Tahribat.Com @ renegadealien

Yeni Başlayanlar İçin VPN

V 1.0 – 30.03.2014

İçindekiler

Güncellemeler

Versiyon – Tarih	Sayfalar	Açıklamalar
V 0.9 – 28.09.2014	• -	İlk Versiyon
V 1.0 – 30.09.2014	• 1,2,3 • - • 52 • 4	• 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 zıkkım olsun.

8. Döküman Tahribat.Com için yazılmıştır. Kaynak belirtmeden paylaşmayın, bozuşuruz.

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 yeralan verilerin kaydedilmesi,

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

Ayrıntılı bilgi için bknz : 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 olarakda, 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 taktirde, 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

YUUUUUUUUUUUUHHHHH!

Hatta bununla kalmadılar, Yandex DNS'den engellendi !

YUUUUUUUUUUUUHHHHH!

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 diyorlar! 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 taktirde tüm iletişimimiz kaydedilecek!

   Eşimle, dostumla, arkadaşımla 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 karşıdakinin 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. Internete çıkartacağız.

Gereksinimler

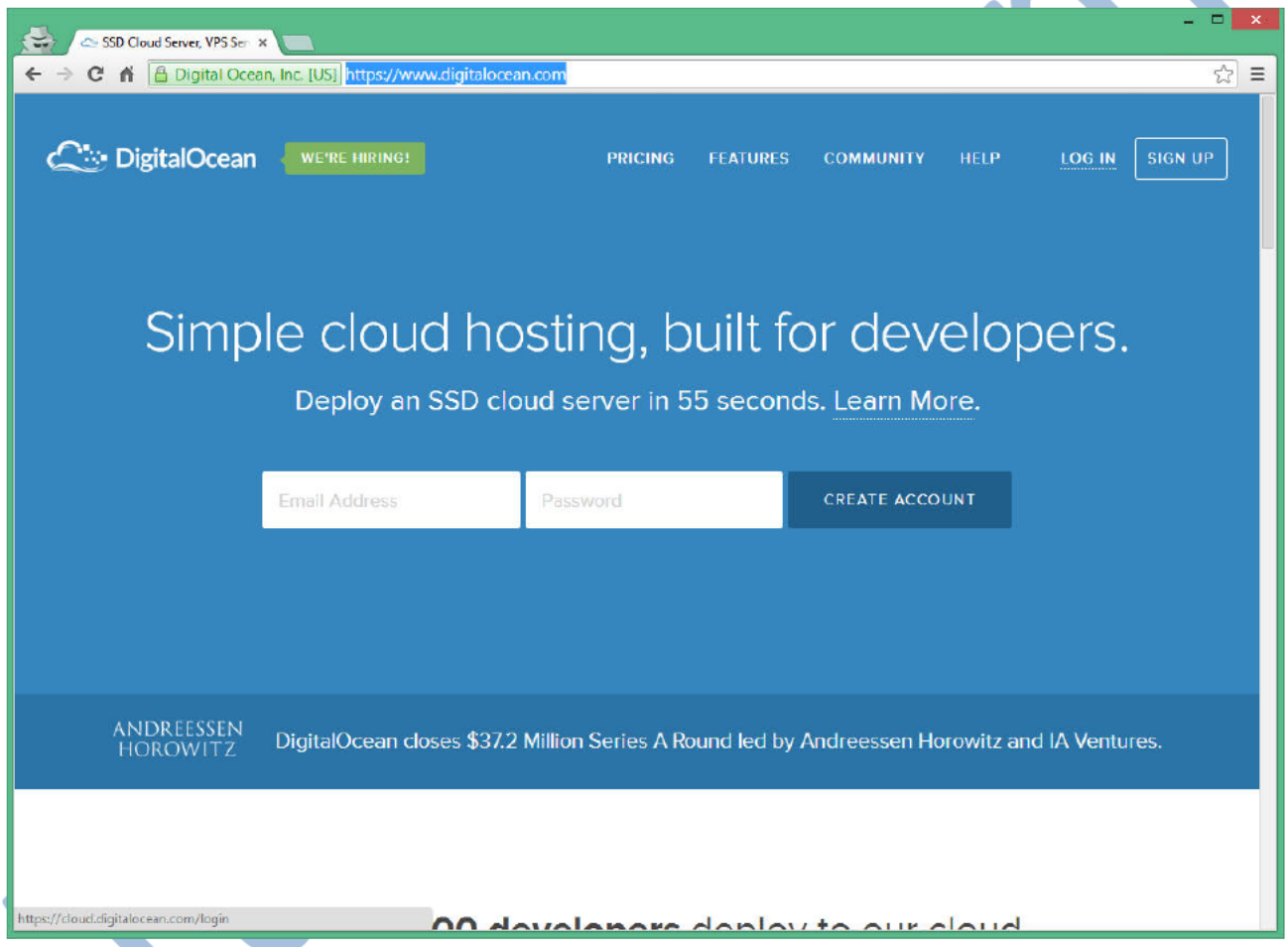
1. 1 adet yurt dışı lokasyonlu sunucu. Fiyatın ucuz olması oldukça avantaj. Aynı zamanda Türkiye'ye yakın olursa, bağlantımız daha hızlı olacaktır. Bu iş için ben www.digitalocean.com dan bir adet amsterdam lokasyonlu minimum konfigurasyonlu sunucu kullanacağım.
2. Sunucunun maliyeti aylık 5$. Eğer sizin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

Başlıyoruz

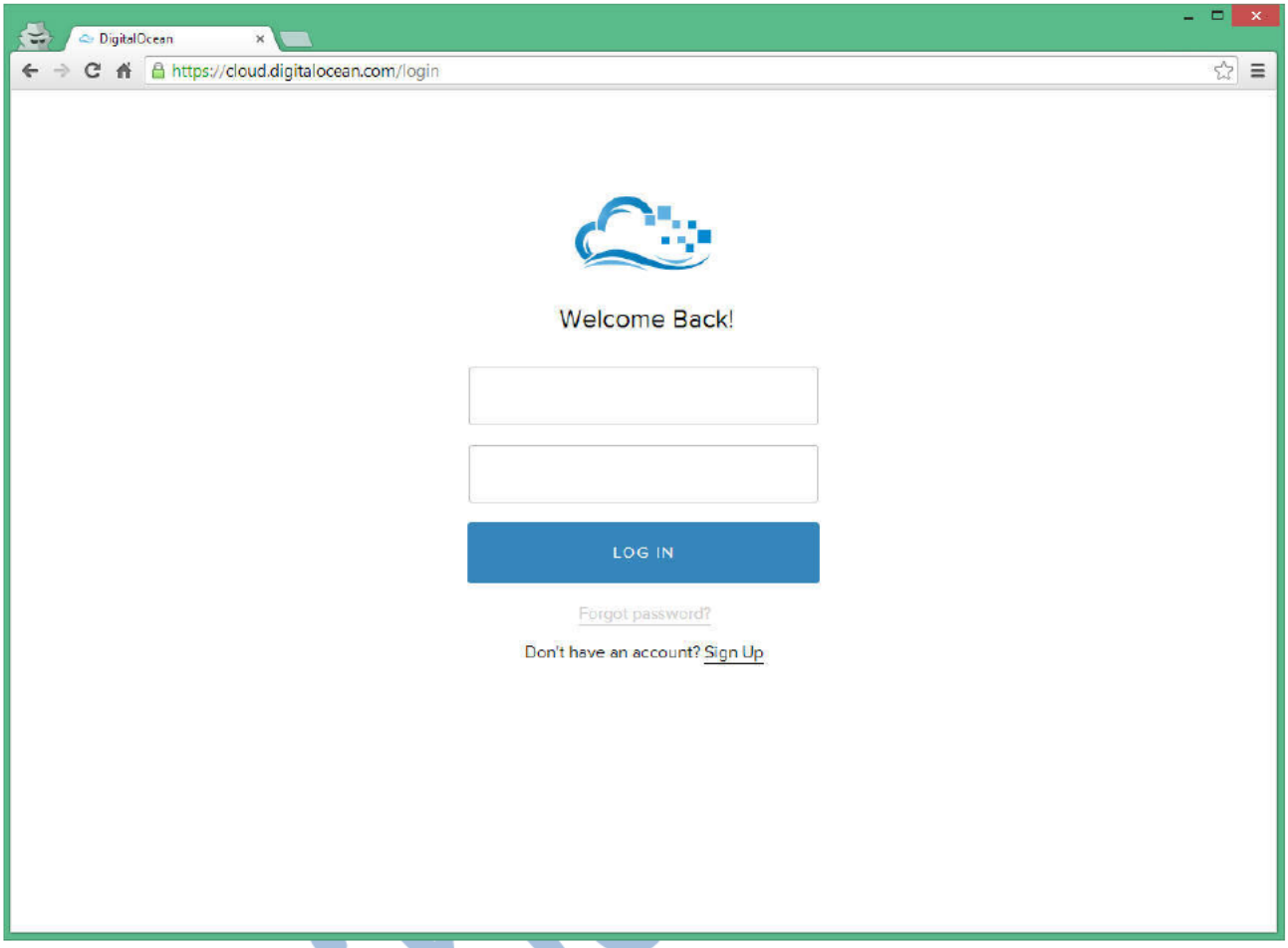
1.Digitalocean.Com Hesap Açılması, İlk VPS'in Kurulması

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.

