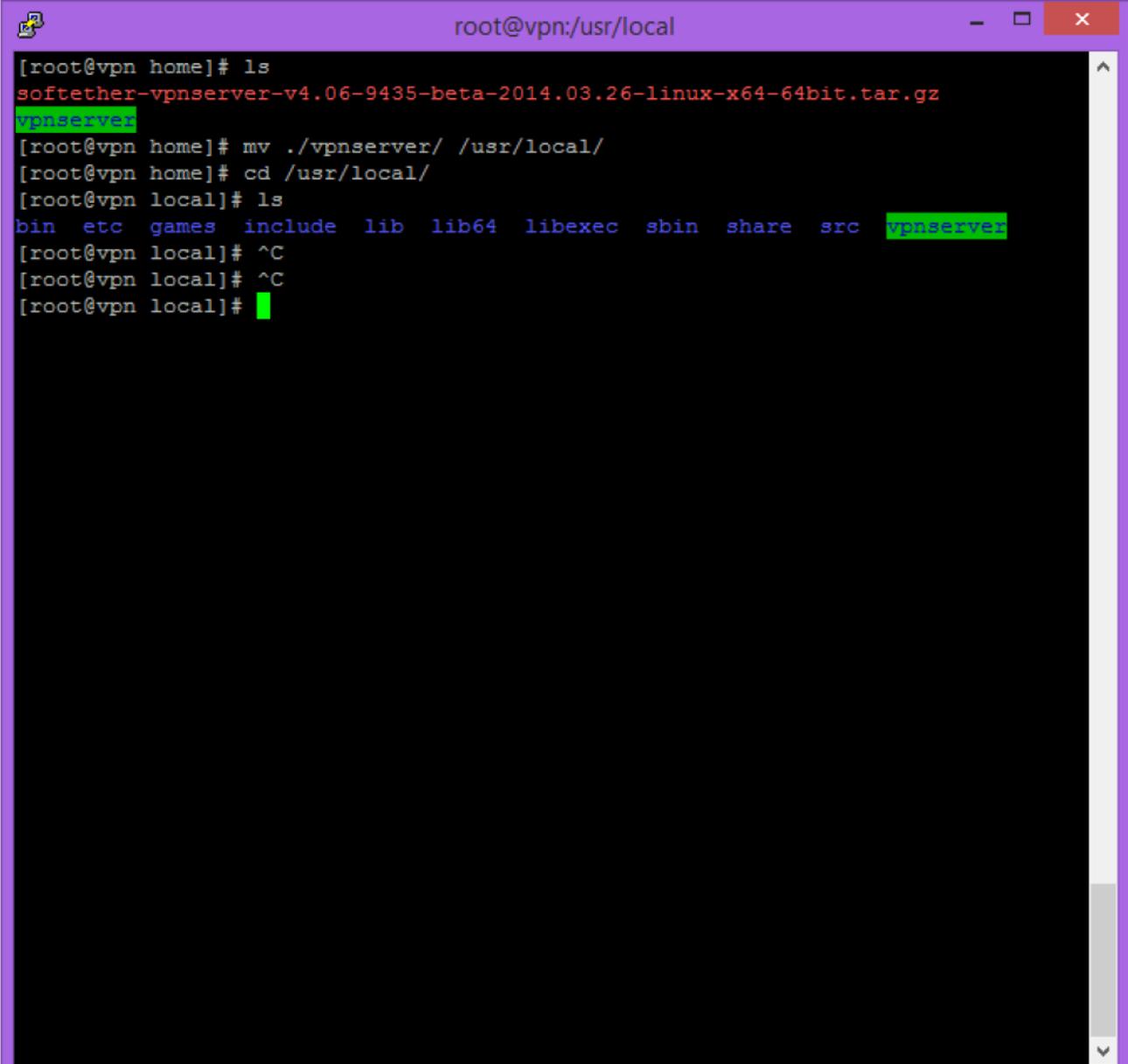
2. Putty aracılığı ile bağlandığım sunucuya geçip aşağıdaki komutları yazdım.

Dikkat ! Linki buradan statik kopyalamayın, gidin en son versiyon ne ise onu indirin. Bu döküman yazıldığı tarihteki son versiyon V4.06-9435-beta idi.

```
clear
cd /home
wget http://....//softether-vpnserver-v4.06-9435.....tar.gz
tar -zxvf softether-vpnserver-v4.06-9435.....tar.gz mv ./vpnserver/ /usr/local/
cd /usr/local/
ls
```



```
root@vpn:/home
[root@vpn ~]# clear
[root@vpn ~]# cd /home
[root@vpn home]# wget http://www.softether-download.com/files/softether/v4.06-9435-beta-2014.03.26-tree/Linux/SoftEther%20VPN%20Server/64bit%20-%20Intel%20x64%20or%20AMD64/softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
--2014-03-27 17:50:36-- http://www.softether-download.com/files/softether/v4.06-9435-beta-2014.03.26-tree/Linux/SoftEther%20VPN%20Server/64bit%20-%20Intel%20x64%20or%20AMD64/softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
Resolving www.softether-download.com... 27.121.46.57
Connecting to www.softether-download.com|27.121.46.57|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5338252 (5.1M) [application/x-gzip]
Saving to: 'softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz'
100%[----->] 5,338,252  1.22M/s  in 4.2s
2014-03-27 17:50:41 (1.22 MB/s) - 'softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz'
[root@vpn home]# ls
softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
[root@vpn home]# tar -zxvf softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
vpnserver/
vpnserver/Makefile
vpnserver/.install.sh
vpnserver/ReadMeFirst_License.txt
vpnserver/Authors.txt
vpnserver/ReadMeFirst_Important_Notices_ja.txt
vpnserver/ReadMeFirst_Important_Notices_en.txt
vpnserver/ReadMeFirst_Important_Notices_cn.txt
vpnserver/code/
vpnserver/code/vpnserver.a
vpnserver/code/vpncmd.a
vpnserver/lib/
```



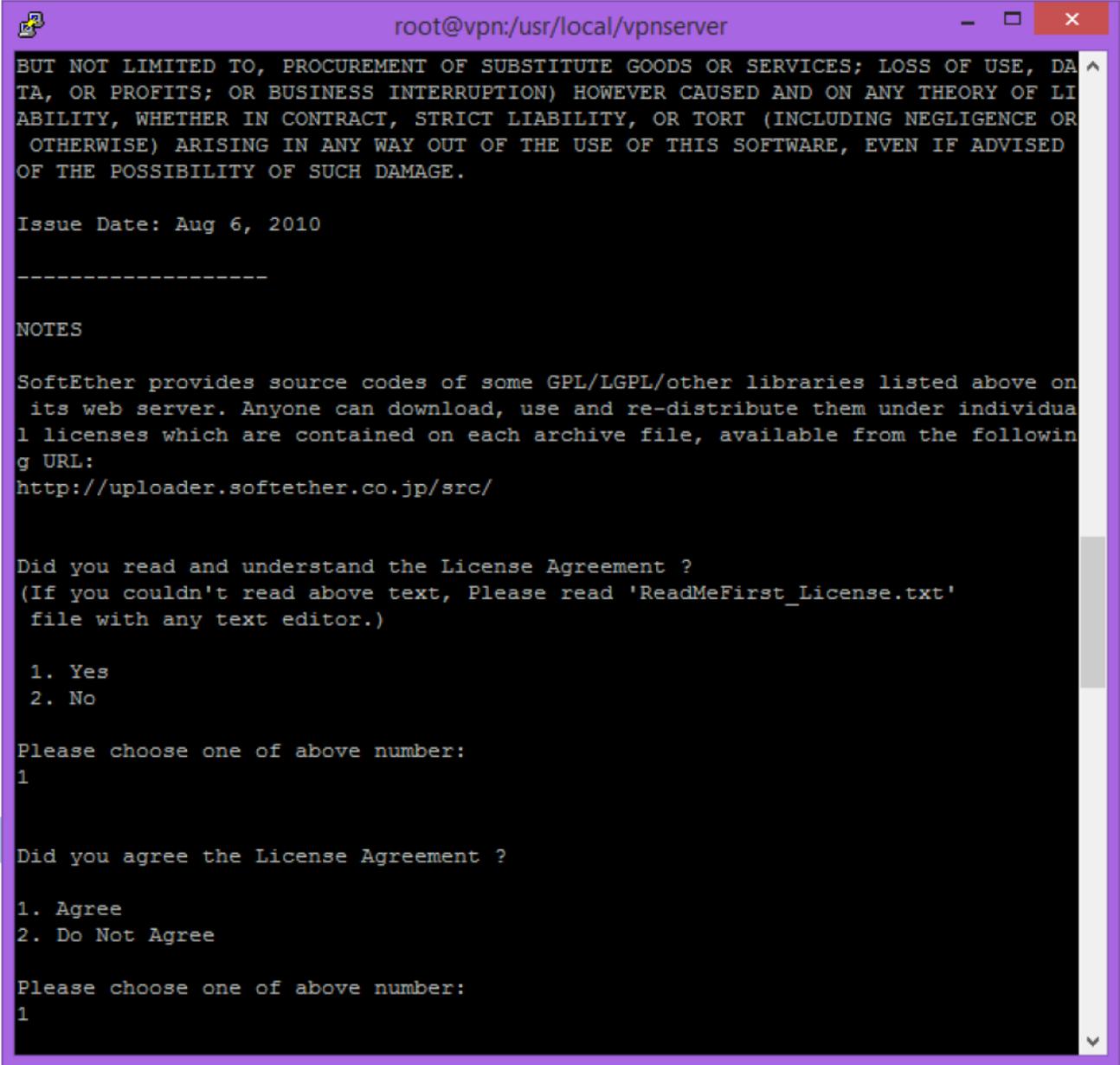
```
root@vpn:/usr/local
[root@vpn home]# ls
softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
vpnserver
[root@vpn home]# mv ./vpnserver/ /usr/local/
[root@vpn home]# cd /usr/local/
[root@vpn local]# ls
bin  etc  games  include  lib  lib64  libexec  sbin  share  src  vpnserver
[root@vpn local]# ^C
[root@vpn local]# ^C
[root@vpn local]#
```

3. Şimdi VPN Serverın kurulumuna geçiyoruz.

Bunun için aşağıdaki komutları kullanacağız.

```
cd /usr/local/vpnserver  
make
```

Daha sonra karşımıza lisans anlaşması geliyor, toplamda 3 kere 1 e basıyoruz.