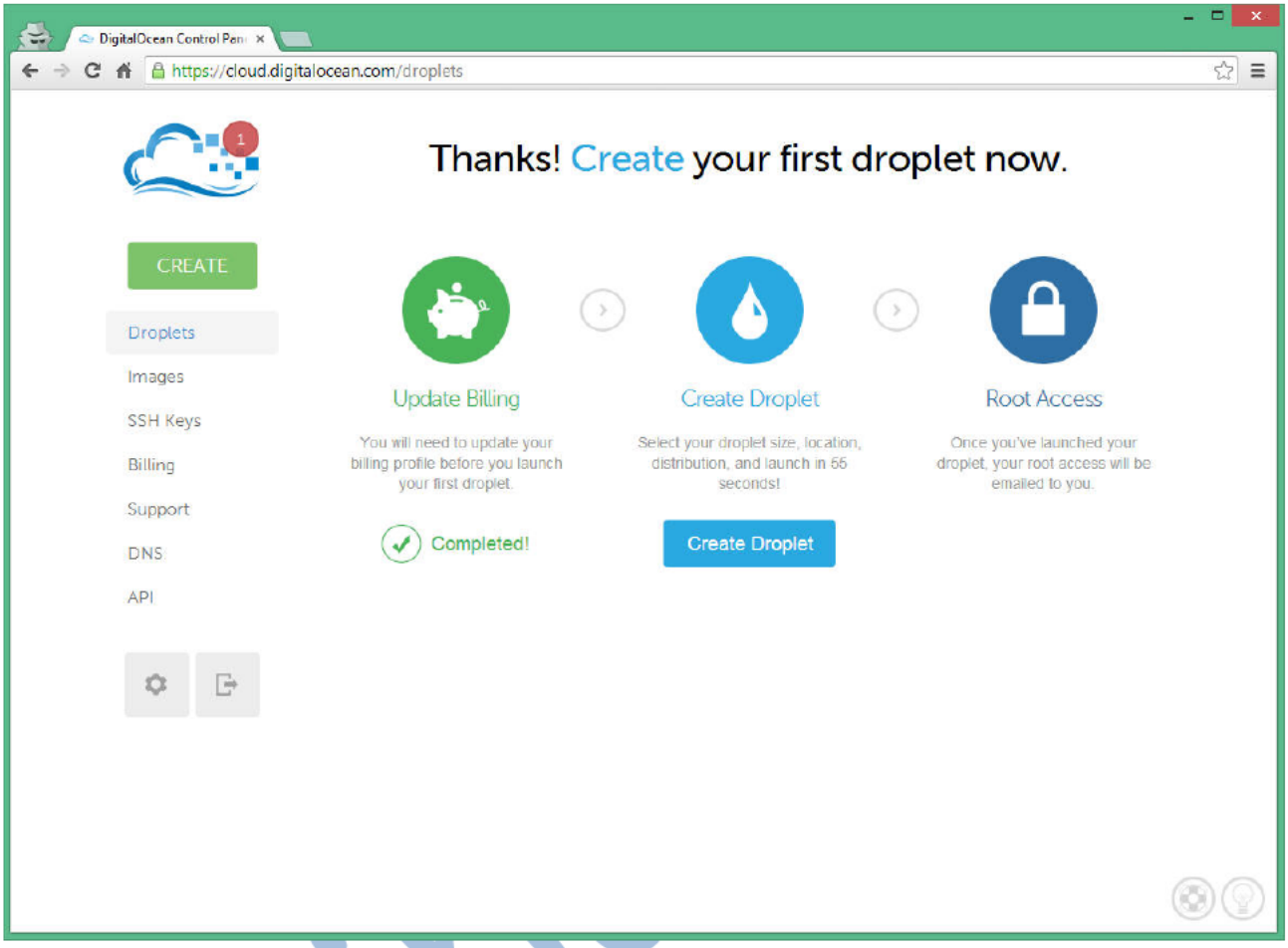


2. Açılan pencere aracılığı ile giriş yapıyoruz.



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

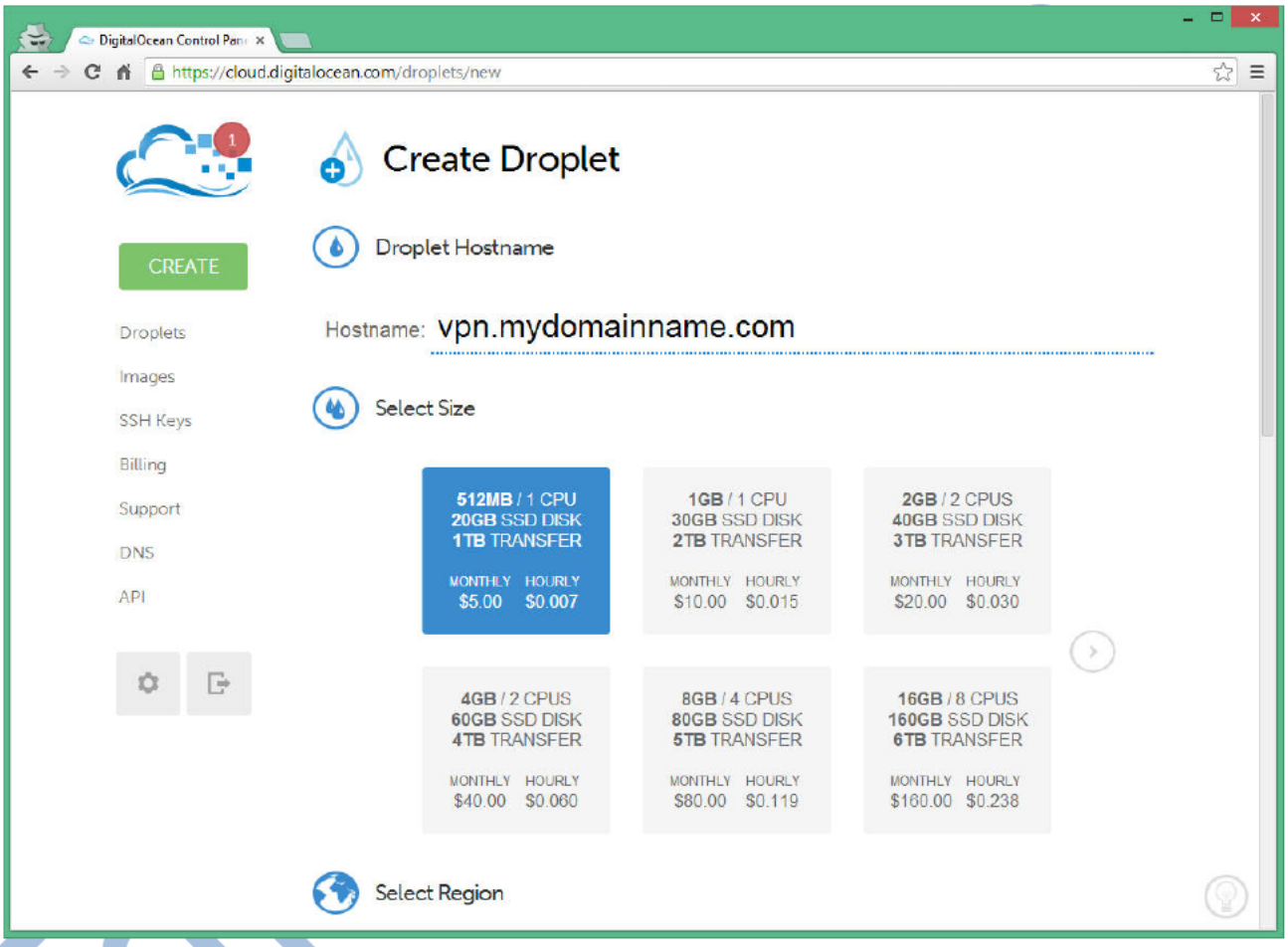
3. Aşağıdaki pencerede Create Droplet sekmesine tıklayın.



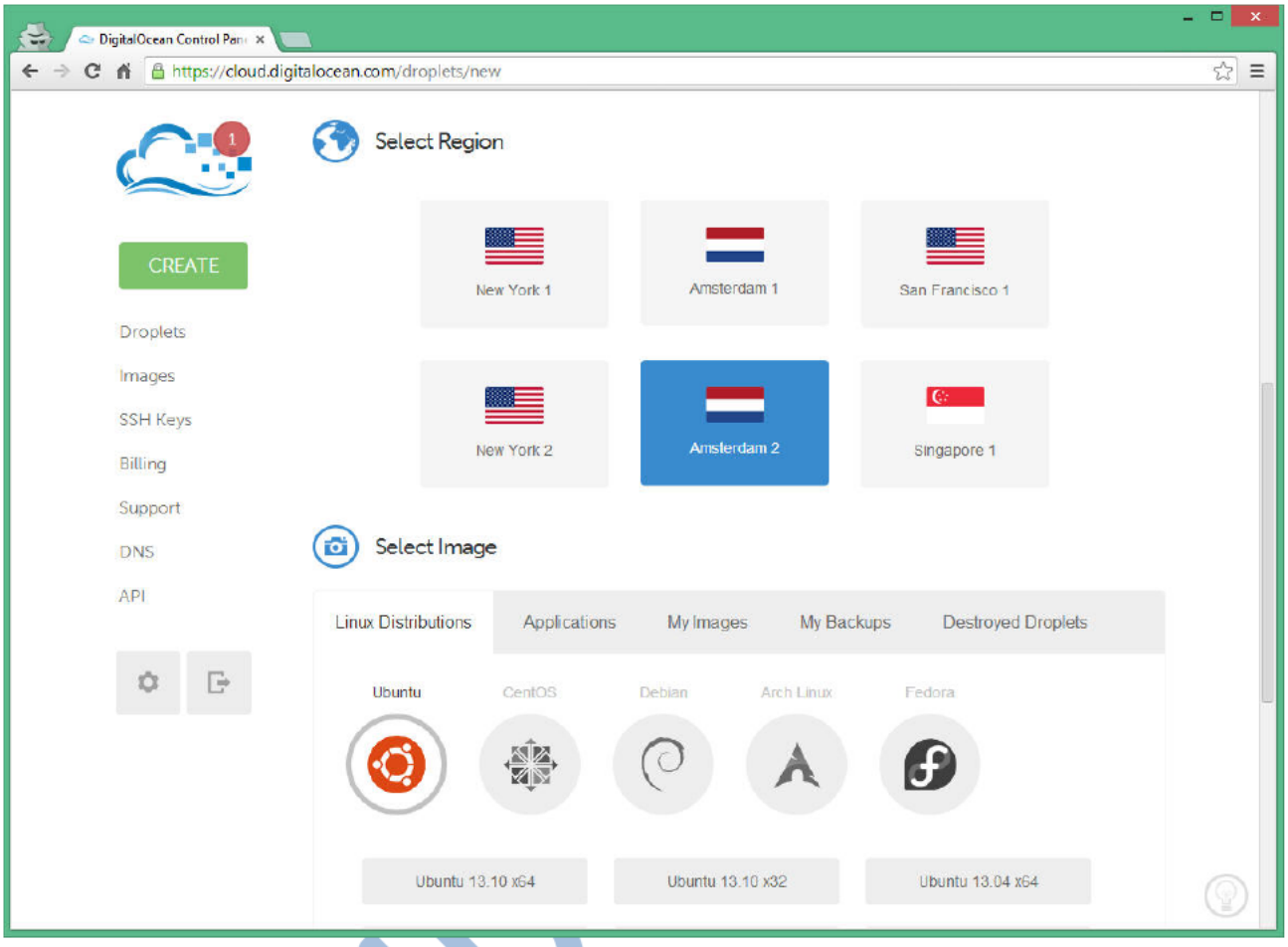
4. Hostname olarak eğer, bir domaininiz var ise, vpn.domainname.com şeklinde yazabilirsiniz. aksi taktirde vpn yazıp geçebilirsiniz. ben vpn.kendidomainim.com yazıyorum, vpn.kendidomainim.com adresini buraya yönlendireceğim.

   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.

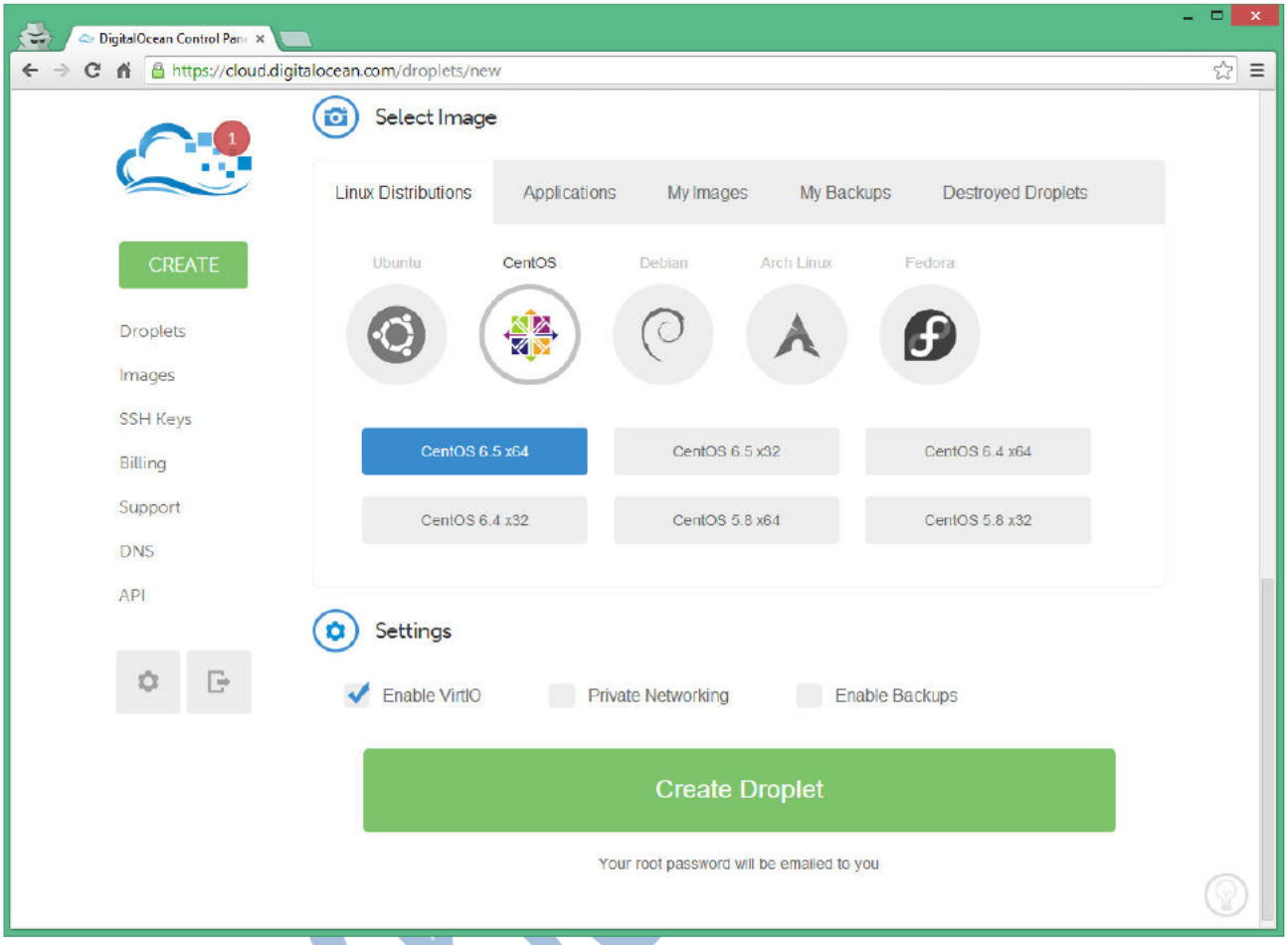
   Şimdilik en düşük versiyonu seçiyorum.



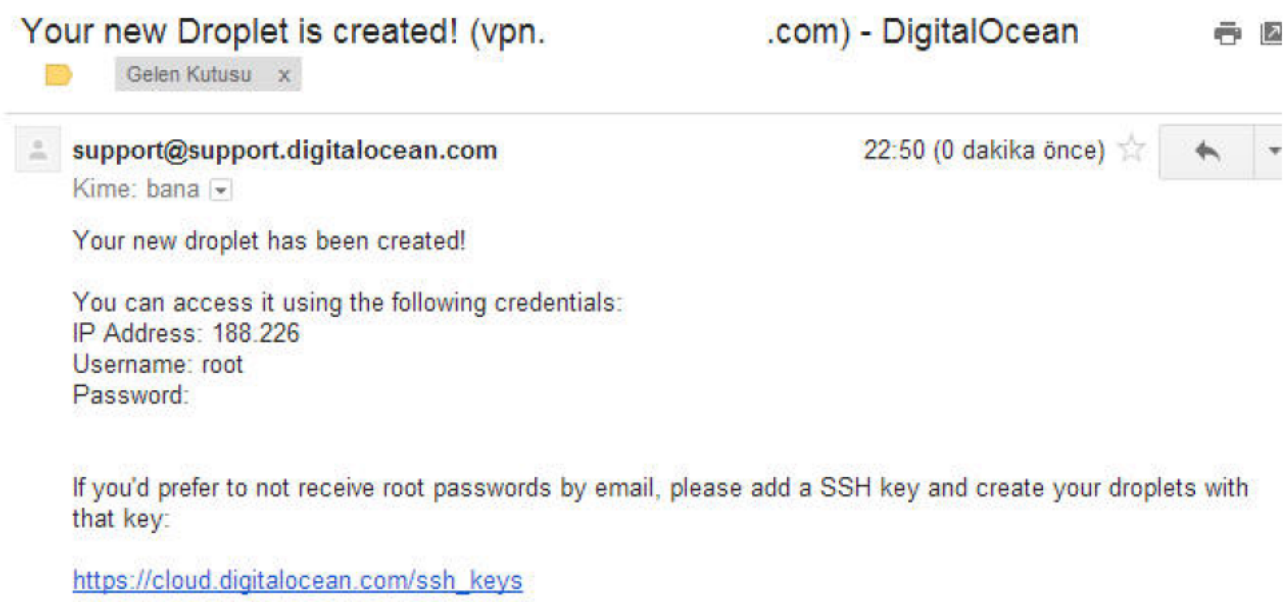
5. Select Region kısmında bölgeyi seçiyorum. Aynı kıtada olmamız Pingimizin düşük olması dolayısı ile bağlantımızın daha hızlı olmasını sağlayacaktır. Ben amstredam 2 lokasyonunu seçiyorum.