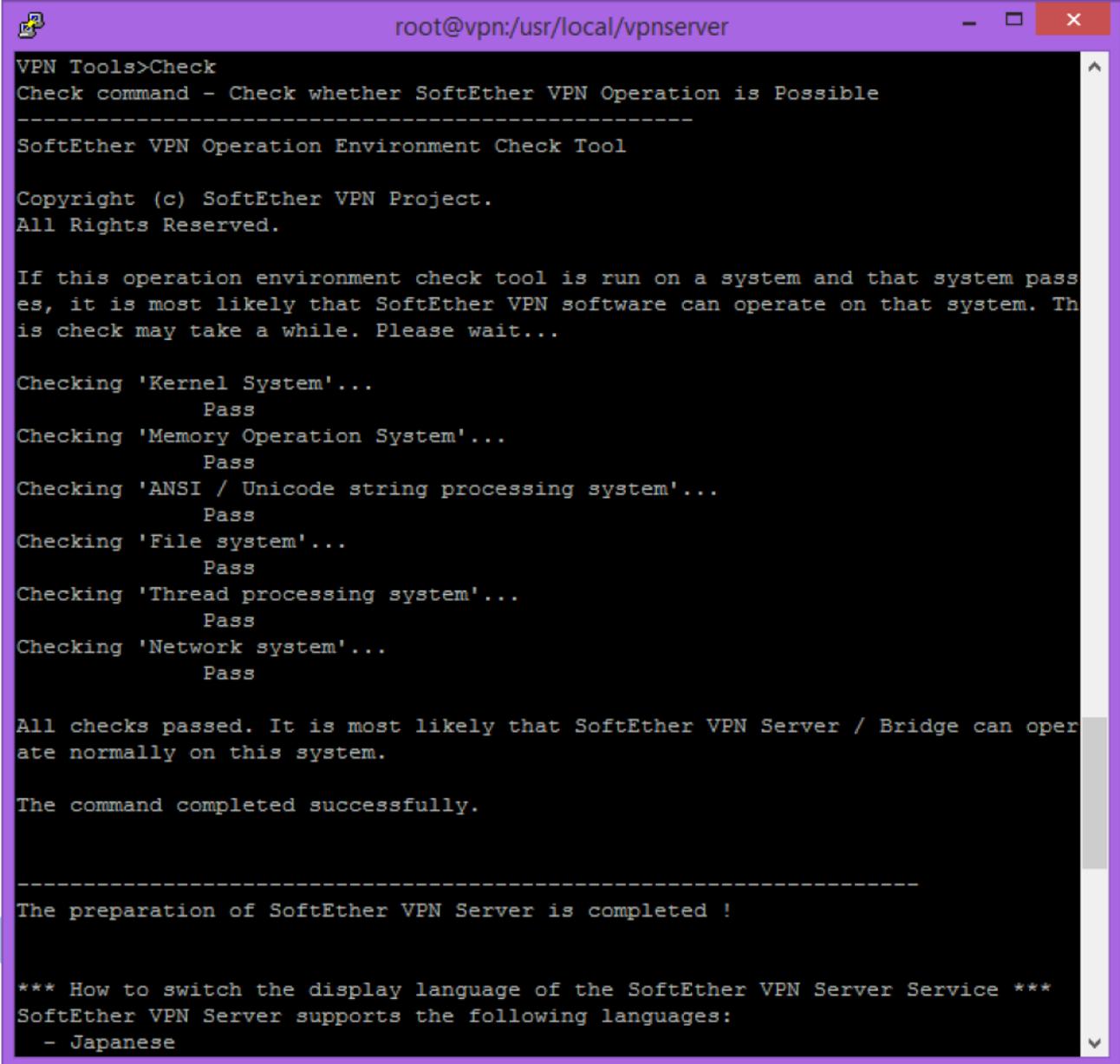


```
root@vpn:/usr/local/vpnserver  
BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DA  
TA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LI  
ABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR  
OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED  
OF THE POSSIBILITY OF SUCH DAMAGE.  
  
Issue Date: Aug 6, 2010  
-----  
  
NOTES  
  
SoftEther provides source codes of some GPL/LGPL/other libraries listed above on  
its web server. Anyone can download, use and re-distribute them under individua  
l licenses which are contained on each archive file, available from the followin  
g URL:  
http://uploader.softether.co.jp/src/  
  
Did you read and understand the License Agreement ?  
(If you couldn't read above text, Please read 'ReadMeFirst_License.txt'  
file with any text editor.)  
  
1. Yes  
2. No  
  
Please choose one of above number:  
1  
  
Did you agree the License Agreement ?  
  
1. Agree  
2. Do Not Agree  
  
Please choose one of above number:  
1
```

4. Kurulum sırasında

VPN Tools > Check

satırlarını arıyoruz ve altında hepsinin PASS olduğundan emin oluyoruz. Aksi takdirde bir sorun var demektir, ayrıca incelemek lazım.



```
root@vpn:/usr/local/vpnserver
VPN Tools>Check
Check command - Check whether SoftEther VPN Operation is Possible
-----
SoftEther VPN Operation Environment Check Tool

Copyright (c) SoftEther VPN Project.
All Rights Reserved.

If this operation environment check tool is run on a system and that system passes, it is most likely that SoftEther VPN software can operate on that system. This check may take a while. Please wait...

Checking 'Kernel System'...
    Pass
Checking 'Memory Operation System'...
    Pass
Checking 'ANSI / Unicode string processing system'...
    Pass
Checking 'File system'...
    Pass
Checking 'Thread processing system'...
    Pass
Checking 'Network system'...
    Pass

All checks passed. It is most likely that SoftEther VPN Server / Bridge can operate normally on this system.

The command completed successfully.

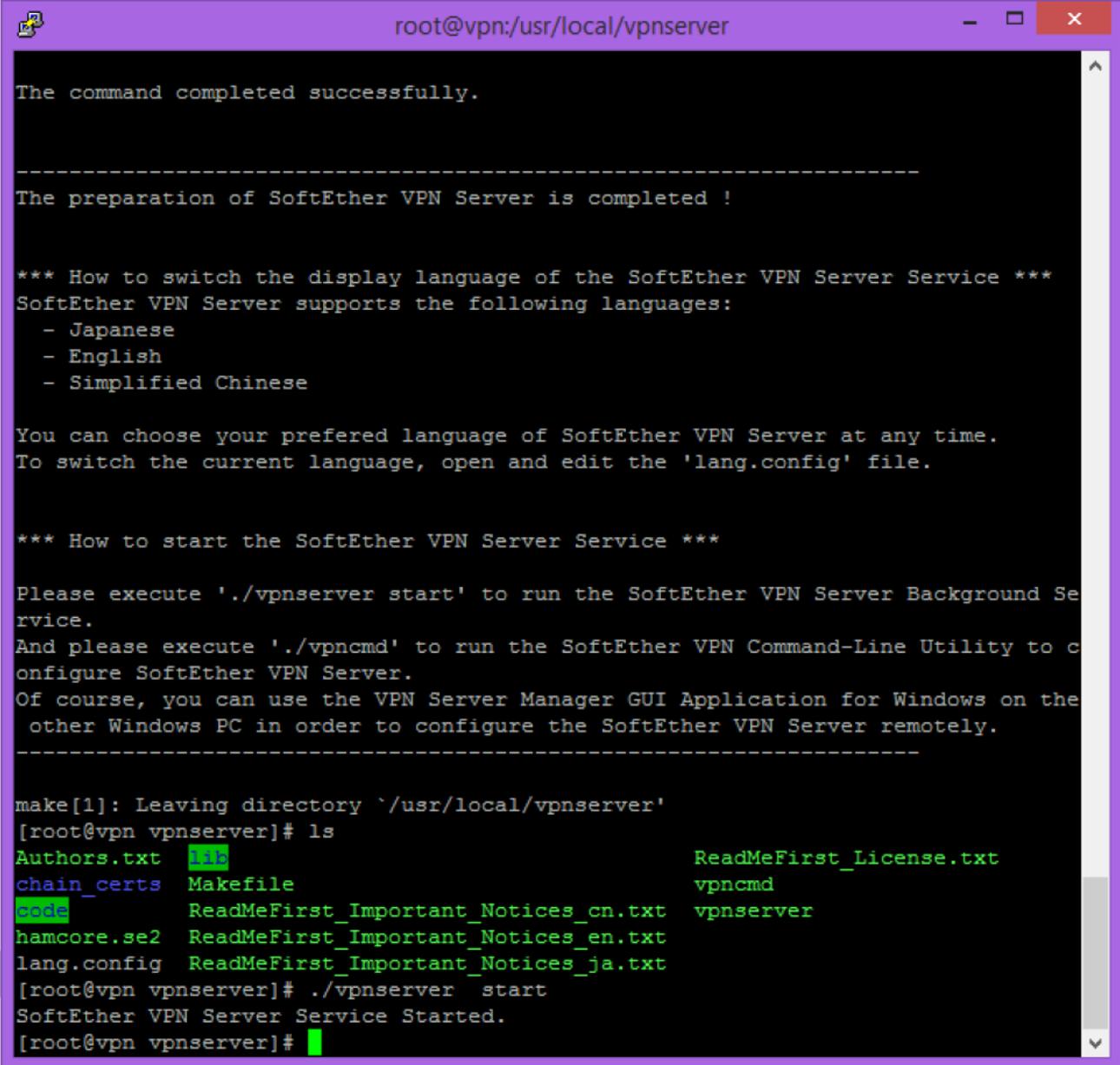
-----
The preparation of SoftEther VPN Server is completed !

*** How to switch the display language of the SoftEther VPN Server Service ***
SoftEther VPN Server supports the following languages:
- Japanese
```

5. Şu anda sunucumuz kuruldu.

```
./vpnservice start
```

komutu ile sunucumuzu başlatıyoruz.



```
root@vpn:/usr/local/vpnservice
The command completed successfully.

-----
The preparation of SoftEther VPN Server is completed !

*** How to switch the display language of the SoftEther VPN Server Service ***
SoftEther VPN Server supports the following languages:
- Japanese
- English
- Simplified Chinese

You can choose your preferred language of SoftEther VPN Server at any time.
To switch the current language, open and edit the 'lang.config' file.

*** How to start the SoftEther VPN Server Service ***

Please execute './vpnservice start' to run the SoftEther VPN Server Background Service.
And please execute './vpncmd' to run the SoftEther VPN Command-Line Utility to configure SoftEther VPN Server.
Of course, you can use the VPN Server Manager GUI Application for Windows on the other Windows PC in order to configure the SoftEther VPN Server remotely.

-----

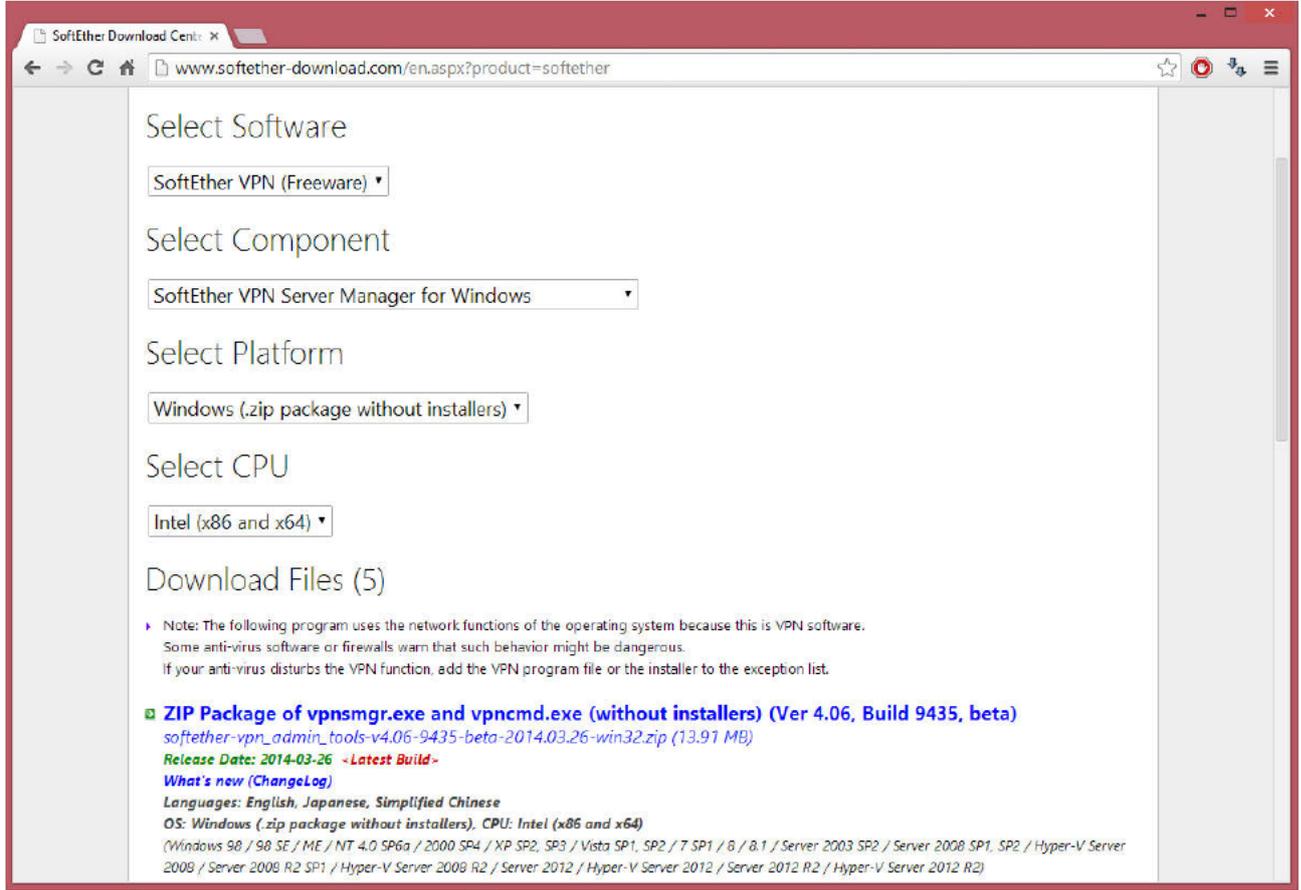
make[1]: Leaving directory `/usr/local/vpnservice'
[root@vpn vpnservice]# ls
Authors.txt      lib                ReadMeFirst_License.txt
chain_certs     Makefile           vpncmd
code             ReadMeFirst_Important_Notices_cn.txt  vpnservice
hamcore.se2     ReadMeFirst_Important_Notices_en.txt
lang.config     ReadMeFirst_Important_Notices_ja.txt
[root@vpn vpnservice]# ./vpnservice start
SoftEther VPN Server Service Started.
[root@vpn vpnservice]#
```

6. Bu andan itibaren sunucu ile işimiz bitti. Windows arayüzlü Management Tool'u kullanarak VPN'imizi konfigure edeceğiz.

4. SoftEther VPN Management Tool'u Bulmak ve İndirmek

1. Sunucunun linkin bulmaktan daha zor değil. Aynı siteye, sunucuyu indirdiğimiz link üzerinde aşağıdaki seçeneği seçiyoruz ve zip dosyasını bilgisayarımıza indiriyoruz.

Dikkat! Ben installer olmayan versiyonunu indiriyorum. Tek exe yönetmek için zaten yeterli.



2. İndirdiğimiz klasörün içerisine giriyoruz ve

vpnsmgr.exe

isimli uygulamayı çalıştırıyoruz.

5. SoftEther VPN Management Tool ile SoftEther VPN Sunucusunun Konfigure Edilmesi

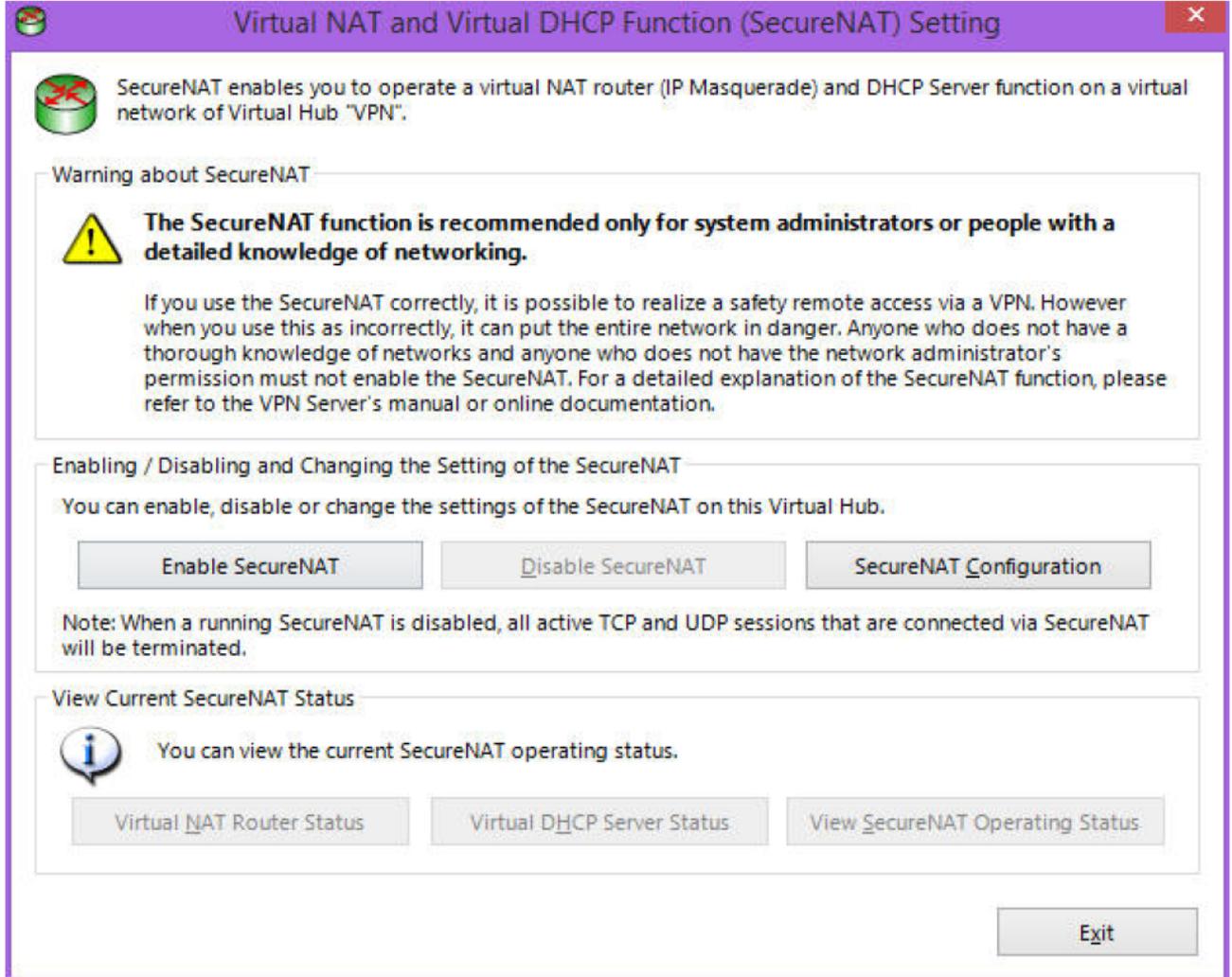
1. Uygulamayı çalıştırıyor ve New Settings butonuna tıklıyoruz.



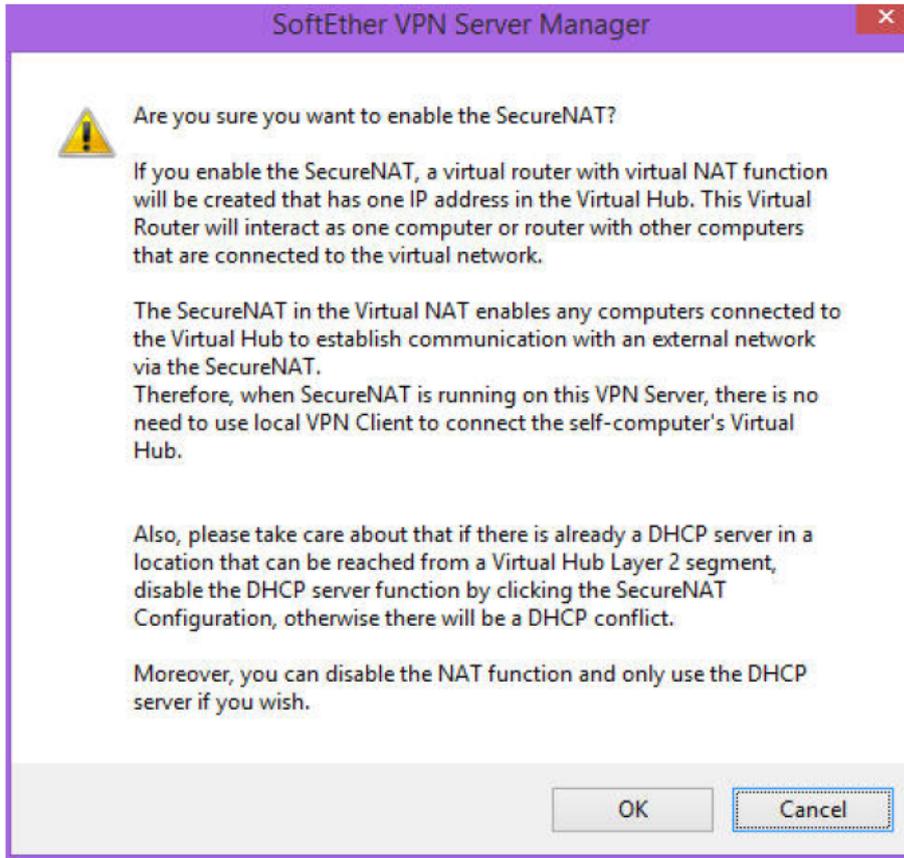
2. Setting Name bölümüne bir isim girin. VPN uygun.

Host Name kısmına sunucunun IP adresini girin.

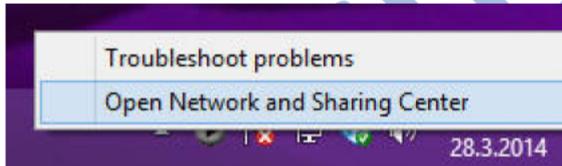
Şifre kısmını boş bırakın ve OK tuşuna basın.



3. Ana bağlantı penceresinde Connect tuşuna basın.

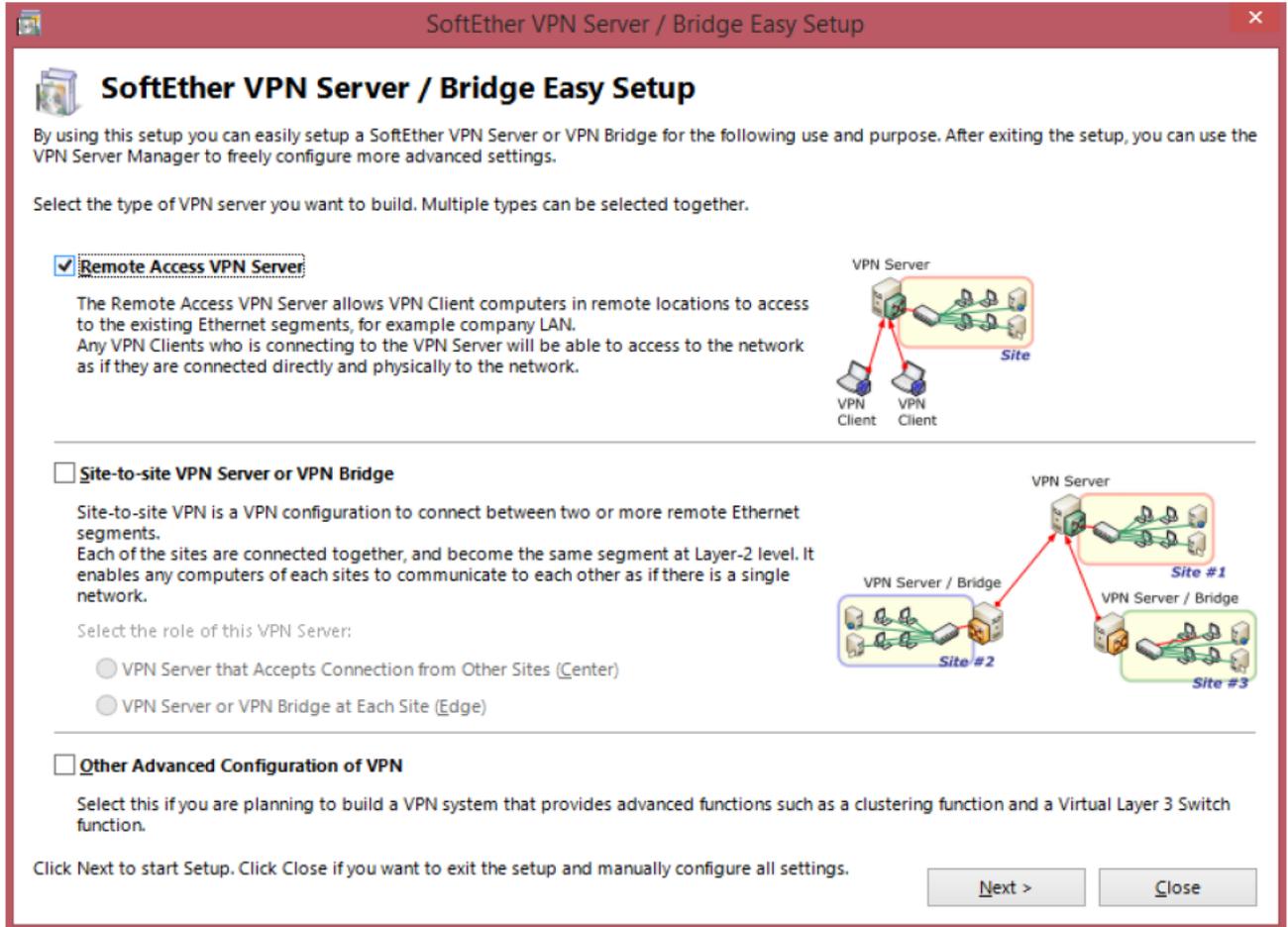


4. Sunucumuza VPN için şifre belirlemediğimiz için yeni şifre belirleme penceresi ekrana geliyor. Yeni şifrenizi 2 kere girerek OK tuşuna basın.