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



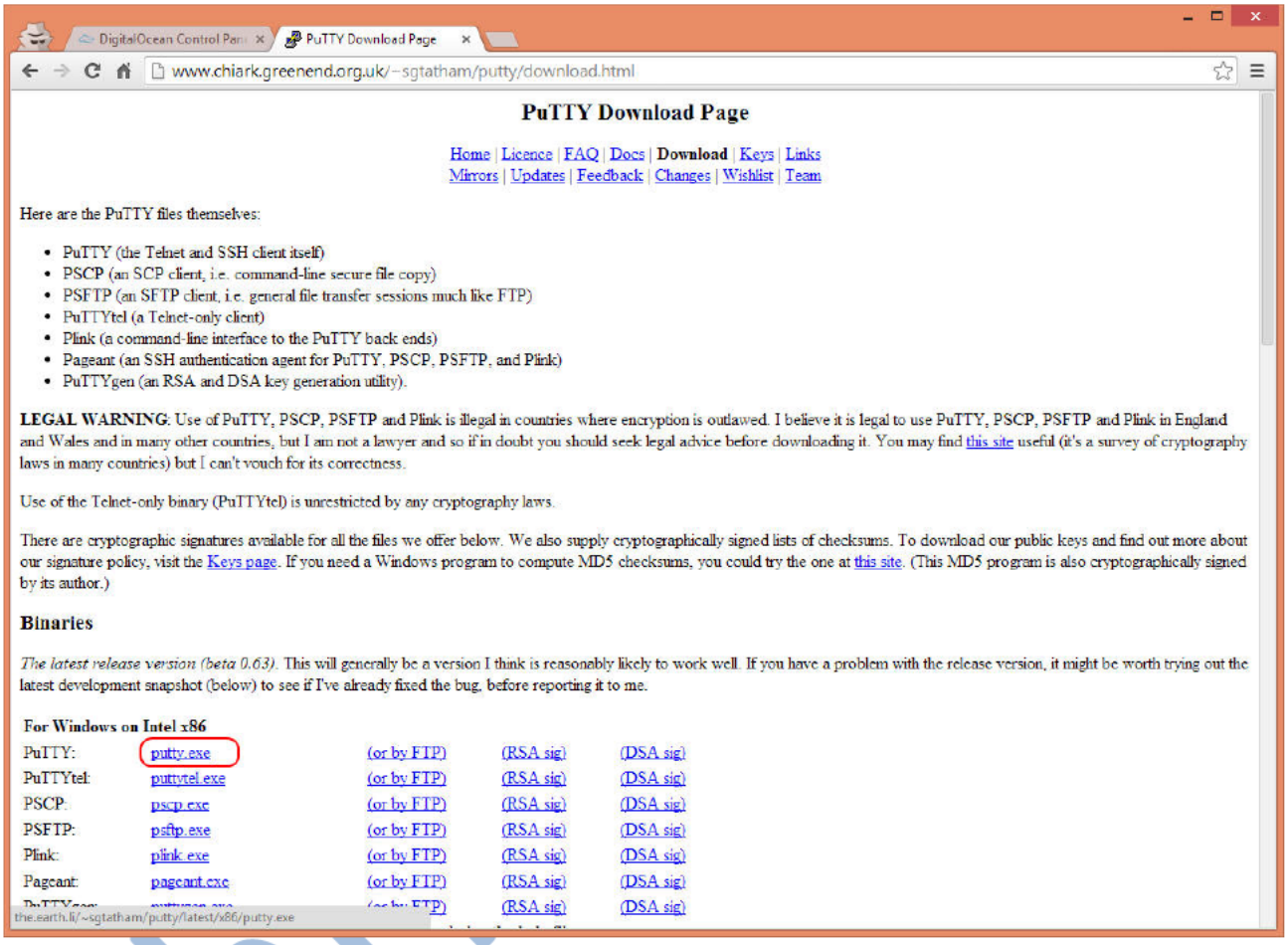
7. Create Droplet'e tıklıyorum. Sunucum hazırlanıyor, yaklaşık 1 dakika içerisinde, sunucu bilgilerinin olduğu aşağıdaki gibi bir mail geldi.



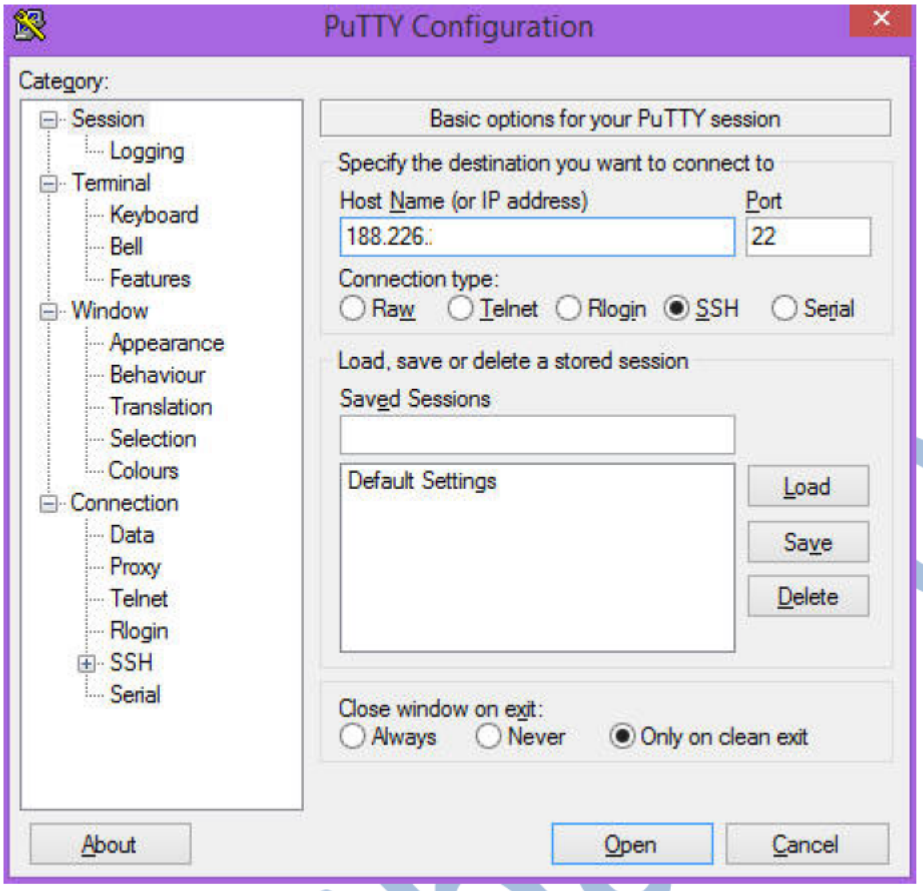
8. Hesap alımı ve sunucu kurulumunun ilk adımı bitti.

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'i indireceğiz.

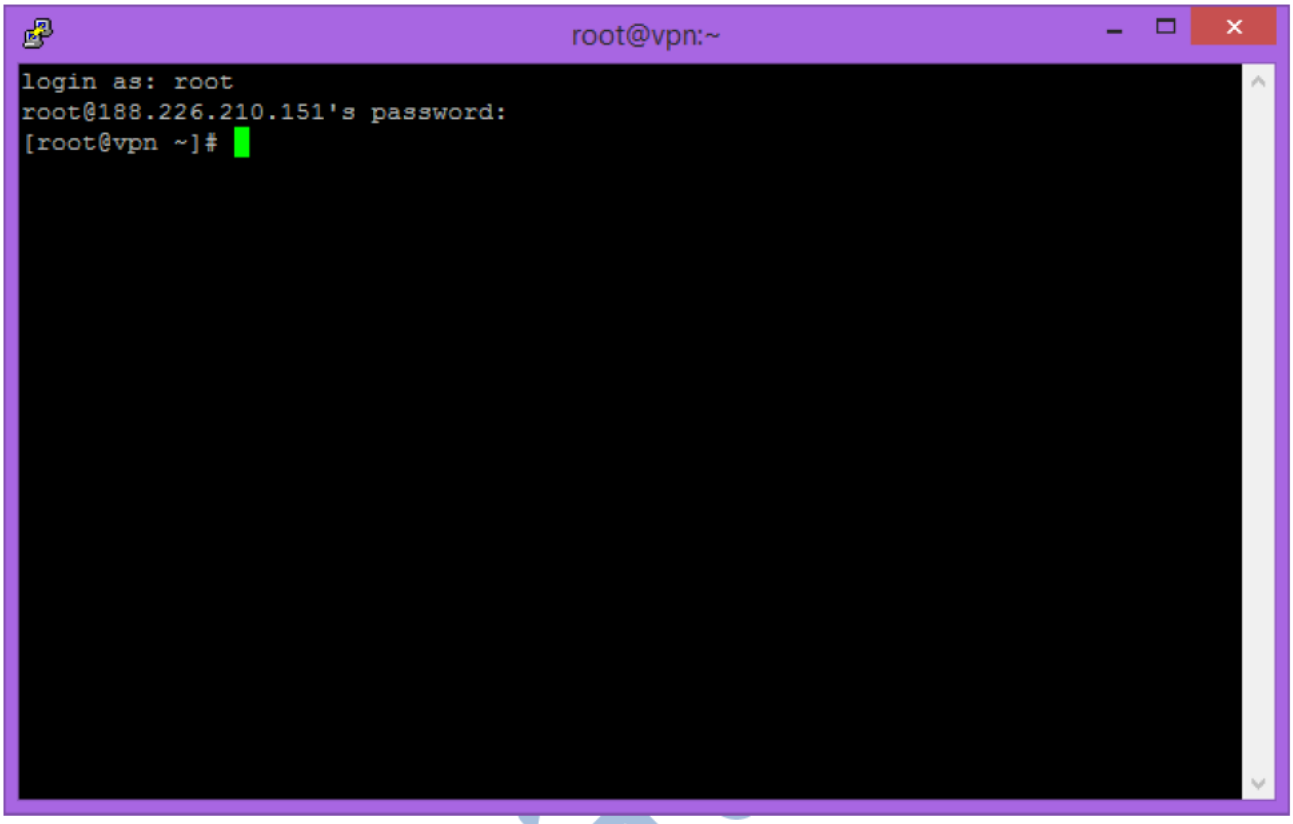


2. Putty indirildikten sonra, Mail'de gelen IP adresini yazarak SSH aracılığı ile 22. porttan sunucuya bağlanıyoruz.



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

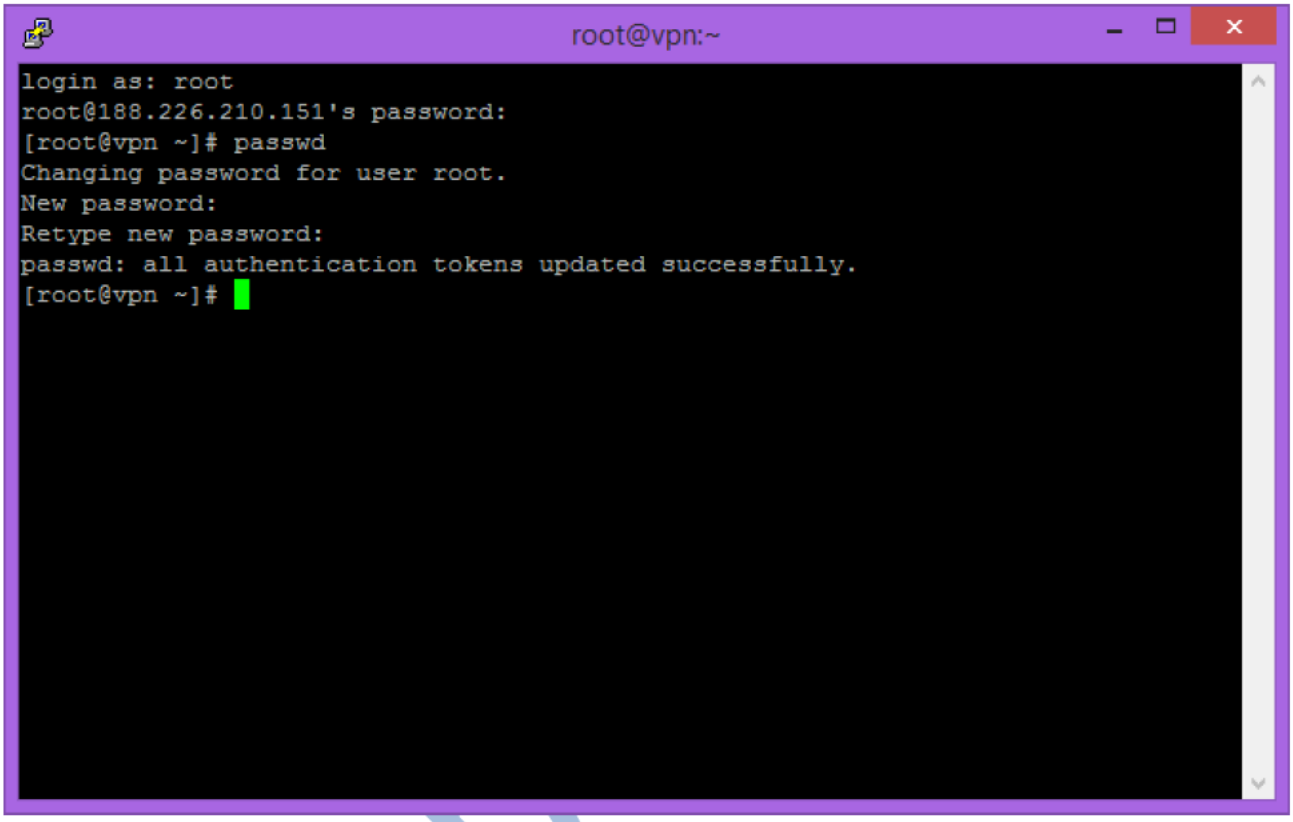
4. Sunucunun konsolu önümüze geldi. Kullanıcı adı olarak root yazıyor şifre olarak mail'de gelen şifreyi yazıyor ve entera basıyoruz.



5. Öncelikle

   passwd

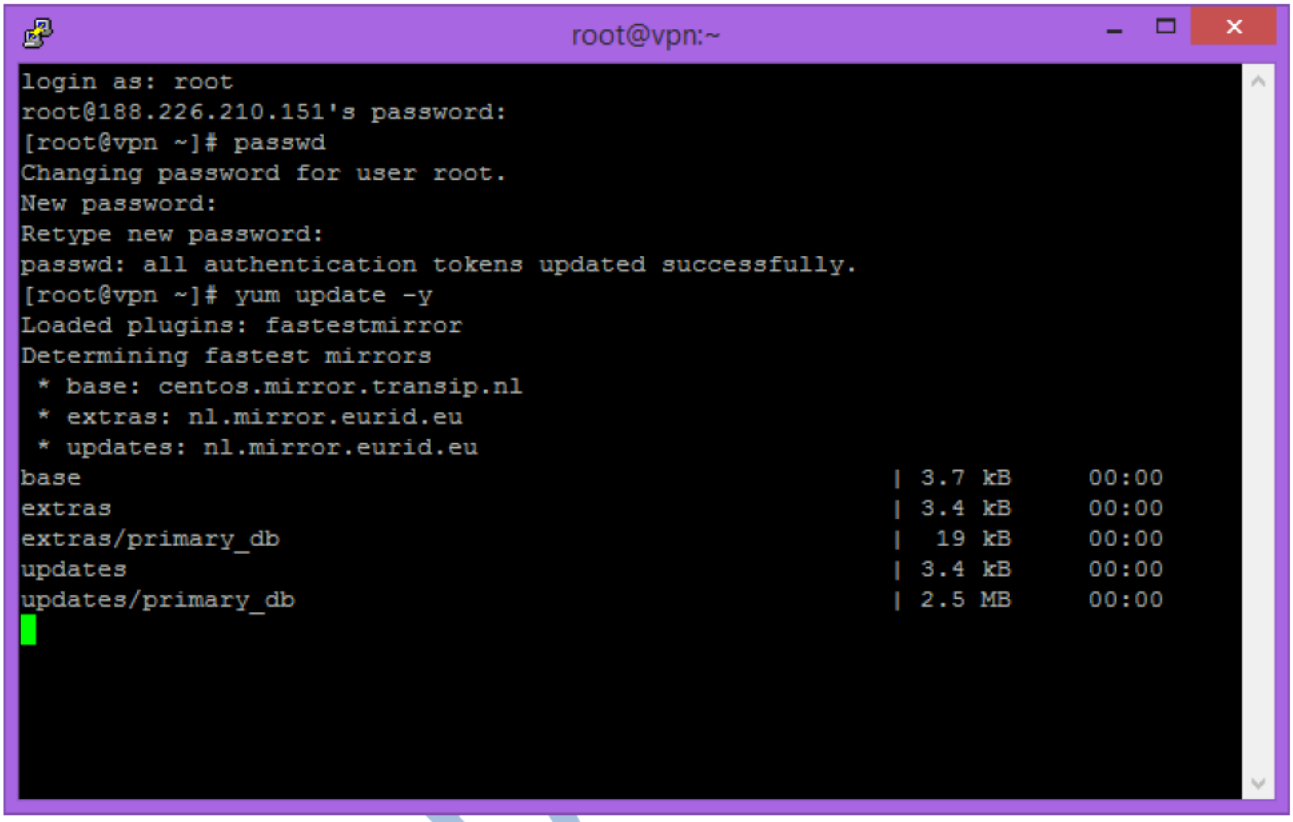
   komutunu kullanarak şifremizi değiştiriyoruz.