5. Önümüze gelen pencerede Remote Access VPN'i seçiyoruz. Diğer seçenekleri burada anlatmıyorum, eğer isteyen var ise, yukarda verdiğim wikipedia linki üzerinden inceleyebilirsiniz.

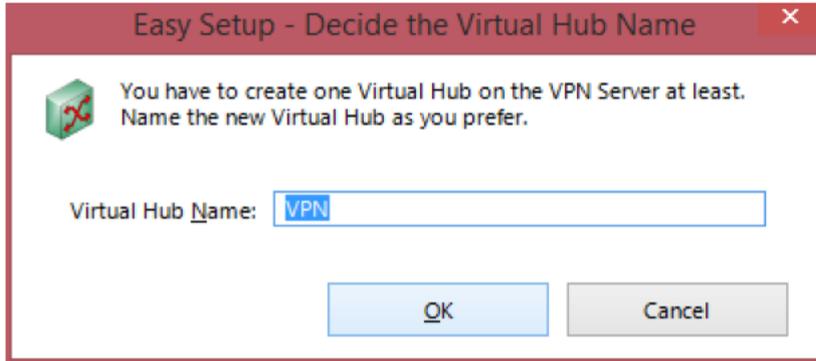
Remote Access VPN ile, kendi cihazlarımızı, Amsterdam'a bağlayacağız ve oradan internete çıkış yapacağız.



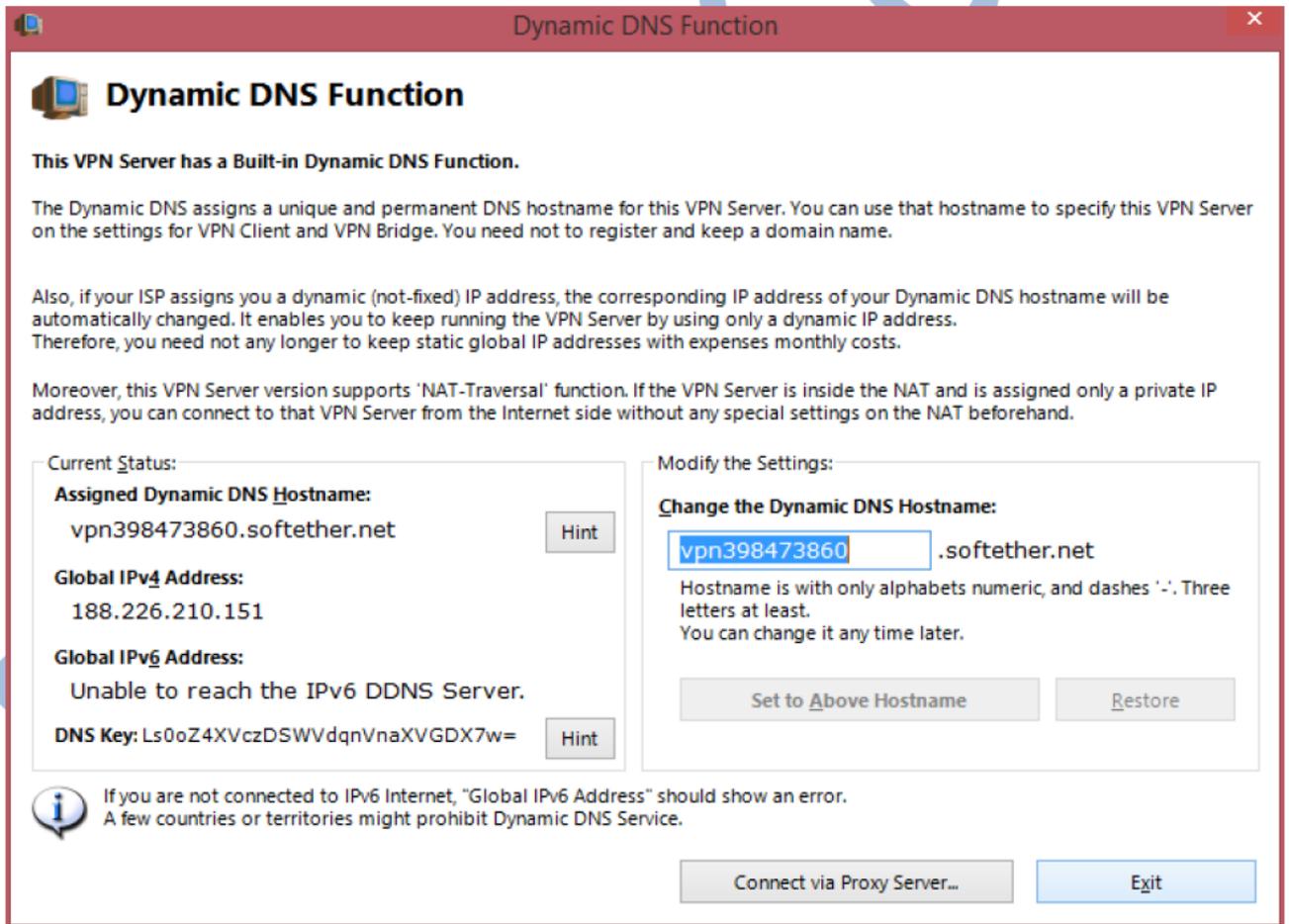
6. VPN initialize edilecek diyor, OK diyoruz.



- 7. VPN'in çalışması için sunucu üzerinde oluşturulacak sanal hub'ın ismini belirlememiz isteniyor. VPN yazıp geçiyoruz.



- 8. SoftEther istediğiniz taktide, IP adresi yerine dinamik olarak dns atayabiliyor. Ben bu özelliği kullanmak yerine, kendi domain adresimden IP'ye redirect yapıyorum, ama siz bunu kullanabilirsiniz.



9. Burası önemli, L2TP Over IPsec'i seçiyoruz. Bu sayede tüm cihazlarımızı herhangi bir client kullanmadan güvenli bir şekilde sunucumuza bağlayacağız.

Hemen altında yer alan IPsec Common Settings kısmına, bir şifre giriyoruz, bu şifreyi de bir yere kaydediyoruz. İlerde bağlanırken lazım olacak.

IPsec / L2TP / EtherIP / L2TPv3 Settings
✕



IPsec / L2TP / EtherIP / L2TPv3 Server Settings

Virtual Hubs on the VPN Server can accept Remote-Access VPN connections from L2TP-compatible PCs, Mac OS X and Smartphones, and also can accept EtherIP / L2TPv3 Site-to-Site VPN Connection.

L2TP Server (Remote-Access VPN Server Function)

VPN Connections from Smartphones suchlike iPhone, iPad and Android, and also from built-in VPN Clients on Mac OS X and Windows can be accepted.

Enable L2TP Server Function (L2TP over IPsec)
Make VPN Connections from iPhone, iPad, Android, Windows, and Mac OS X acceptable.

Enable L2TP Server Function (Raw L2TP with No Encryptions)
It supports special VPN Clients which uses L2TP with no IPsec encryption.



 Users should specify their username such as "Username@Target Virtual Hub Name" to connect this L2TP Server. If designation of a Virtual Hub is omitted, the below Hub will be used as the target.

Default Virtual Hub in a case of omitting a name of Hub on the Username:

EtherIP Server Function (Site-to-Site VPN Connection)

Router products which are compatible with EtherIP / L2TPv3 over IPsec can connect to Virtual Hub on the VPN Server and establish Layer-2 (Ethernet) Bridging.

Enable EtherIP / L2TPv3 over IPsec Server Function



[EtherIP / L2TPv3 Detail Settings](#)

IPsec Common Settings

IPsec Pre-Shared Key:

IPsec Pre-Shared Key is also called "PSKs" or "Secrets". Specify it with around eight ASCII characters, and let all VPN users know.

10. VPN Session Relay özelliği kullanmayacağız, direk Disable VPN Azure'e tıklayıp OK tuşuna basıyoruz.

VPN Azure Cloud VPN Service (Free)

VPN Azure makes it easier to establish a VPN Session from your home PC to your office PC. While a VPN connection is established, you can access to any other servers on the private network of your company.

You don't need a global IP address on the office PC (VPN Server). It can work behind firewalls or NATs. No network administrator's configuration required. You can use the built-in SSTP-VPN Client of Windows in your home PC.

VPN Azure VPN Azure is a cloud VPN service operated by SoftEther VPN Project. VPN Azure is free of charge and available to anyone. Press the right button to see details and how-to-use instructions.

VPN Azure Setting

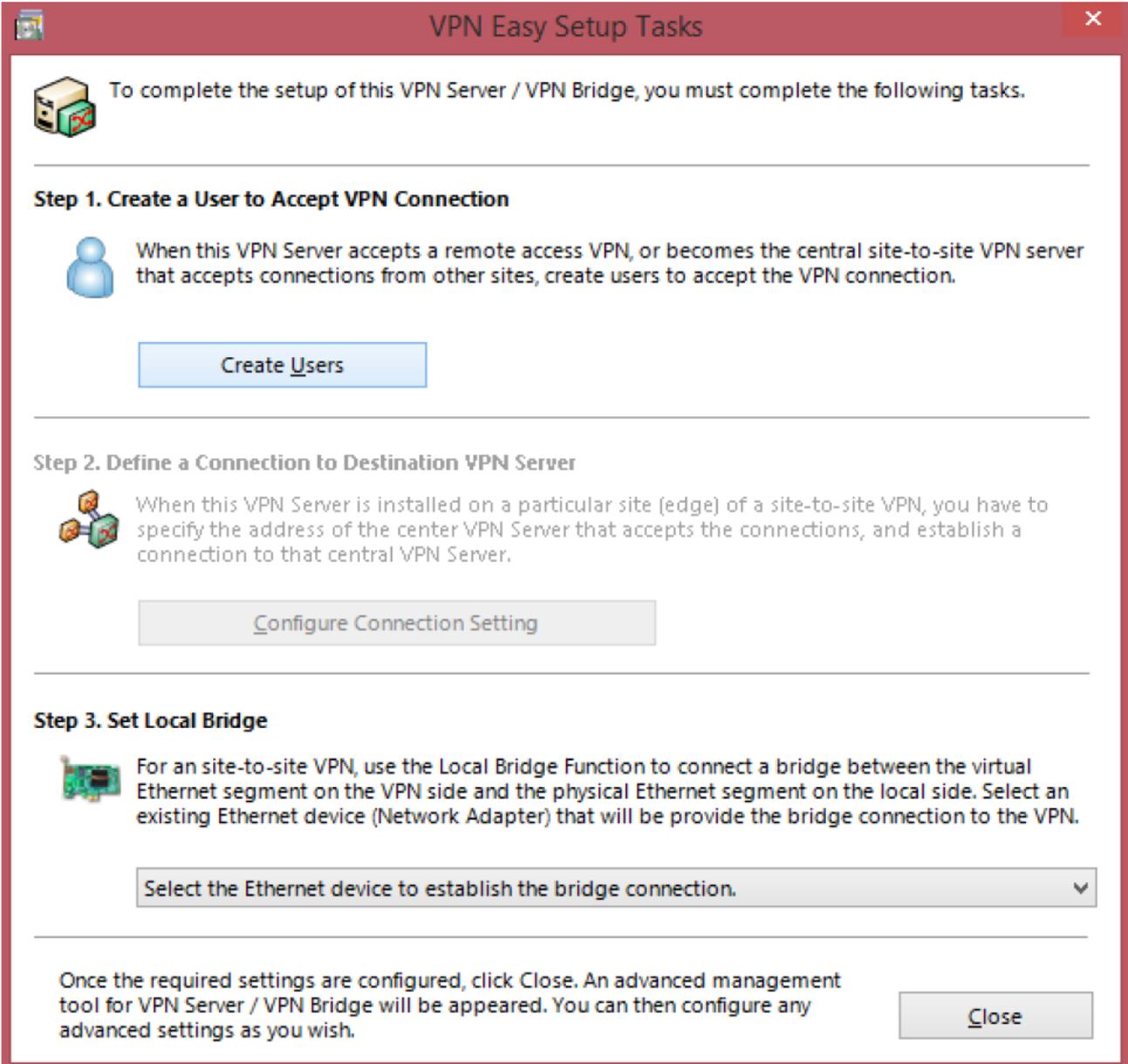
Enable VPN Azure
Status: Not Connected

Disable VPN Azure

How to Use VPN Azure (Visit the Web)

OK

11. Kullanıcı oluşturma penceresine geliyoruz, Create Users butonuna tıklıyoruz.



VPN Easy Setup Tasks

To complete the setup of this VPN Server / VPN Bridge, you must complete the following tasks.