6. Sunucu güncellemeleri için

   yum update -y

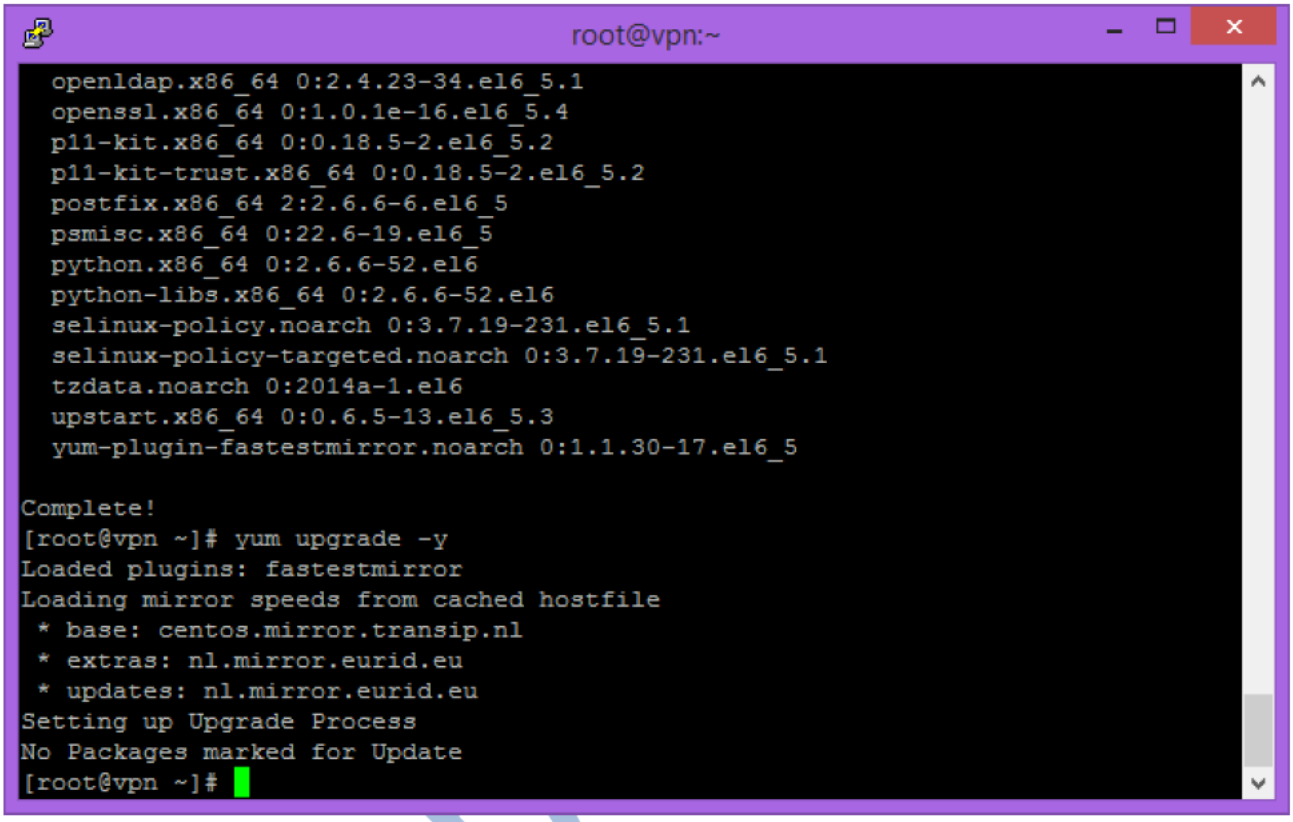
   komutunu kullanıyoruz.



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

   yum upgrade -y

   komutunu kullanıyoruz.



8. Kullanacağımız uygulamaları yüklemek için

   yum install wget ftp gcc make nano -y

   komutunu kullanıyoruz. Komutları kısaca açıklayım.

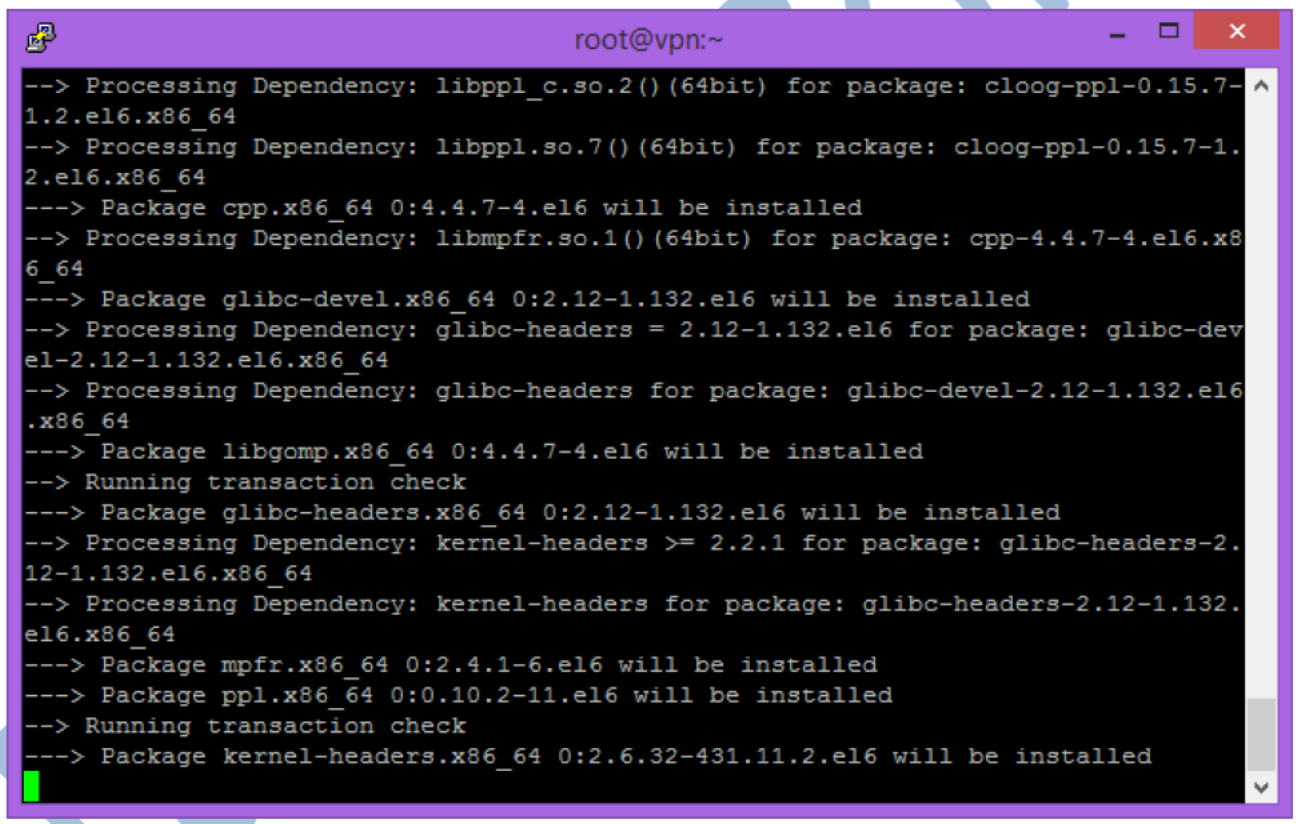
   wget : HTTP protokolü kullanarak dosya indirmek için kullanacağız.

   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 :)



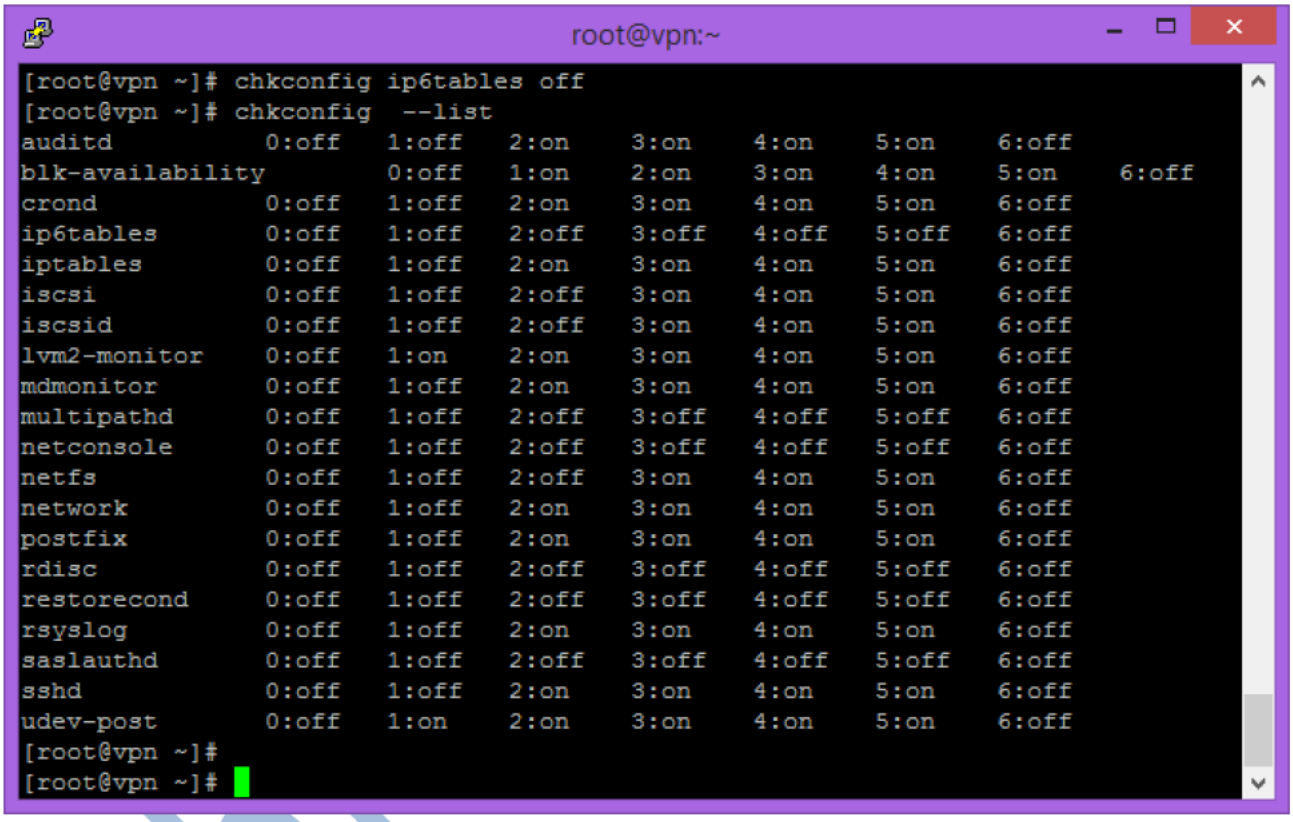
9. Servisleri

   chkconfig --list

   ile kontrol ettim. ip6tables, IPv6 Firewallı, kullanamayacağımız için

   chkconfig ip6tables off

   ile kapattım.

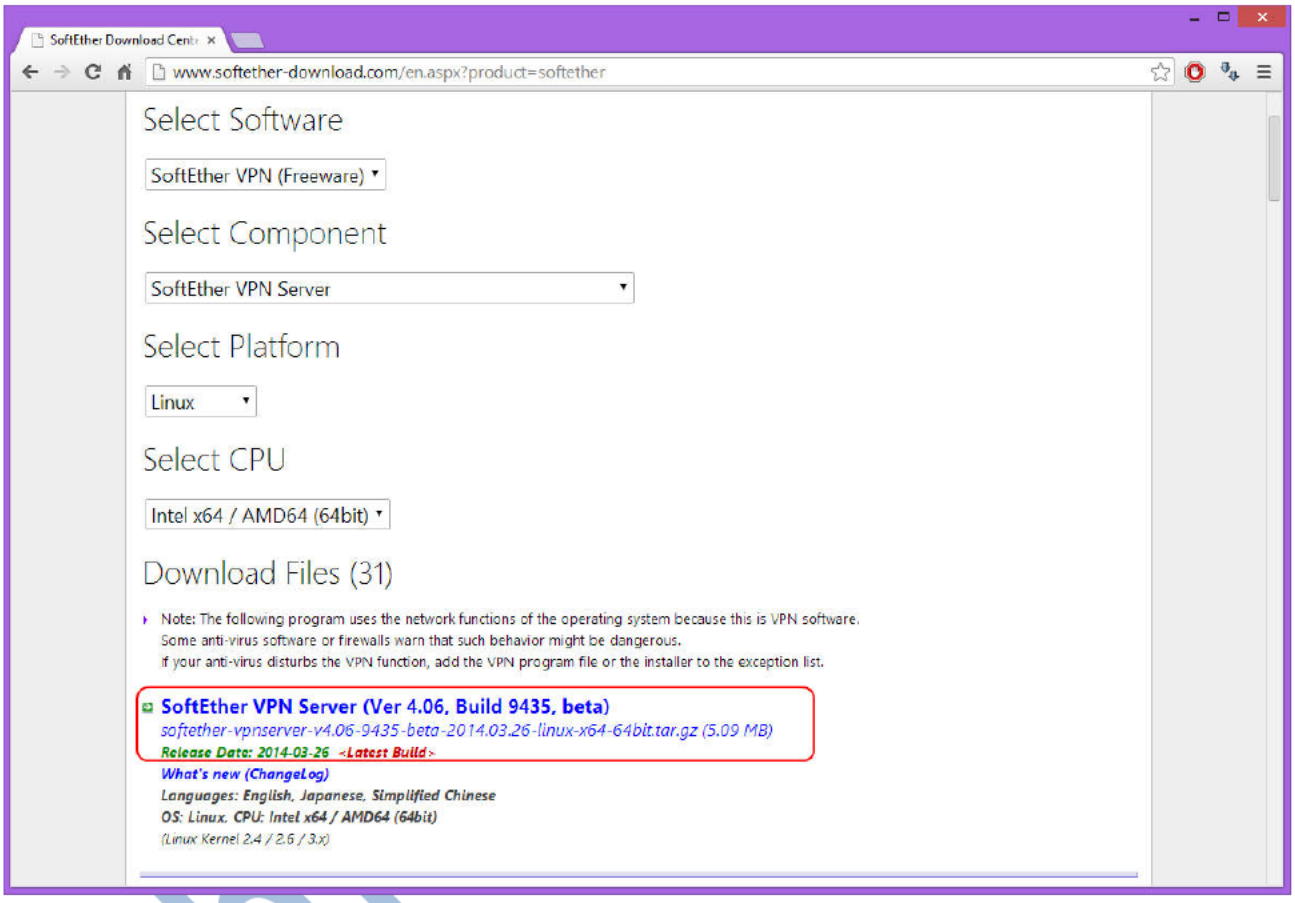


10. Sunucudaki genel kurulumum bitti. Şimdi VPN Serverı bulacağız.

3. SoftEther VPN Serverı Bulmak ve İndirmek

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

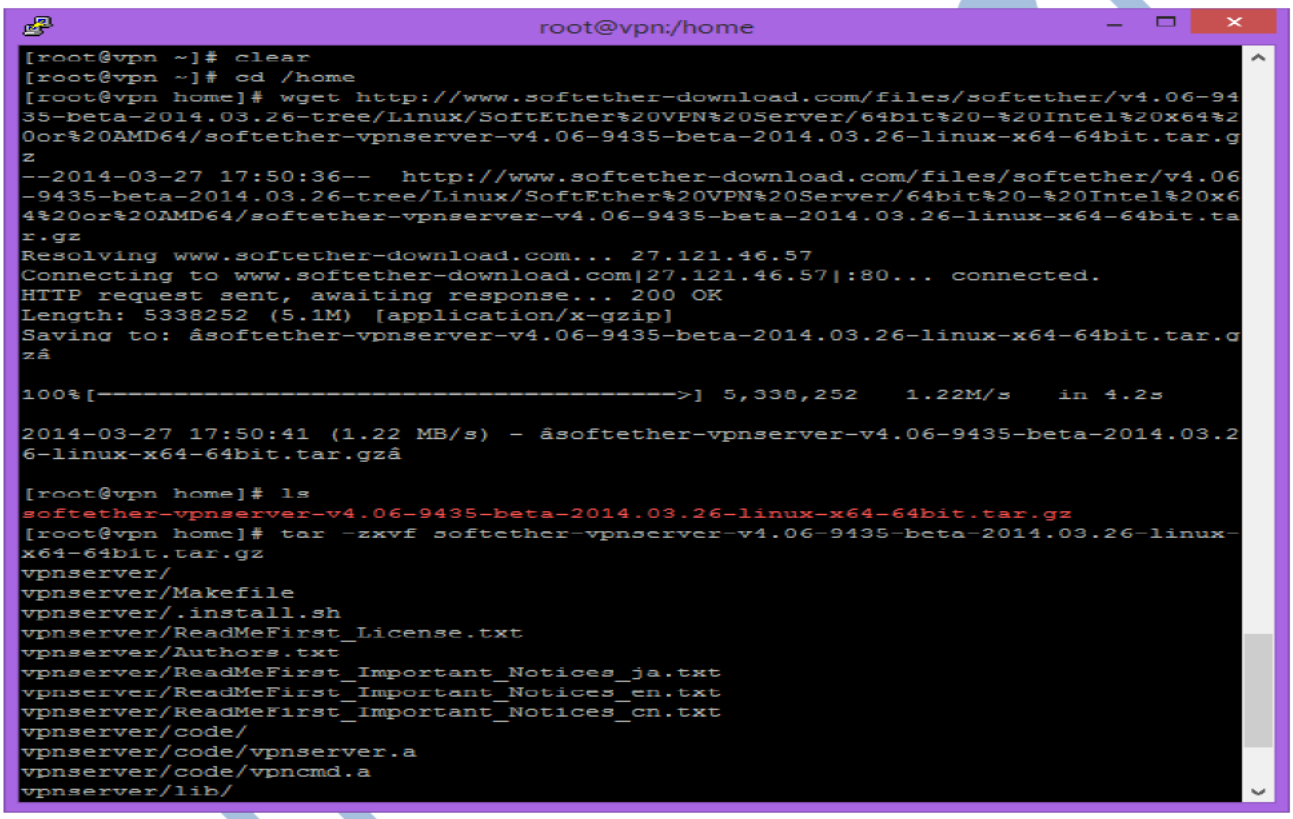
   Aşağıdaki seçenekleri seçerek Linux 64 Bit SoftEther VPN Serverın en son versiyonun linkini buldum ve sağ tuş ile kopyaladım.

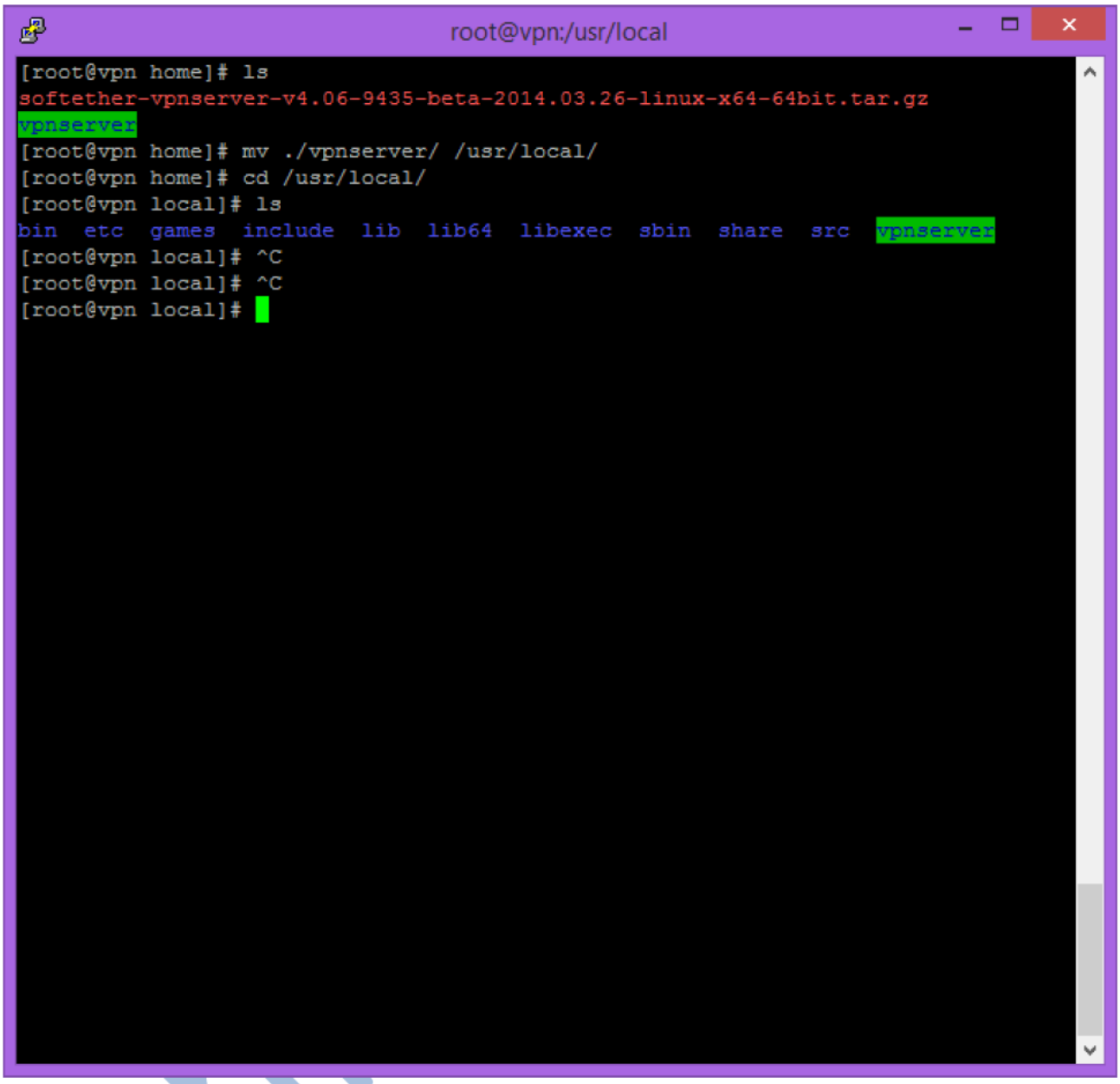


2. Putty aracılığı ile bağlandığım sunucuya geçip aşağıdaki komutları yazdım.

   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



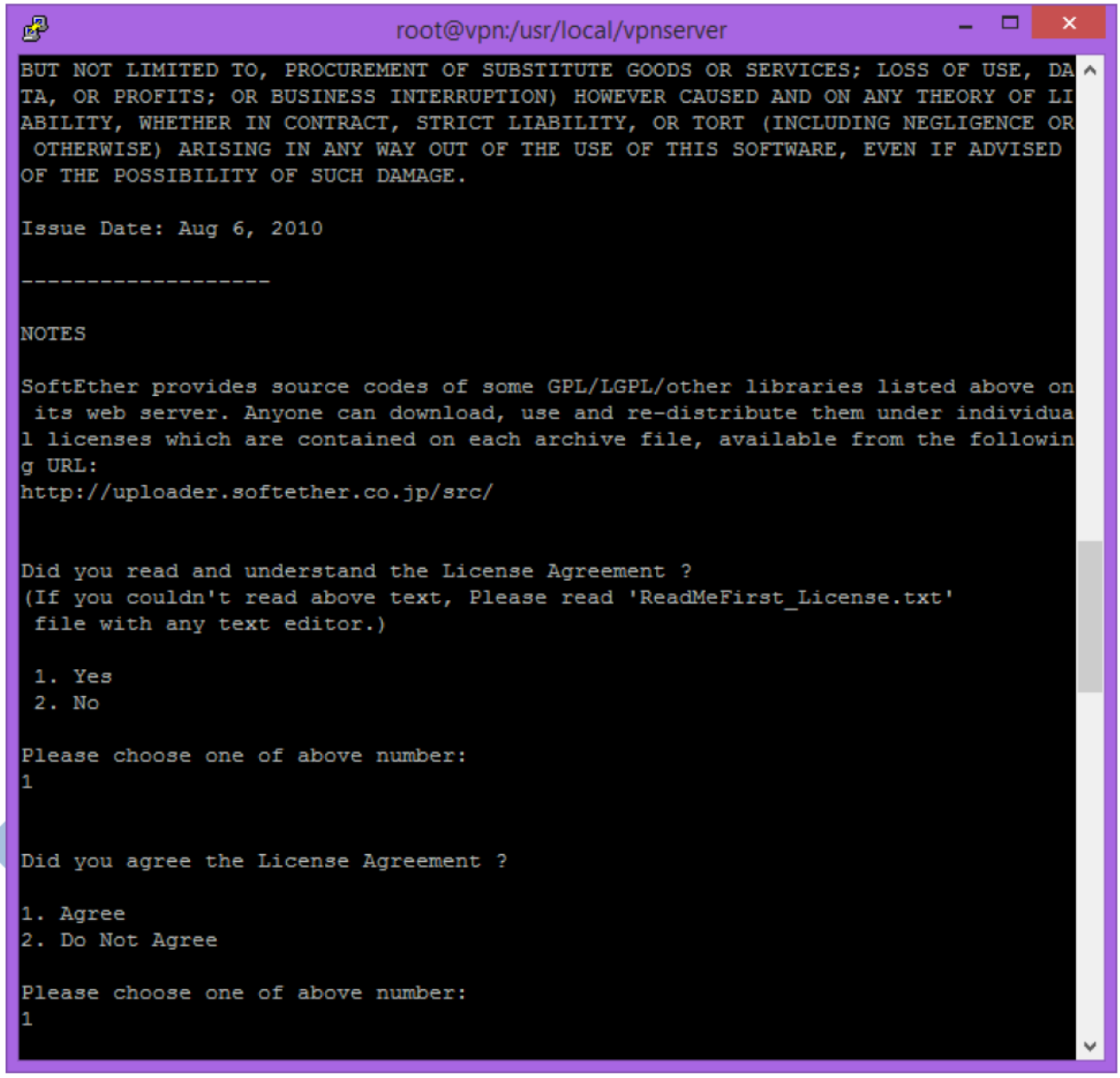

root@vpn:/usr/local
[root@vpn home]# ls
softether-vpnserver-v4.06-9435-beta-2014.03.26-linux-x64-64bit.tar.gz
vpnserver
[root@vpn home]# mv ./vpnserver/ /usr/local/
[root@vpn home]# cd /usr/local/
[root@vpn local]# ls
bin etc games include lib lib64 libexec sbin share src vpnserver
[root@vpn local]#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

3. Şimdi VPN Serverın kurulumuna geçiyoruz.