Step 1. Create a User to Accept VPN Connection

 When this VPN Server accepts a remote access VPN, or becomes the central site-to-site VPN server that accepts connections from other sites, create users to accept the VPN connection.

Step 2. Define a Connection to Destination VPN Server

 When this VPN Server is installed on a particular site (edge) of a site-to-site VPN, you have to specify the address of the center VPN Server that accepts the connections, and establish a connection to that central VPN Server.

Step 3. Set Local Bridge

 For an site-to-site VPN, use the Local Bridge Function to connect a bridge between the virtual Ethernet segment on the VPN side and the physical Ethernet segment on the local side. Select an existing Ethernet device (Network Adapter) that will be provide the bridge connection to the VPN.

Once the required settings are configured, click Close. An advanced management tool for VPN Server / VPN Bridge will be appeared. You can then configure any advanced settings as you wish.

12. Kullanıcı adı giriyoruz, Auth Type kısmından Password Authentication'ı seçiyoruz. Password Authentication Settings kısından, giriş için kullanacağımız şifreyi giriyoruz.

Ok tuşuna basıyoruz.

Create New User

User Name:

Full Name:

Note:

Group Name (Optional):

Set the Expiration Date for This Account

29. 3.2014 00:00:00

Auth Type:

- Anonymous Authentication
- Password Authentication
- Individual Certificate Authentication
- Signed Certificate Authentication
- RADIUS Authentication
- NT Domain Authentication

RADIUS or NT Domain Authentication Settings:

Specify User Name on Authentication Server

User Name on Authentication Server:

Security Policy

Set Security Policy

Password Authentication Settings:

Password:

Confirm Password:

Individual Certificate Authentication Settings:

The users using 'Individual Certificate Authentication' will be allowed or denied connection depending on whether the SSL client certificate completely matches the certificate that has been set for the user beforehand.

Signed Certificate Authentication Settings:

Verification of whether the client certificate is signed is based on a certificate of a CA trusted by this Virtual Hub.

Limit Common Name (CN) Value

Limit Values of the Certificate Serial Number

Note: Enter hexadecimal values. (Example: 0155ABCDEF)

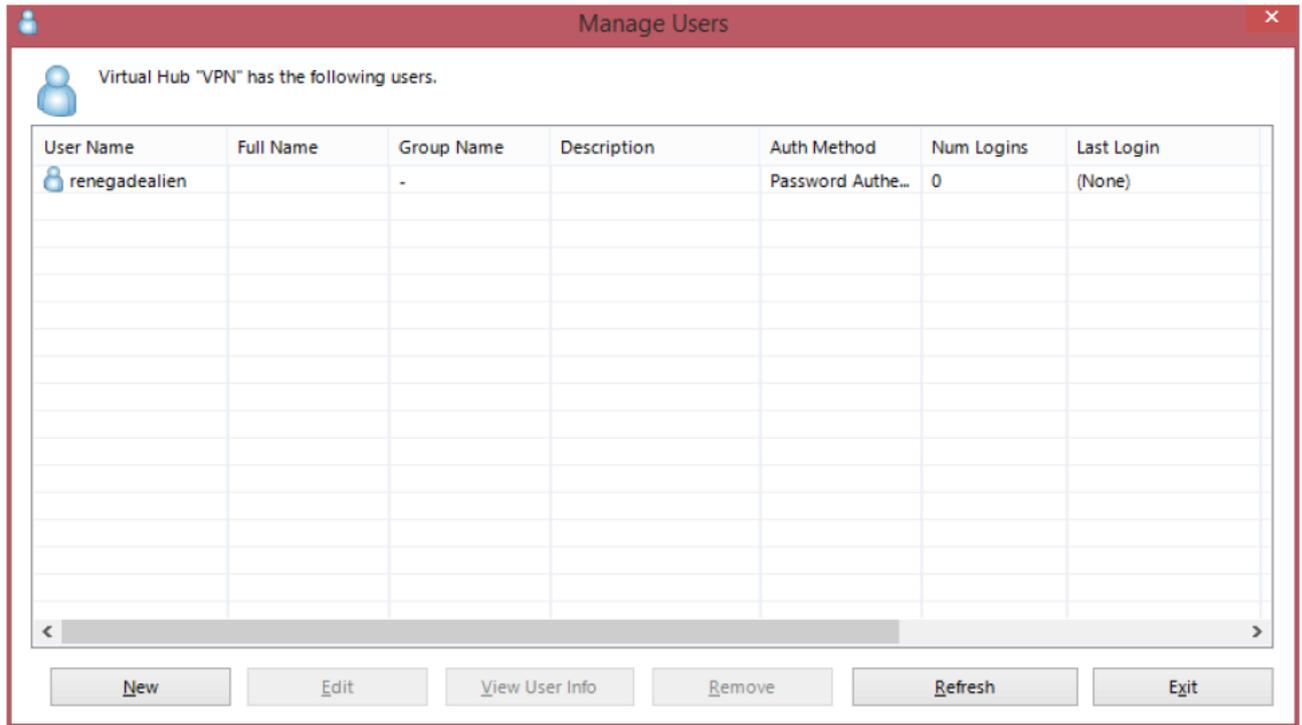
Hint: Define a user object with username "*" (asterisk) in order to accept a login attempt of a user which does not match any of registered explicit user objects. Such a special user will use the external user-authentication server to verify the login.

13. Kullanıcı kaydımız başarı ile tamamlandı.

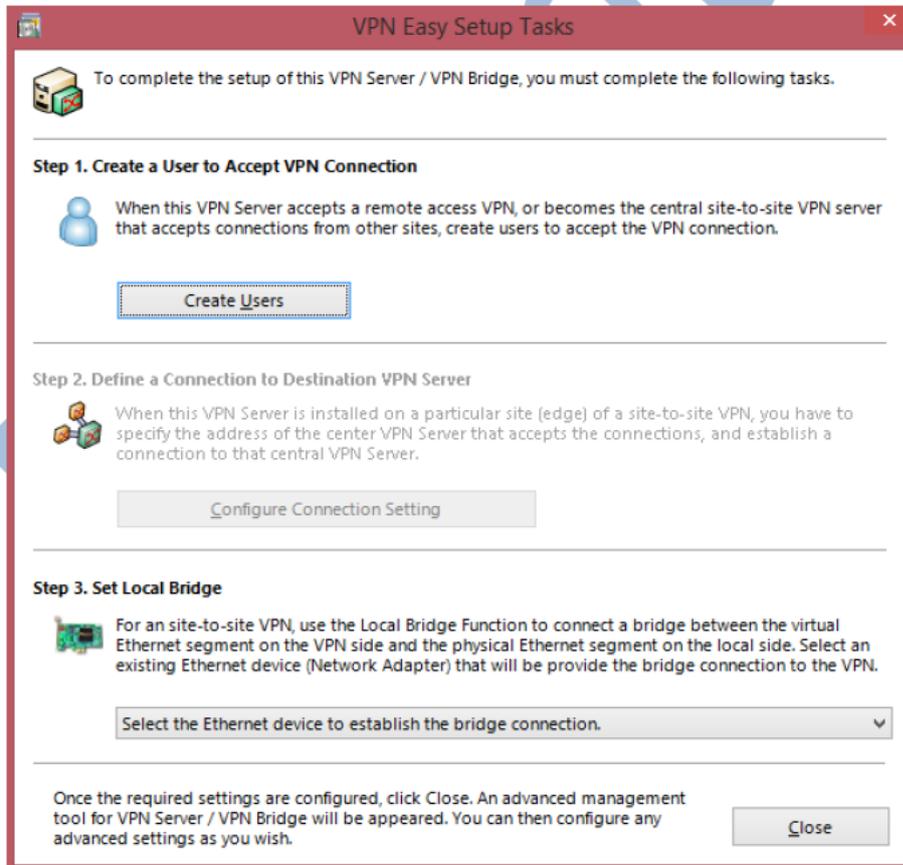
SoftEther VPN Server Manager

User renegadealien has been created.

14. Ekranda VPN adlı HUB'a bağlı kullanıcılar görüntüleniyor. Exit diyerek çıkıyoruz.



15. Close diyerek ekranı kapatıyoruz.



16. Şu anda VPN'imiz kuruldu.

vpn.renegadealien.com - SoftEther VPN Server Manager

Manage VPN Server "188.226.210.151"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Online	Standalone	1	0	0	0	0

[Manage Virtual Hub](#)
[Online](#)
[Offline](#)
[View Status](#)
[Create a Virtual Hub](#)
[Properties](#)
[Delete](#)

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

[Create](#)
[Delete](#)
[Start](#)
[Stop](#)

VPN Server and Network Information and Settings:

[Encryption and Network](#)
[Clustering Configuration](#)

[View Server Status](#)
[Clustering Status](#)

[About this VPN Server](#)
[Show List of TCP/IP Connections](#)

[Edit Config](#)

[Local Bridge Setting](#)
[Layer 3 Switch Setting](#)

[Dynamic DNS Setting](#)
[VPN Azure Setting](#)

[IPsec / L2TP Setting](#)

[OpenVPN / MS-SSTP Setting](#)

Refresh [Exit](#)

Current DDNS Hostname: vpn398473860.softether.net

Tahribat

17. Kurulumun ardından, şu anda aslında network bağlantısı yapabilecek durumdayız. Fakat, sunucuya bağlanacak clientların IP alabilmesi için DHCP ve bağlanan kullanıcıların internete çıkarken sunucunun reel IP'sini kullanabilmeleri için NAT kurulumu yapacağız. Bunu için virtual hubımızı seçiyoruz ve Manage Virtual Hub butonuna basıyoruz.

vpn.renegadealien.com - SoftEther VPN Server Manager

Manage VPN Server "188.226.210.151"

Virtual Hub Name	Status	Type	Users	Groups	Sessions	MAC Tables	IP Tables
VPN	Online	Standalone	1	0	0	0	0

[Manage Virtual Hub](#)
[Online](#)
[Offline](#)
[View Status](#)
[Create a Virtual Hub](#)
[Properties](#)
[Delete](#)

Management of Listeners:

Listener List (TCP/IP port):

Port Number	Status
TCP 443	Listening
TCP 992	Listening
TCP 1194	Listening
TCP 5555	Listening

[Create](#)
[Delete](#)
[Start](#)
[Stop](#)

VPN Server and Network Information and Settings:

[Encryption and Network](#)
[Clustering Configuration](#)
[View Server Status](#)
[Clustering Status](#)
[About this VPN Server](#)
[Show List of TCP/IP Connections](#)
[Edit Config](#)

[Local Bridge Setting](#)
[Layer 3 Switch Setting](#)
[IPsec / L2TP Setting](#)
[OpenVPN / MS-SSTP Setting](#)

[Dynamic DNS Setting](#)
[VPN Azure Setting](#)
[Refresh](#)
[Exit](#)

Current DDNS Hostname: vpn398473860.softether.net

18. Virtual Nat and Virtual DHCP Server butonuna tikliyoruz.

Management of Virtual Hub - 'VPN'

Virtual Hub 'VPN'

Management of Security Database:

- Manage Users**
Add, delete or edit user accounts.
- Manage Groups**
Add, delete or edit groups.
- Manage Access Lists**
Add or delete access lists (Packet filtering rules).

Virtual Hub Settings:

- Virtual Hub Properties**
Configure this Hub.
- Authentication Server Setting**
Use external RADIUS authentication server for user authentication.
- Manage Cascade Connections**
Establish Cascade Connection to Hubs on local or remote VPN Servers.