   Bunun için aşağıdaki komutları kullanacağız.

   cd /usr/local/vpnserver
   make

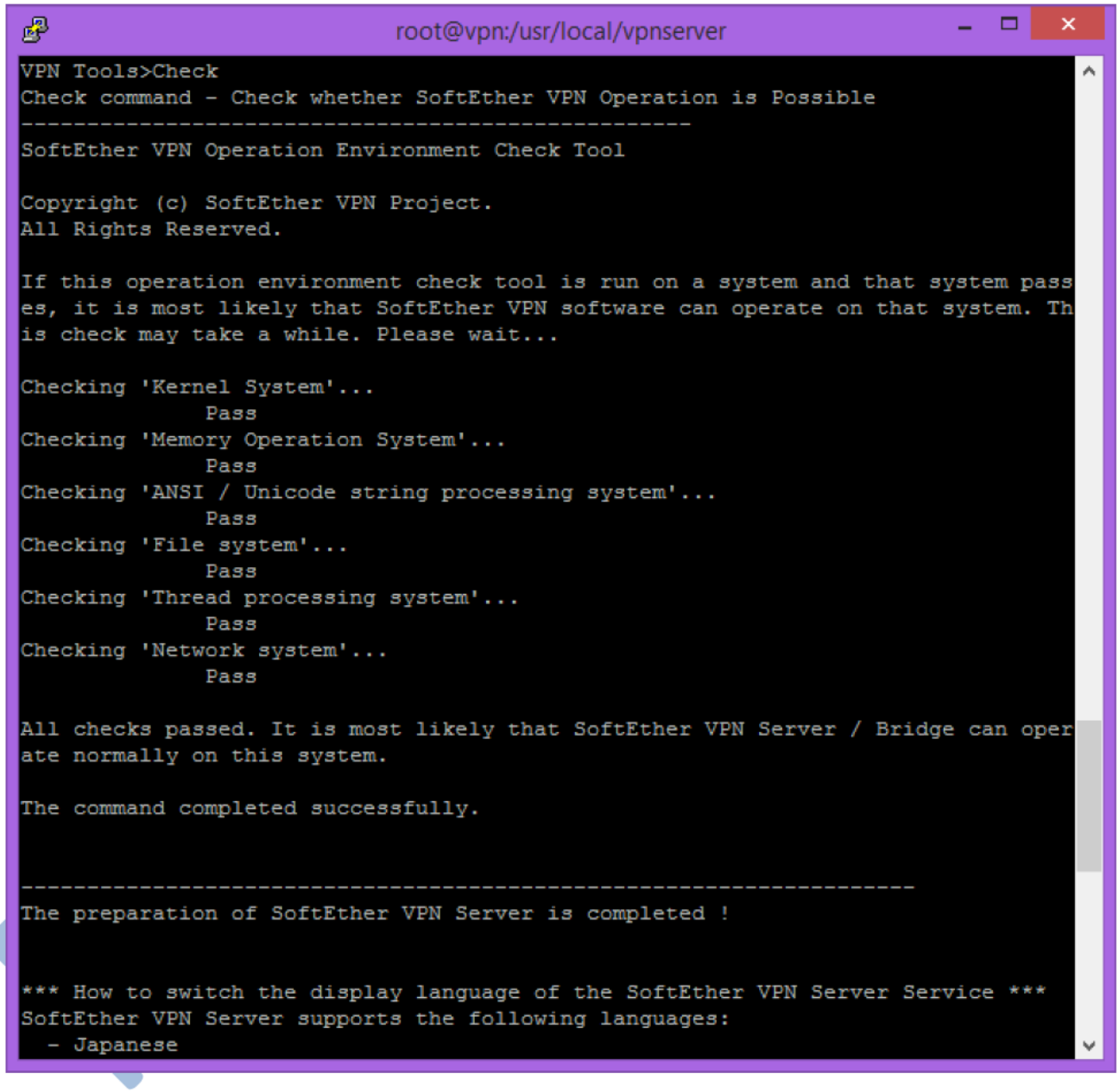
   Daha sonra karşımıza lisans anlaşması geliyor, toplamda 3 kere 1 e basıyoruz.



4. Kurulum sırasında

   VPN Tools > Check

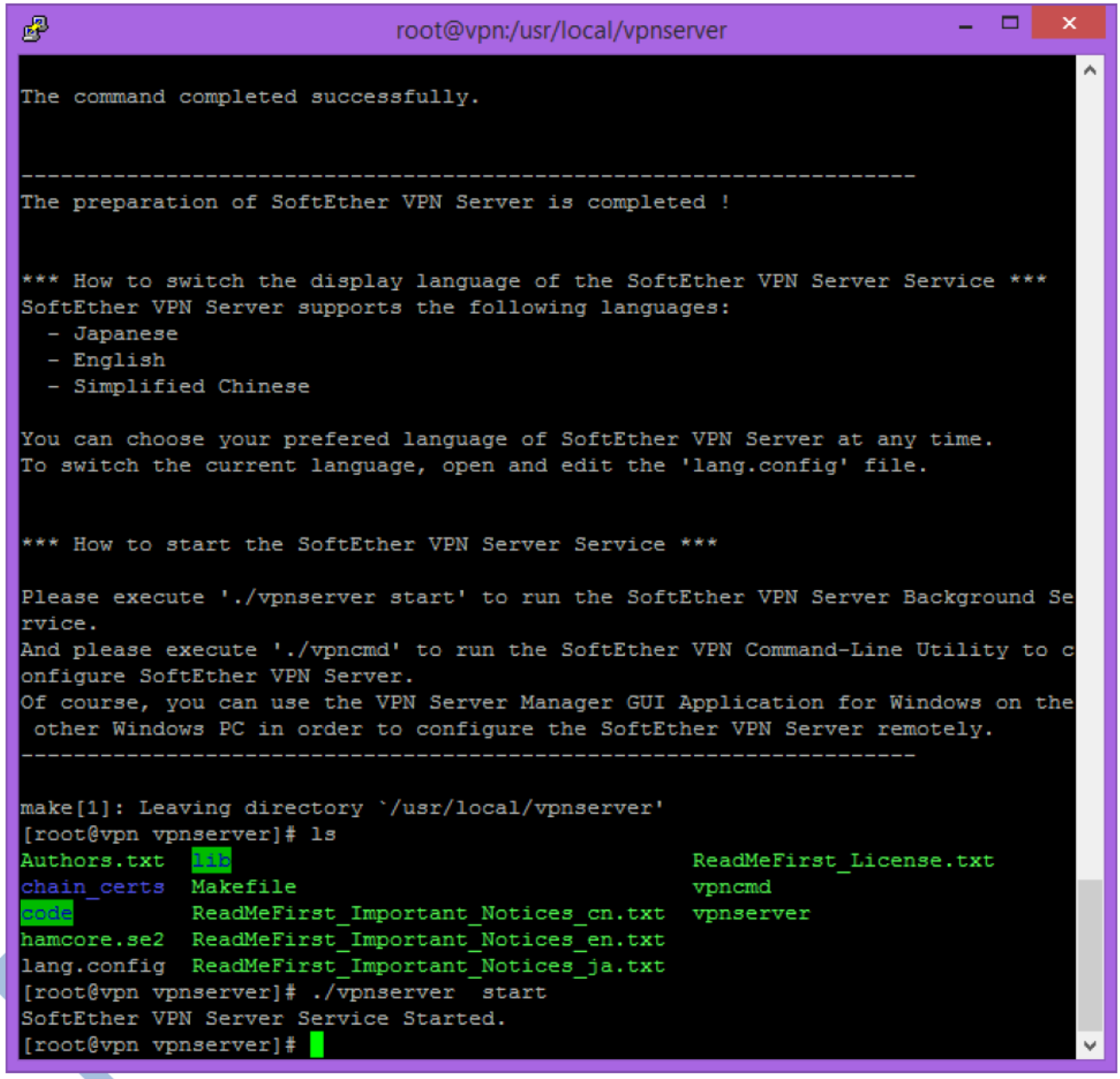
   satırlarını arıyoruz ve altında hepsinin PASS olduğundan emin oluyoruz. Aksi taktirde bir sorun var demektir, ayrıca incelemek lazım.



5. Şu anda sunucumuz kuruldu.

   ./vpnserver start

   komutu ile sunucumuzu başlatıyoruz.

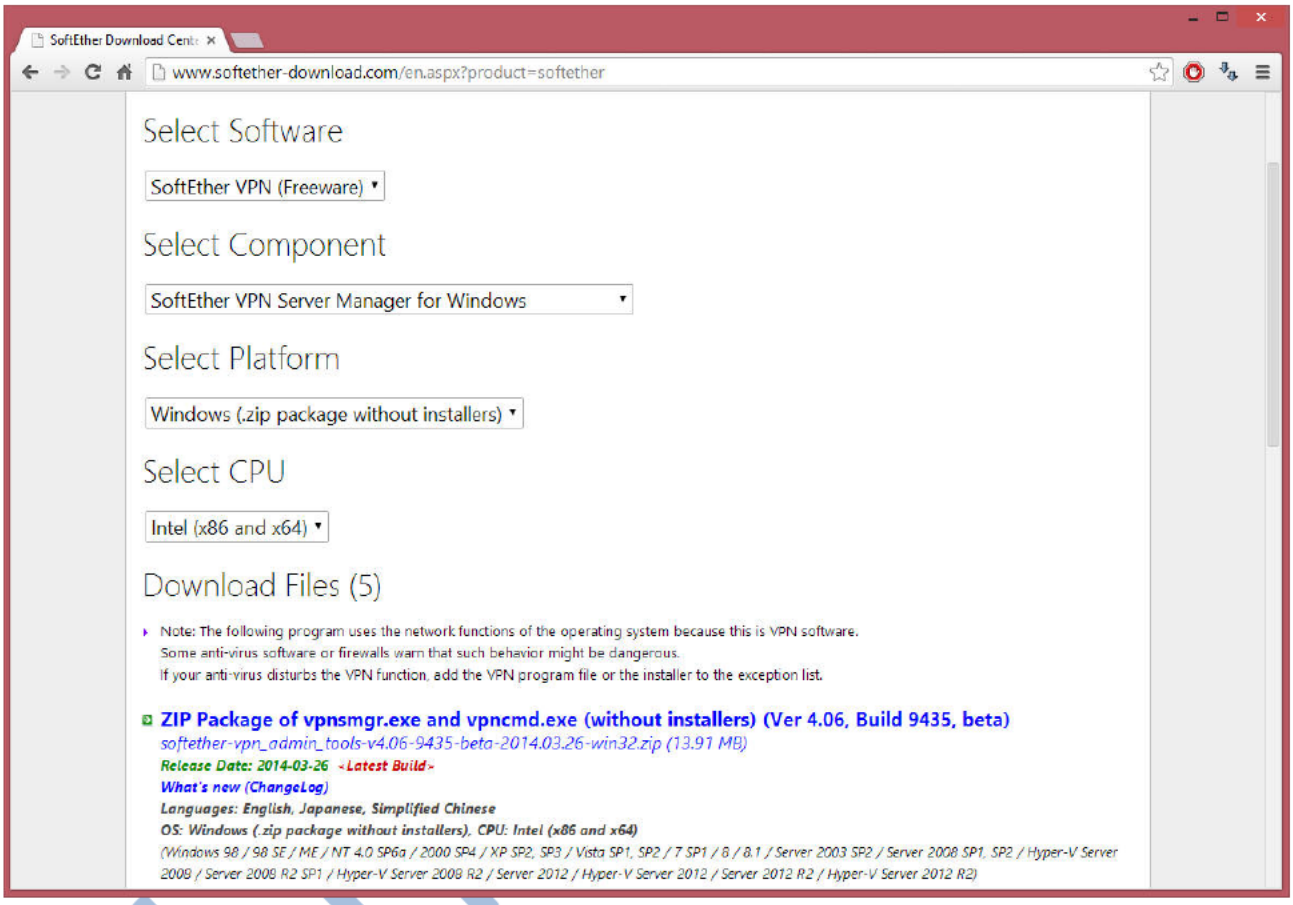


6. Bu andan itibaren sunucu ile işimiz bitti. Windows arayüzlü Management Tool'u kullanarak VPN'imizi konfigure edeceğiz.

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.

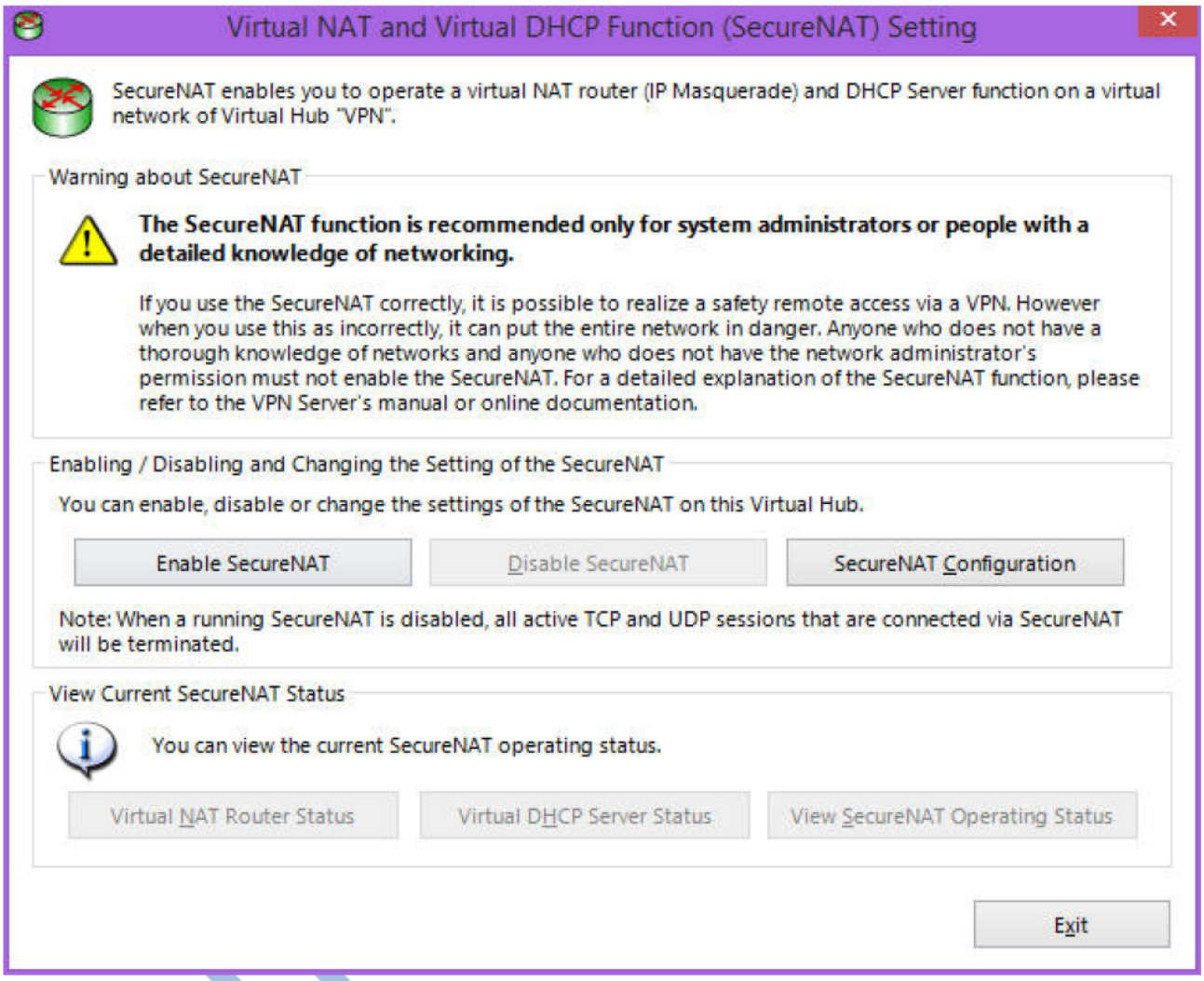
5. SoftEther VPN Management Tool ile SoftEther VPN Sunucusunun Konfigure Edilmesi

1. Uygulamayı çalıştırıyor ve New Settings butonuna tıklıyoruz.

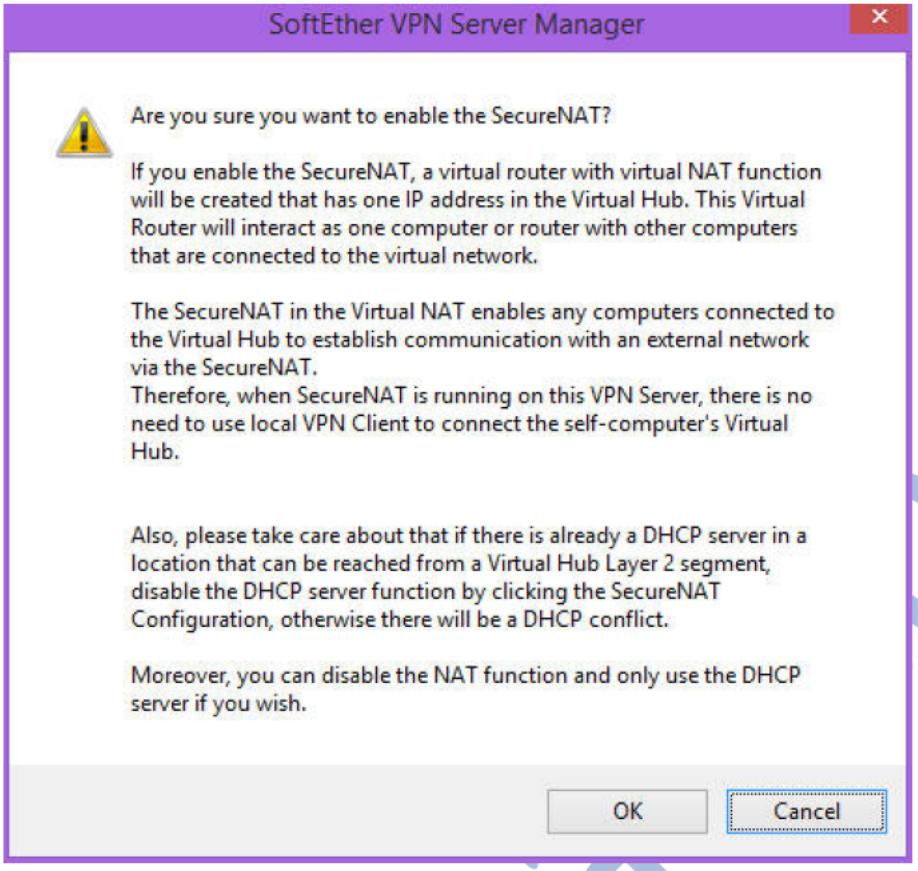
2. Setting Name bölümüne bir isim girin. VPN uygun.

   Host Name kısmına sunucunun IP adresini girin.

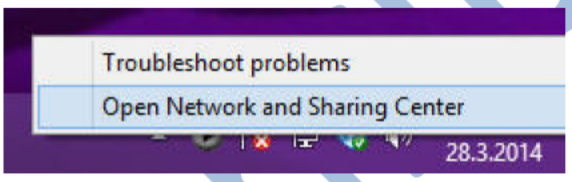
   Şifre kısımını boş bırakın ve OK tuşuna basın.



3. Ana bağlantı penceresinde Connect tuşuna basın.

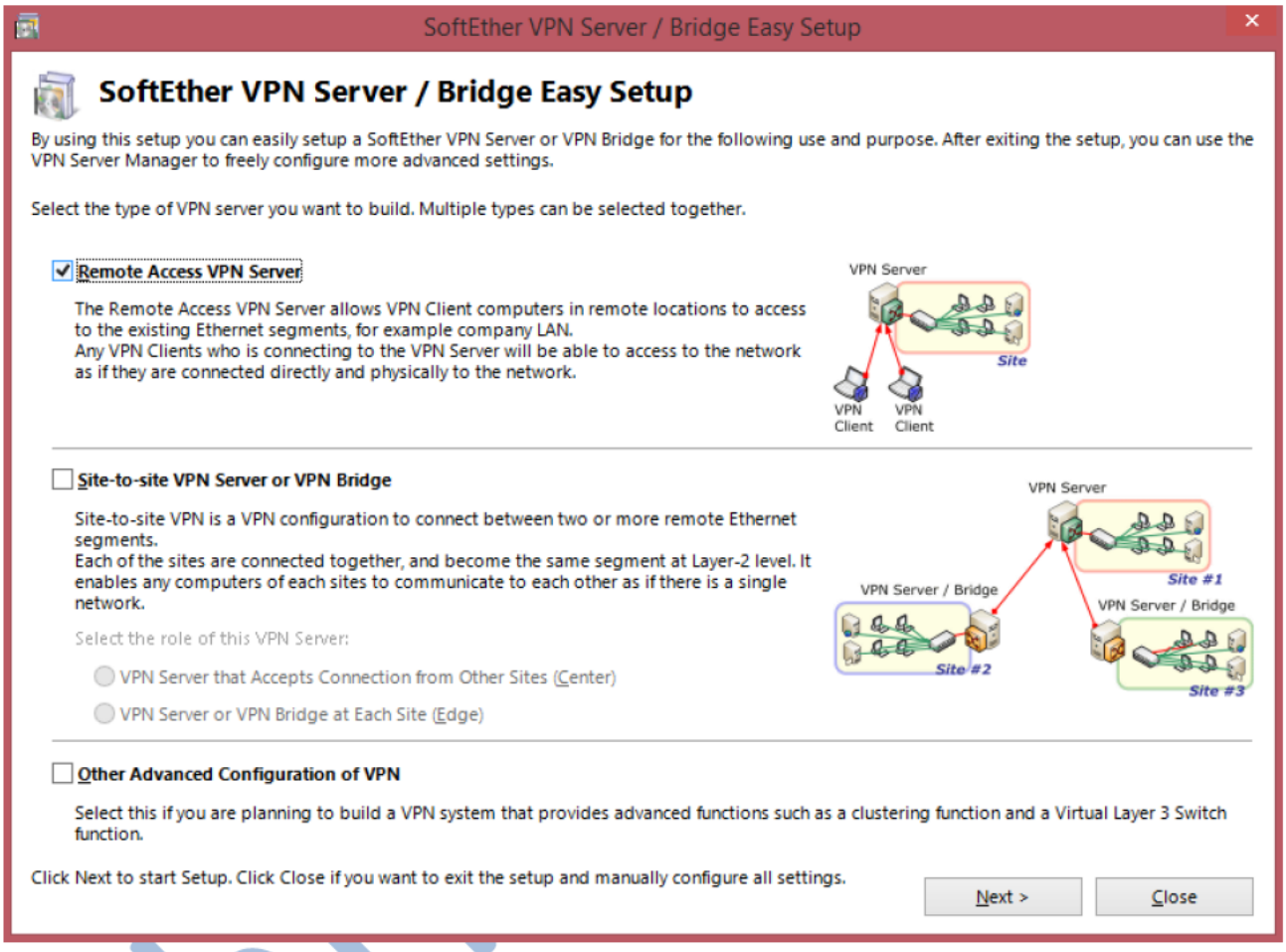


4. Sunucumuza VPN için şifre belirlemediğimiz için yeni şifre belirleme penceresi ekrana geliyor. Yeni şifrenizi 2 kere girerek OK tuşuna basın.

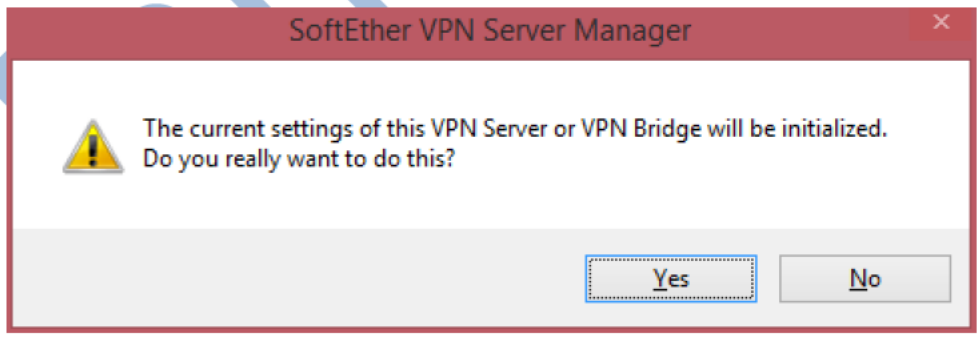


5. Önümüze gelen pencerede Remote Access VPN'i seçiyoruz. Diğer seçenekleri burada anlatmıyorum, eğer isteyen var ise, yukarda verdiğim vikipedia linki üzerinden inceleyebilirsiniz.

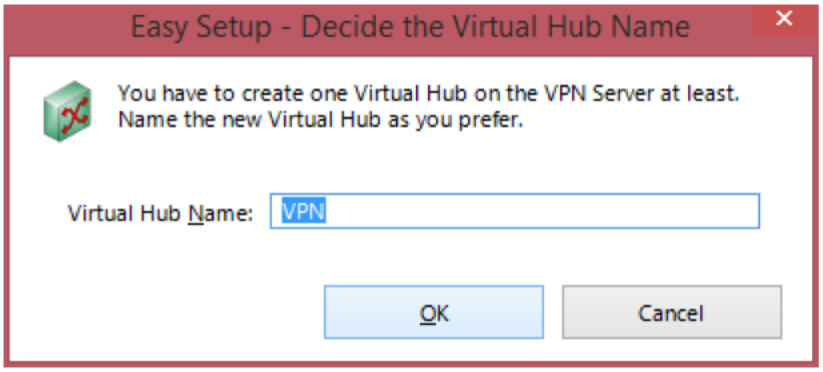
   Remote Access VPN ile, kendi cihazlarımızı, Amsterdam'a bağlayacağız ve oradan internete çıkış yapacağız.



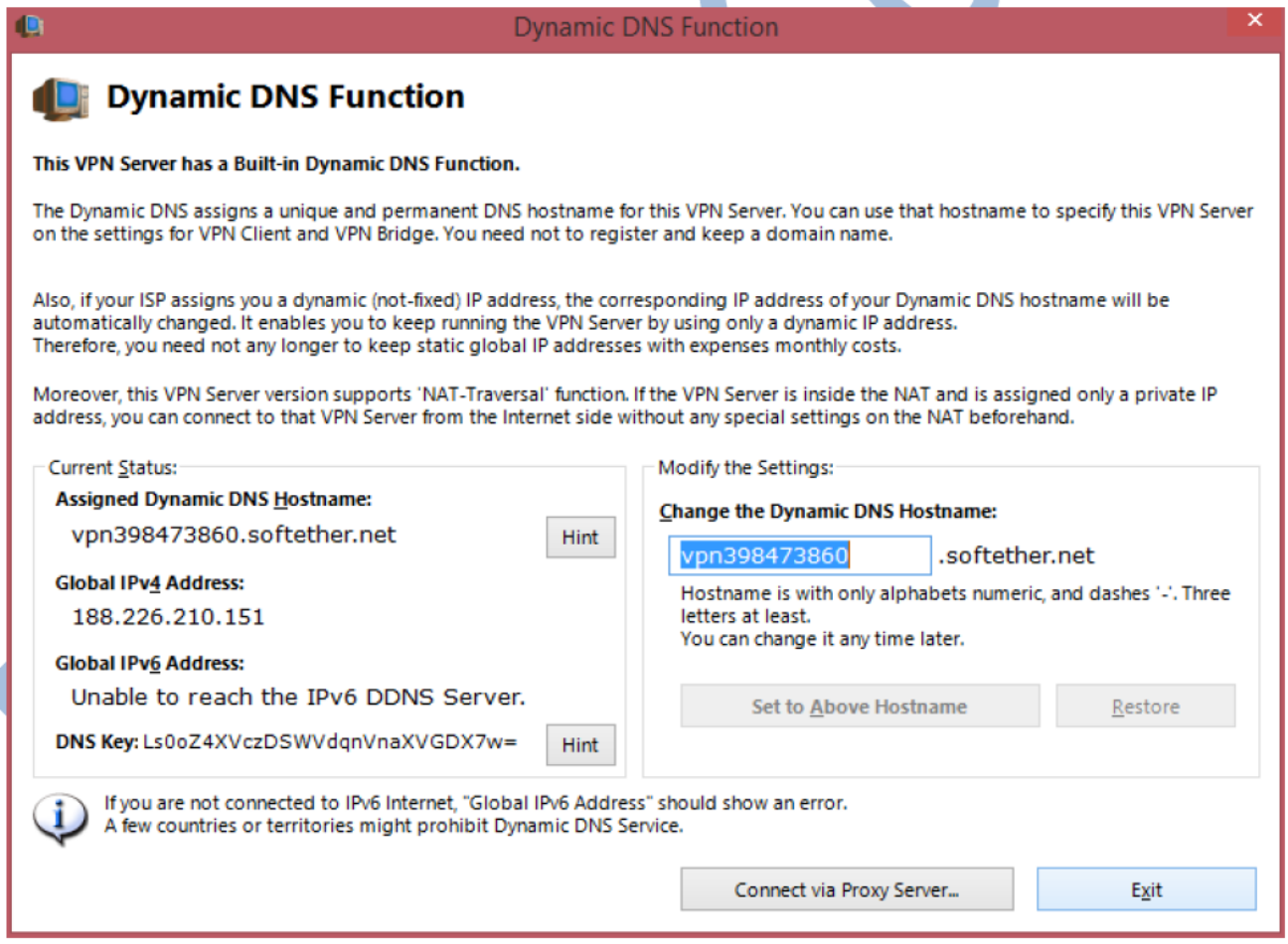
6. VPN initialize edilecek diyor, OK diyoruz.