Current Status of this Virtual Hub:

Item	Value
Virtual Hub Name	VPN
Status	Online
Type	Standalone
SecureNAT	Disabled
Sessions	0
Access Lists	0
Users	1
Groups	0
MAC Tables	0

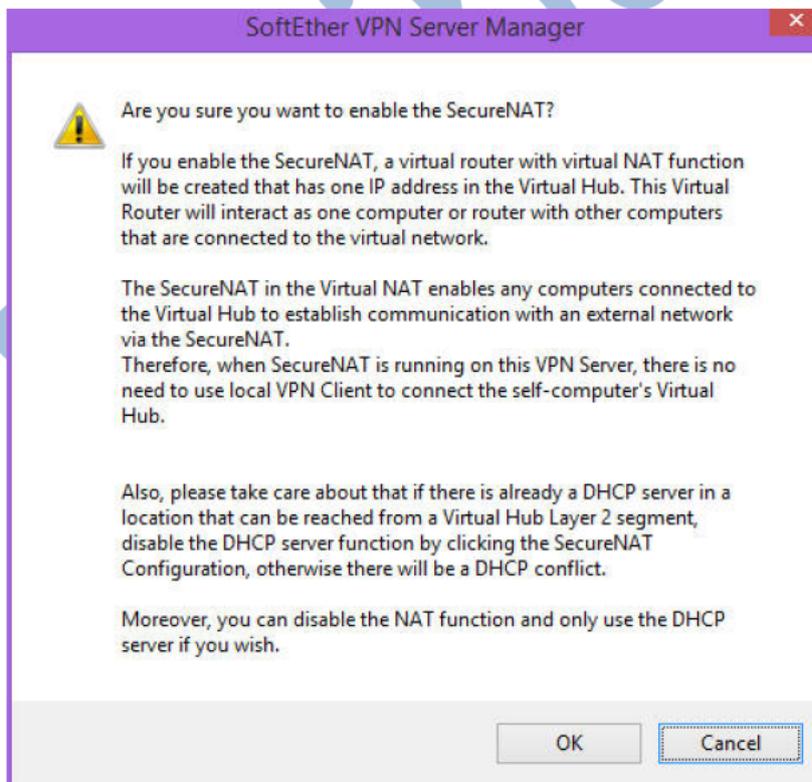
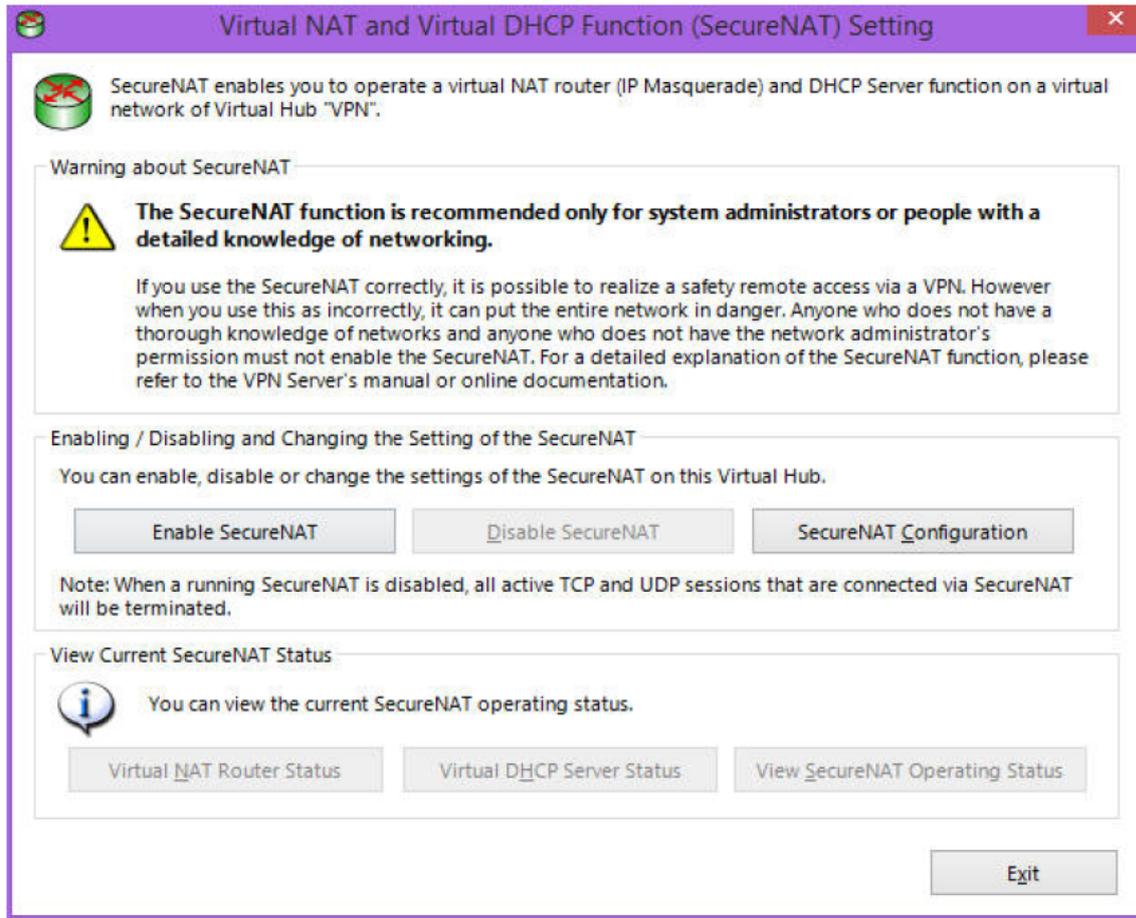
Other Settings:

- Log Save Setting** | **Log File List**
Configure settings of log saving function.
- Trusted CA Certificates** | **Revoked Certs**
Manage trusted CA certificates.
- Virtual NAT and Virtual DHCP Server (SecureNAT)**
Secure NAT is available on this Virtual Hub. You can run Virtual NAT and Virtual DHCP.

VPN Sessions Management:

- Manage Sessions**
- Exit**

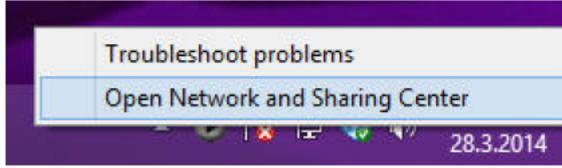
19. Enable Secure Nat butonuna tıklıyor, gelen ekrandan OK butonuna tıklıyoruz.



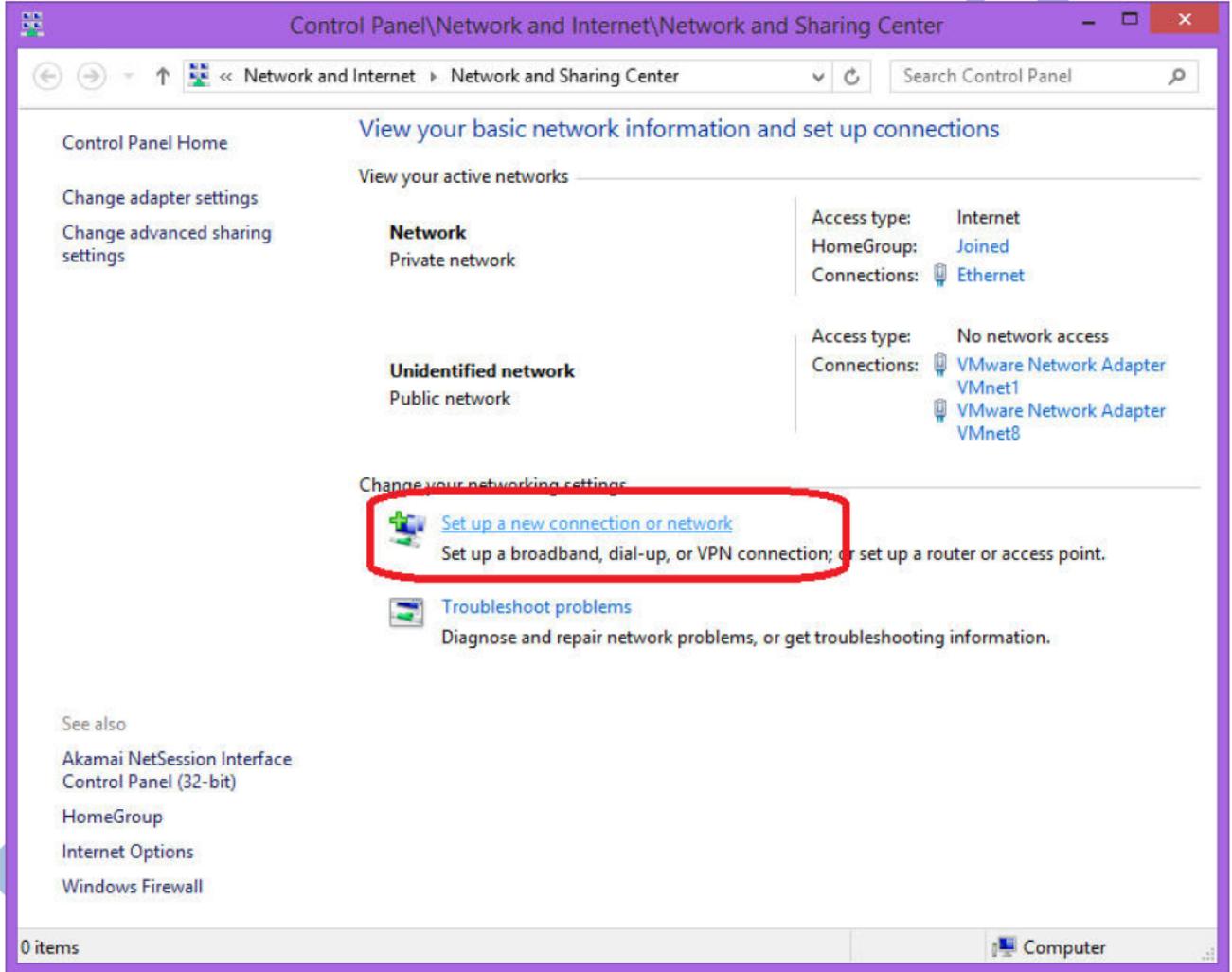
20. Şu anda VPN sunucu kurulumumuz bitti.

6. Windows7 / Windows 8 Üzerinden VPN'e Bağlanmak

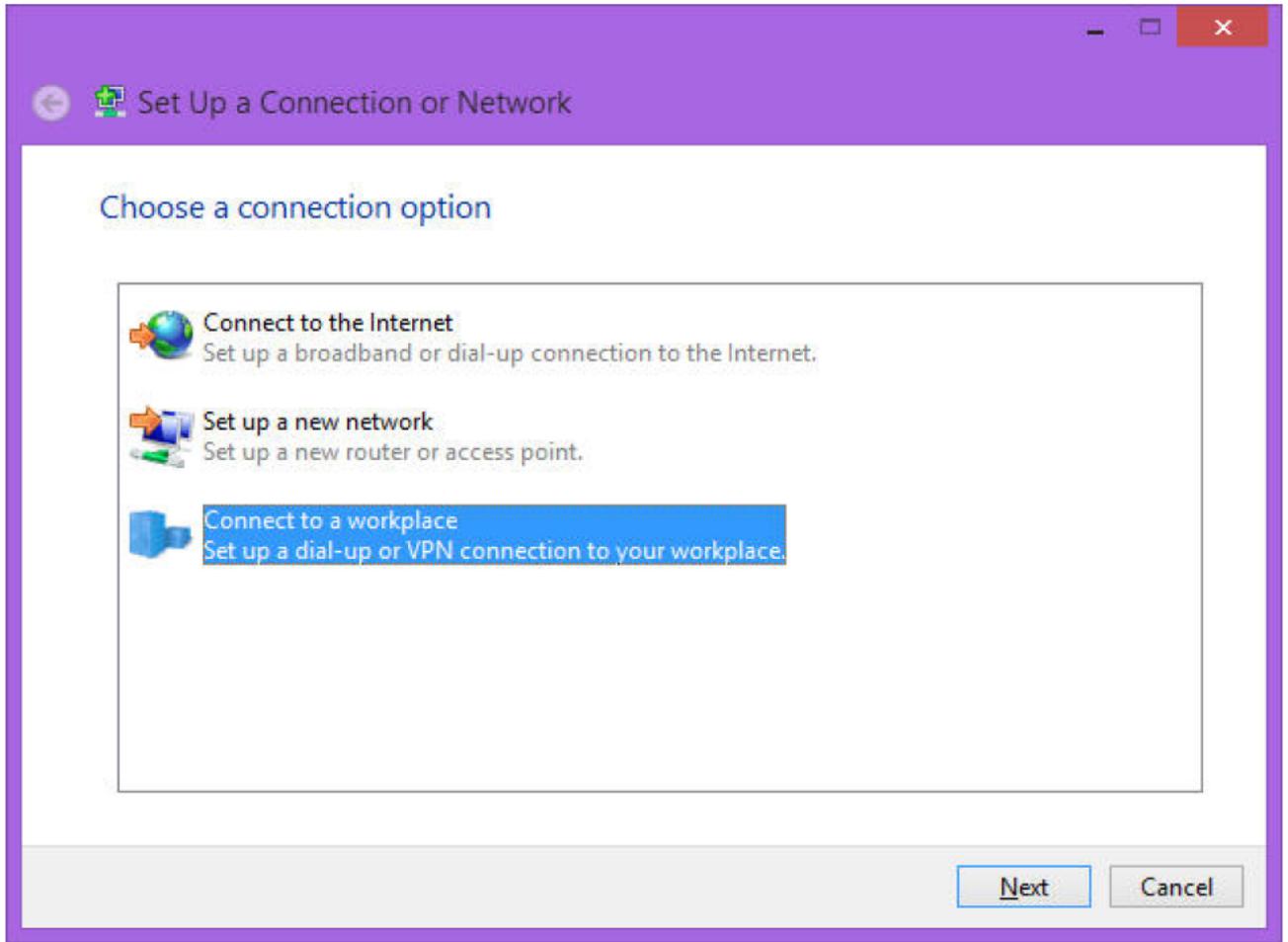
1. Open Network and Sharing Center butonuna tıklıyoruz.



2. Set up a new connection or network linkine tıklıyoruz.

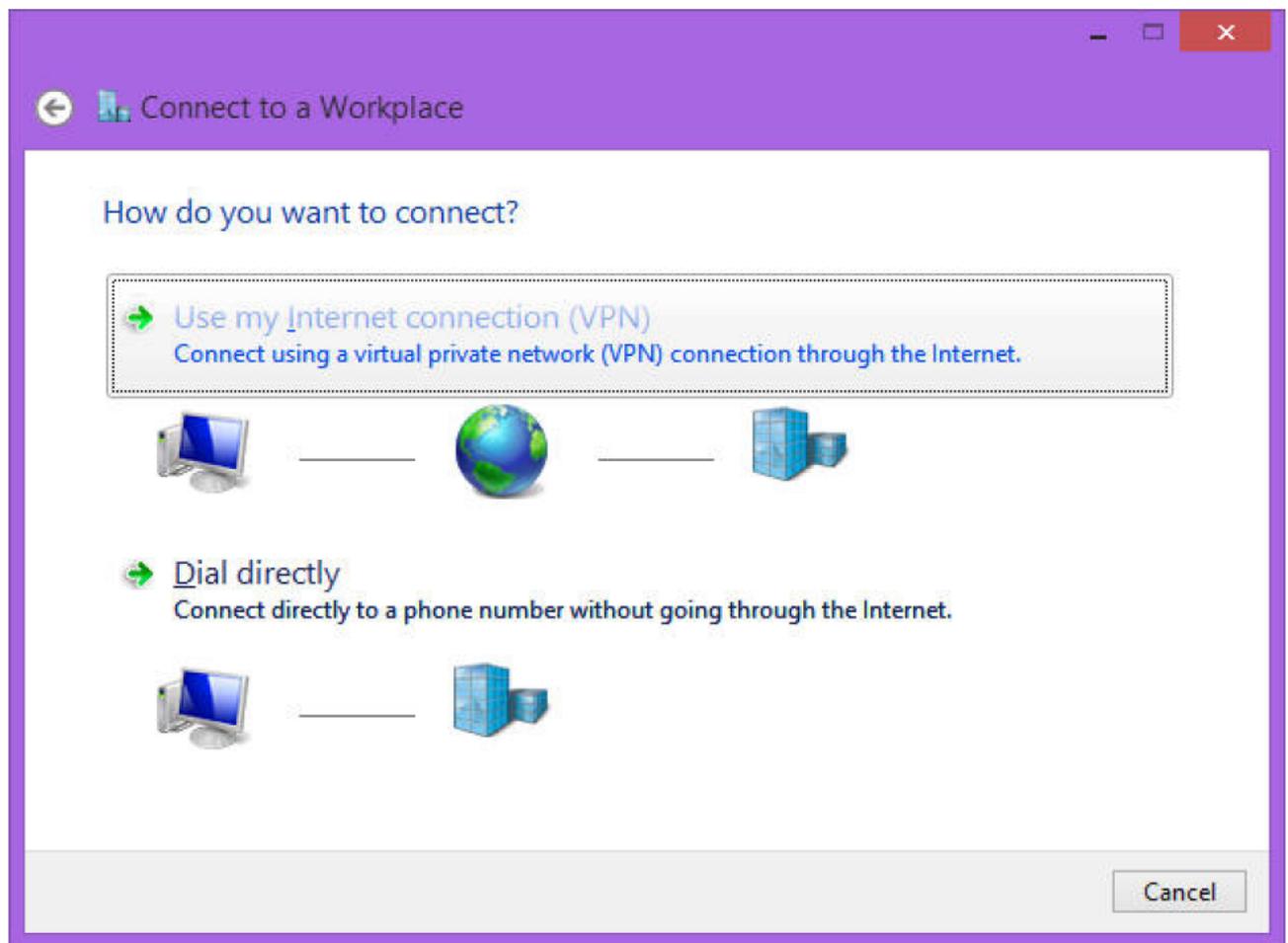


3. VPN bağlantısını seçiyoruz.



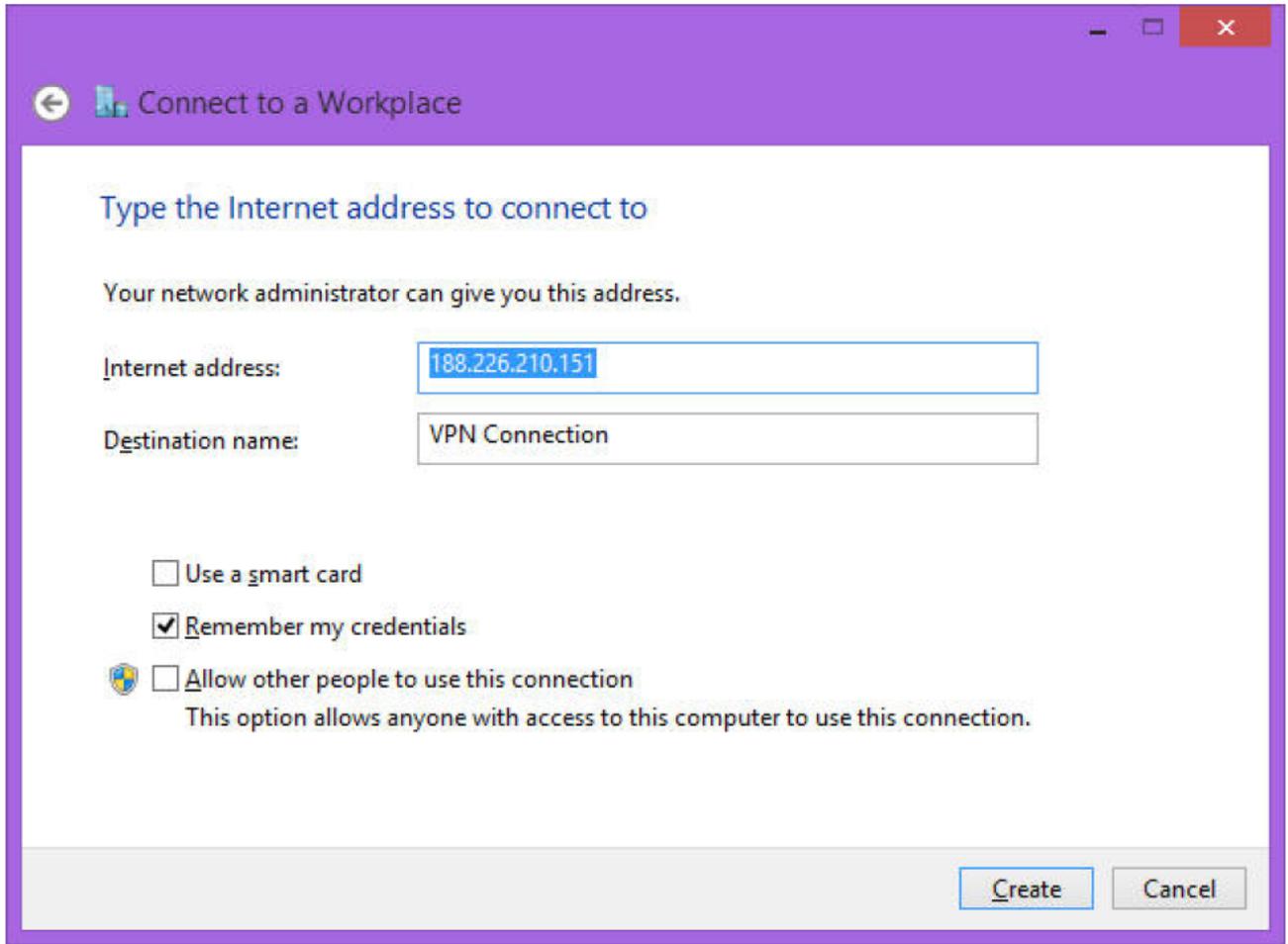
Tahribat

4. Use My Internet Connection botununa tıklıyoruz.

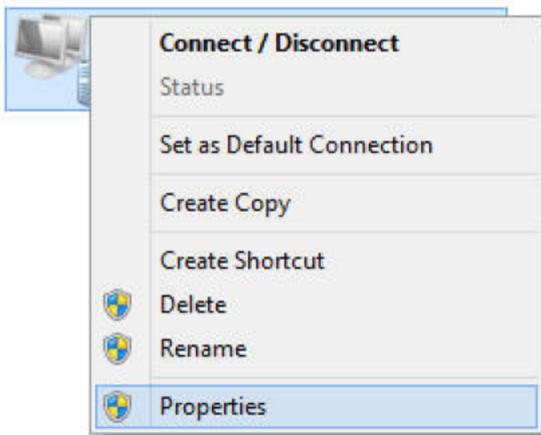


Tahribat

5. Sunucunun adresini giriyoruz ve bir isim veriyoruz.

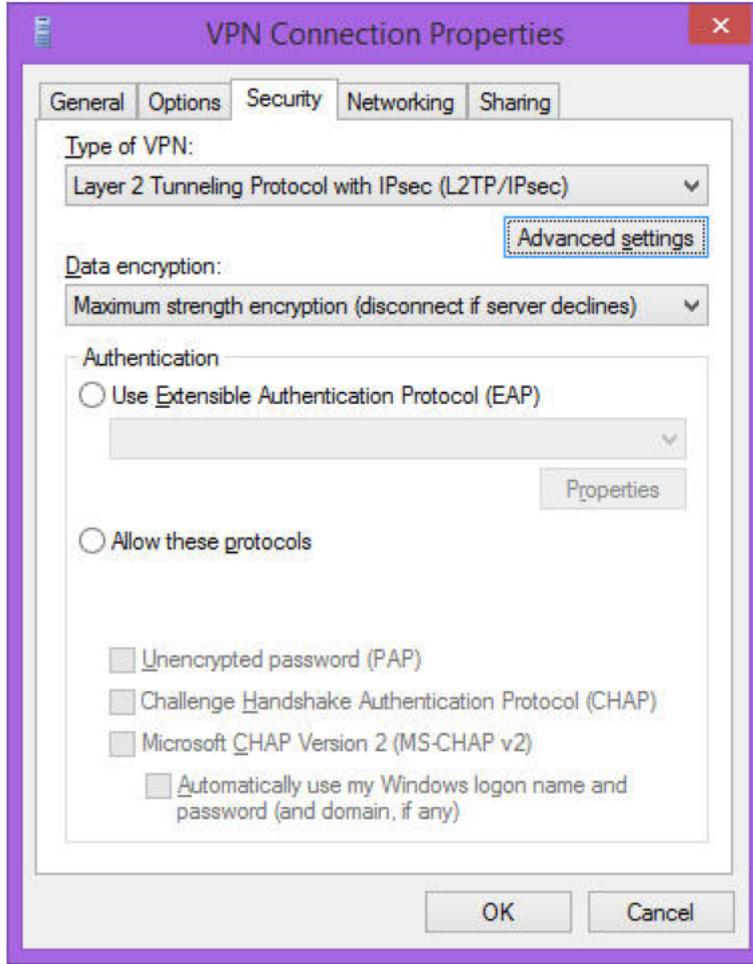


6. Ağ Bağlantılarına giriyoruz. VPN Connection isimli Connection'u bulup sağ tuş, properties penceresini açıyoruz.

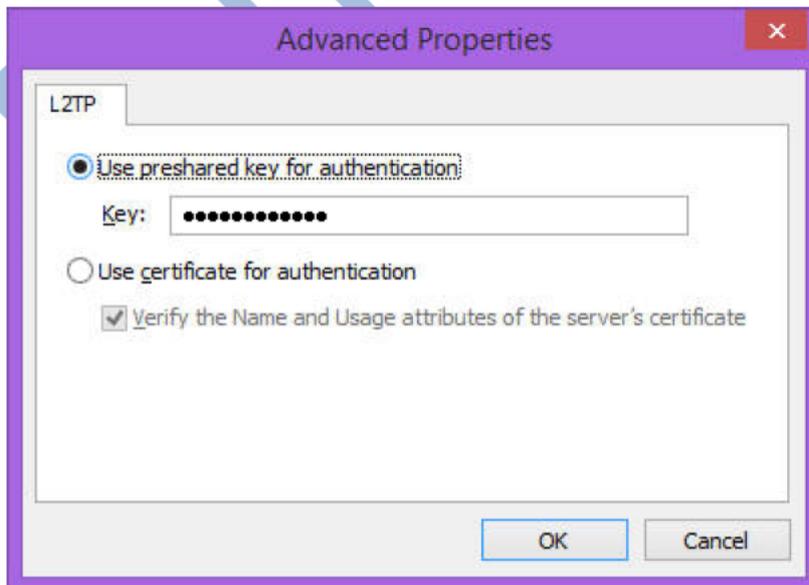


7. Security sekmesinde aynen kurduğumuz gibi Layer2 Tunneling Protocol Over IPsec'i seçiyoruz.

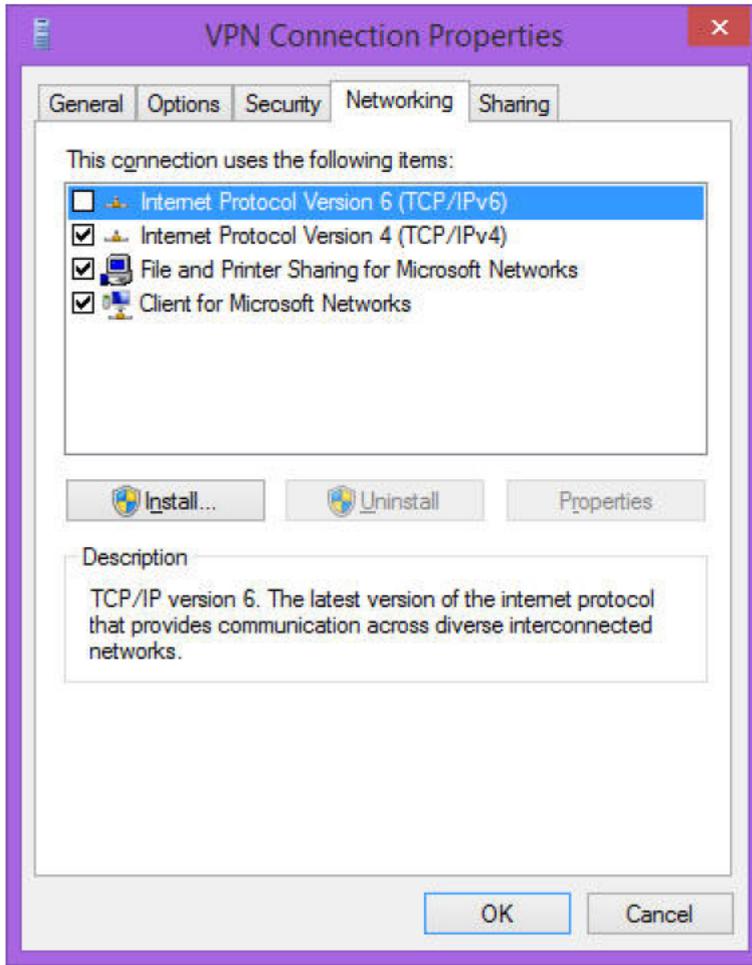
Data Encryption kısmında, Maximum strength'i seçiyoruz.



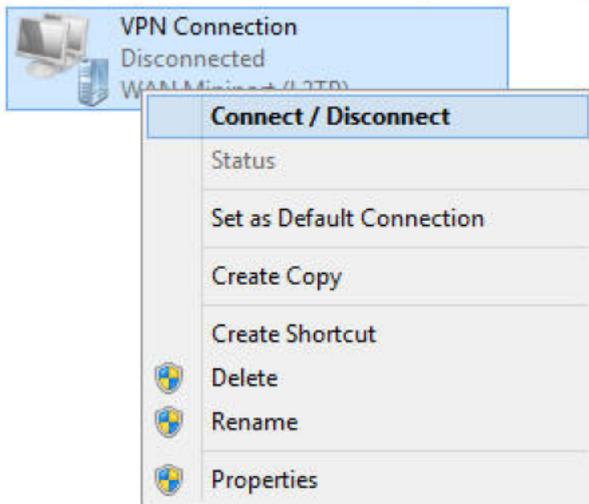
8. Advanced tabına tıklayıp, 4. bölümün 9. adımında belirlediğimiz şifreyi giriyoruz :) O zaman not alın demiştim:)



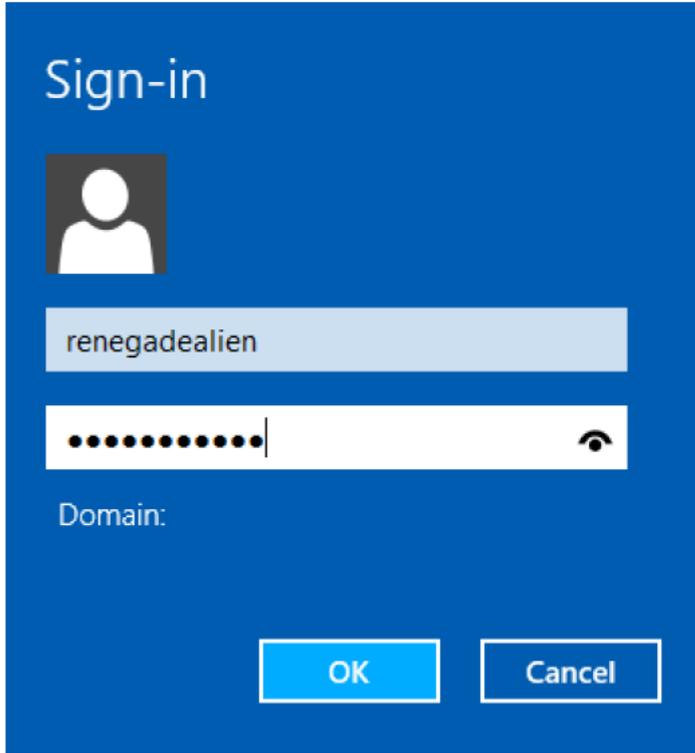
9. Networking sekmesinden IPv6'yı kaldırıyoruz. OK diyerek kapatıyoruz.



10. VPN Bağlantımıza sağ tuş tıklayarak Connect diyoruz.



11. 4. bölümün 12. adımında belirlediğimiz Kullanıcı adı ve şifremizi giriyoruz.



12. Sonunda bitti :) <http://ip.proxy.lc/> adresinden anonimliğimizi kontrol ediyoruz.

Hollanda'dayız :))

Your IP address: 188.226.210.151

IP Address Location
Country: Netherlands
Latitude: 52.5
Longitude: 5.75
Organization: Digital Ocean

Proxy Tests Results for 188.226.210.151

Proxy Headers Test
 Proxy: not detected

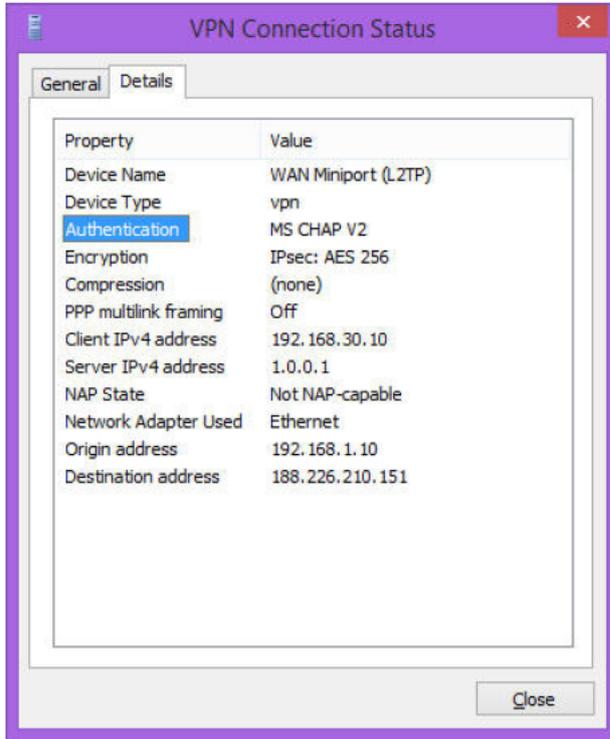
Heuristic proxy tests
 Proxy probability: proxy was not detected by heuristic tests

OPB Test
 OPB doesn't know anything about IP 188.226.210.151

Your browser headers

HTTP_USER_AGENT: Mozilla/5.0 (Windows NT 6.3; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.154 Safari/537.36
 HTTP_ACCEPT_LANGUAGE: tr-TR,tr;q=0.8,en-US;q=0.6,en;q=0.4
 HTTP_REFERER: http://www.samair.ru/
 HTTP_ACCEPT: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8

13. Network bağlantılarından bağlantı özelliklerine baktığımızda, iç bacak ve dış bacak IP'lerini görebilirsiniz.



7. Android, iPhone ve Diğer Cihazlar Üzerinden VPN'e Bağlanmak

Her cihaz için döküman yazıp, Amerikayı yeniden keşfetmeye gerek yok. https://www.softether.org/4-docs/2-howto/9.L2TPIPsec_Setup_Guide_for_SoftEther_VPN_Server adresini kullanarak tüm clientlar için, bağlantının nasıl yapılacağını kontrol edebilirsiniz.

Yukarıdaki satırları yazarken, aynı sayfada Windows için bağlantı örneği olduğunda üzülerek görmüş bulunmaktayım :)

Tahribat.Com

8. Linux Üzerinden VPN'e Bağlanmak

Linux işletim sistemlerinde, L2TP default olarak gelmiyor. İnternette L2TP on <linux dağıtımınız > şeklinde aratarsanız, uygun sonuca ulaşacaksınız.

Ubuntu için yaptığım araştırmada, bu link geldi Bknz : <http://bailey.st/blog/2011/07/14/connecting-to-a-l2tpipsec-vpn-from-ubuntu-desktop/>

Tahribat.Com

9. Sonuç

Yukarıdaki adımları sırayla tamamlayarak, yurtdışı kaynaklı, güvenli ve size özel VPN servisinizi kurabilir, arkadaşlarınız ile paylaşabilirsiniz. Paylaşım yapacağınız tüm arkadaşlarınıza açacağınız kullanıcı adı ve şifre sayesinde, bandwidth kullanımı gibi verileri kontrol edebilirsiniz.

VPN bağlantısı sırasında compression seçeneğini aktif ederek kotanızı bir miktar düşürebilirsiniz. (Bu noktada OnTheFly Gzip Compression yapıldığı için, sunucunun kaynak kullanımının artacağını ve az bir miktar gecikme/delay yaşanabileceğini gözönüne alınız.

VPN kurarak para kazanmanız durumunda, payımı isterim :)

Bu döküman Tahribat.Com müritleri için, özel olarak yazılmıştır, istekleriniz için Tahribat.Com üzerinden iletişime geçebilirsiniz.

renegadealien @ 28.03.2014