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

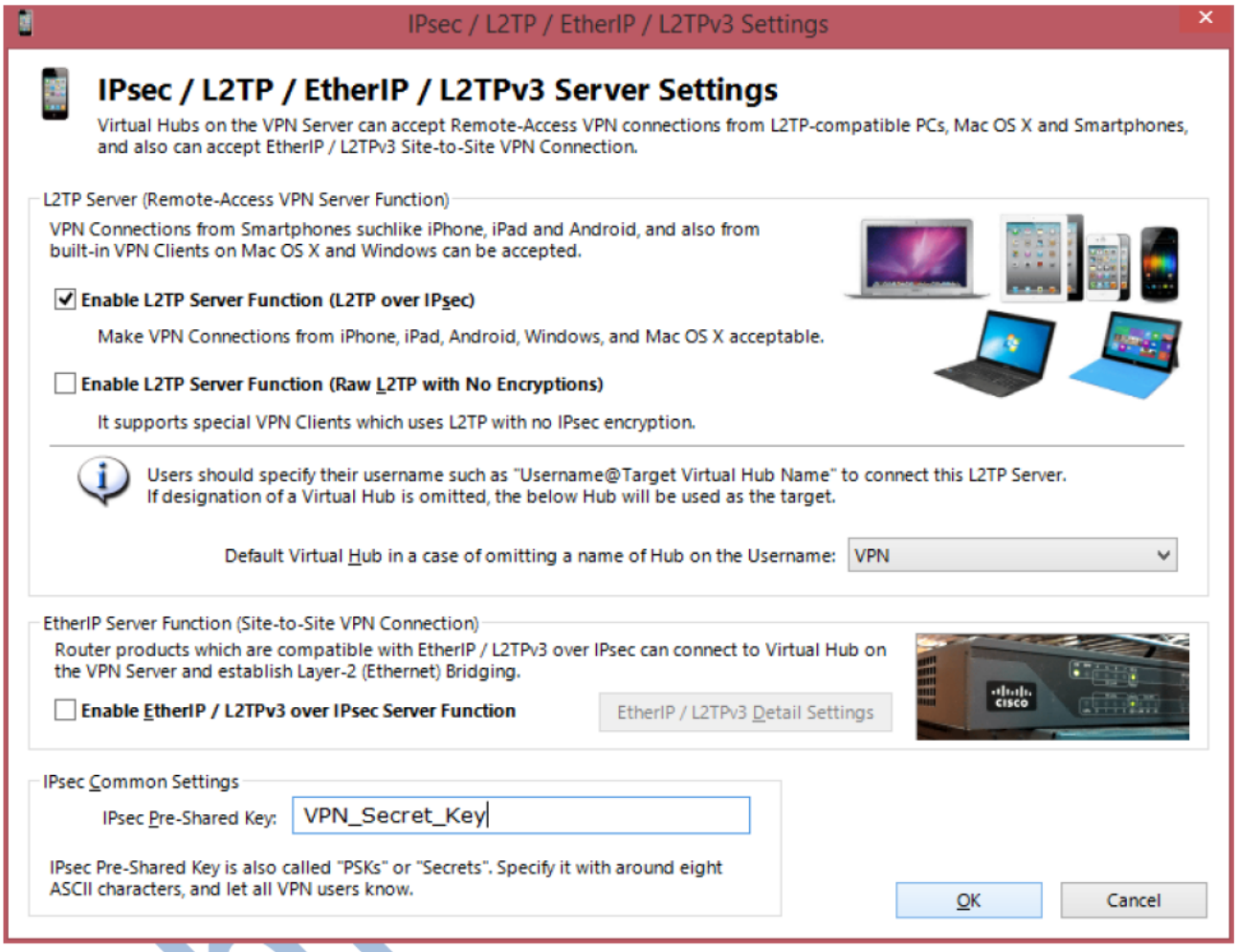


8. SoftEther istediğiniz taktide, IP adresi yerine dinamik olarak dns atayabiliyor. Ben bu özelliği kullanmak yerine, kendi domain adresimden IP'ye redirect yapıyorum, ama siz bunu kullanabilirsiniz.

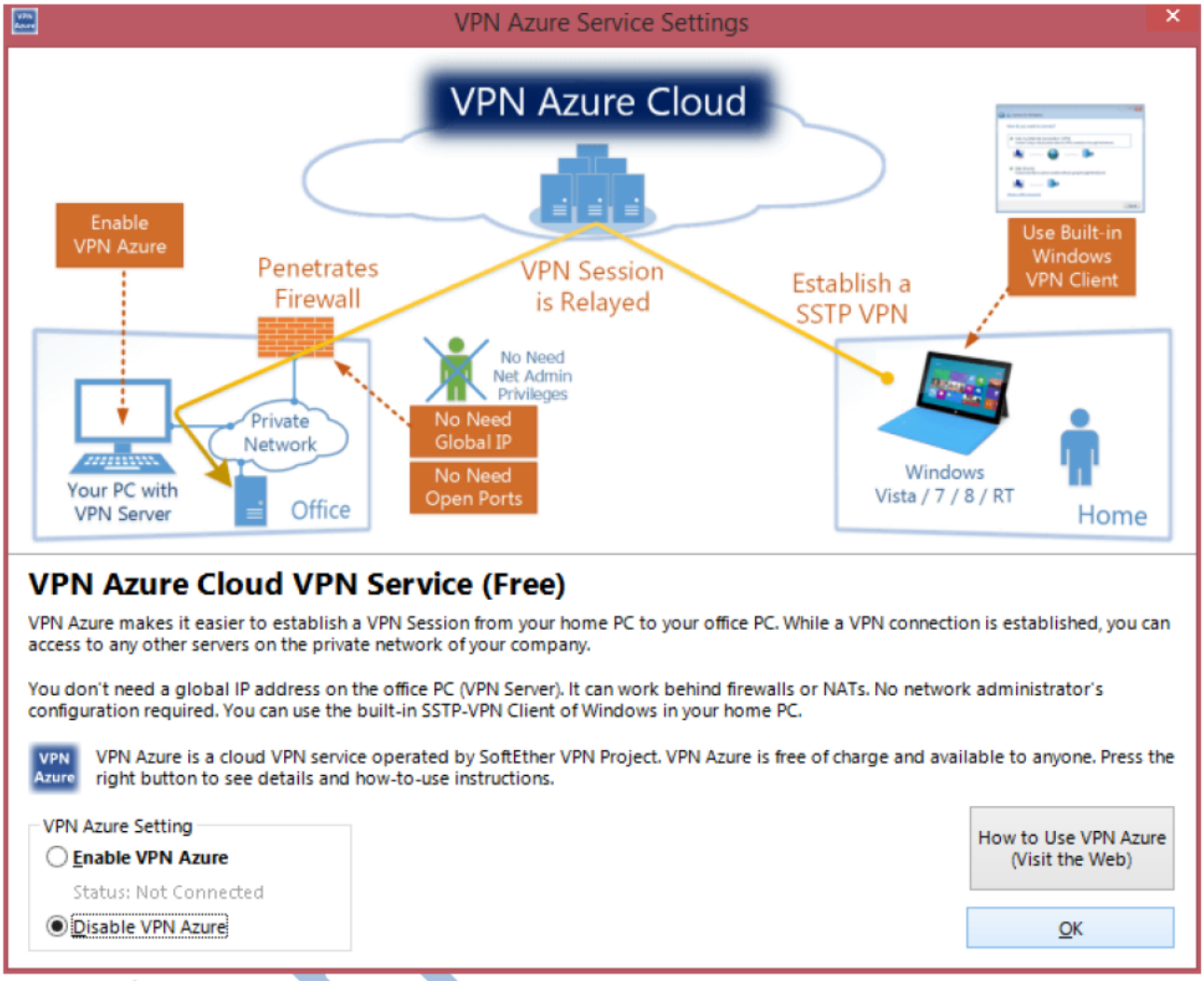


9. Burası önemli, L2TP Over IPsec'i seçiyoruz. Bu sayede tüm cihazlarımızı herhangi bir client kullanmadan güvenli bir şekilde sunucumuza bağlayacağız.

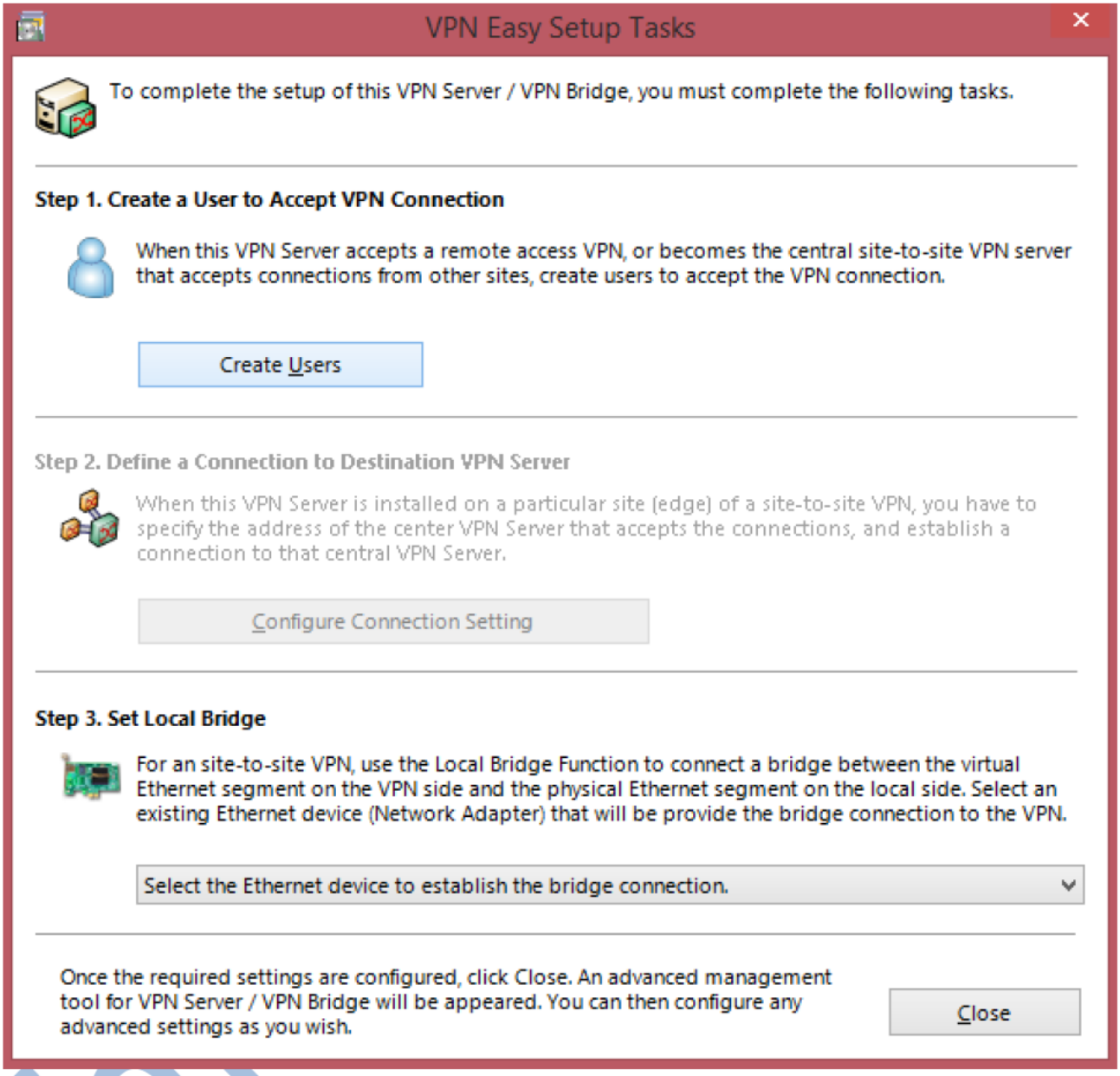
   Hemen altında yer alan IPsec Common Setttings kısmına, bir şifre giriyoruz, bu şifreyi de bir yere kaydediyoruz. İlerde bağlanırken lazım olacak.



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

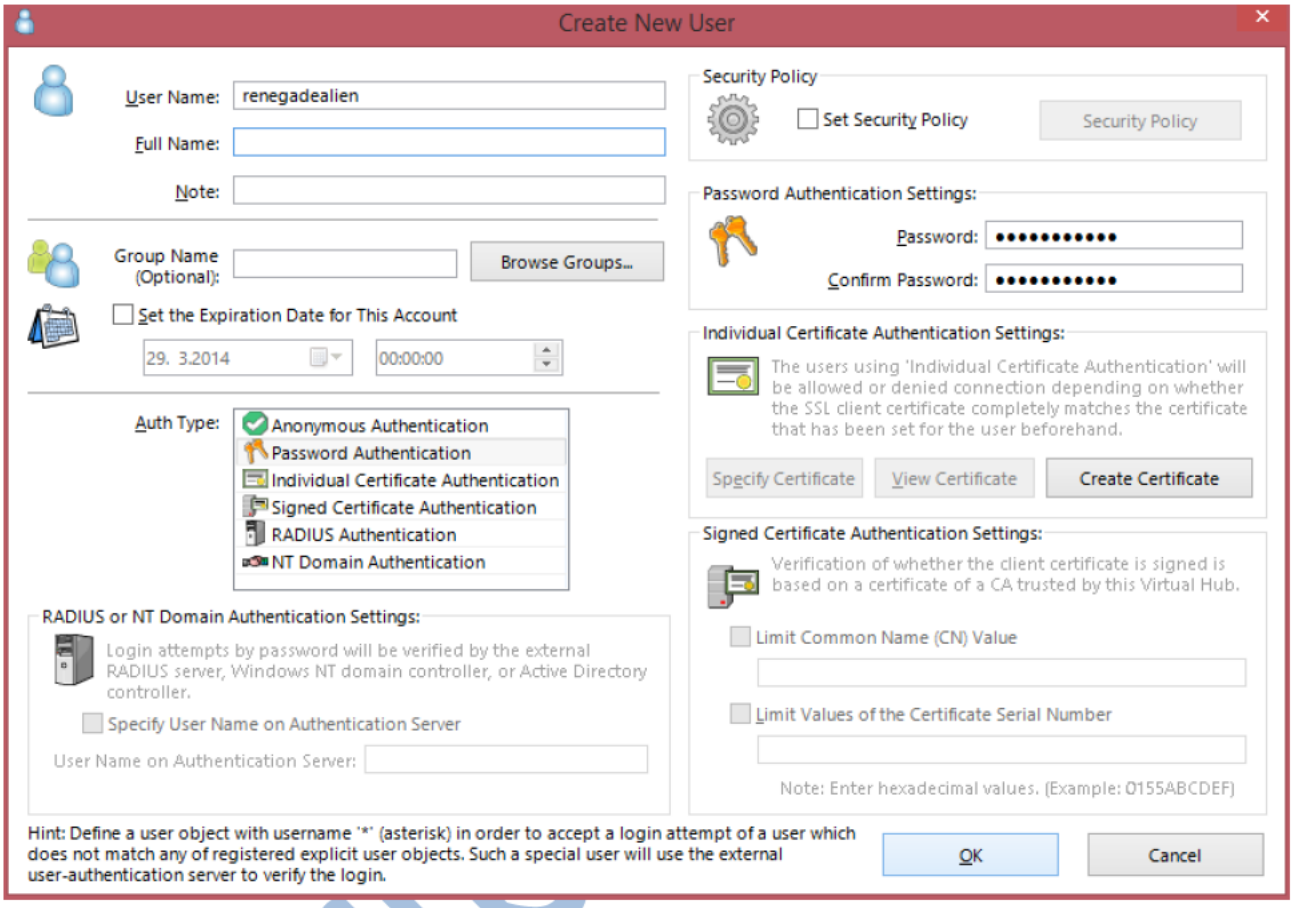


11. Kullanıcı oluşturma penceresine geliyoruz, Create Users butonuna tıklıyoruz.

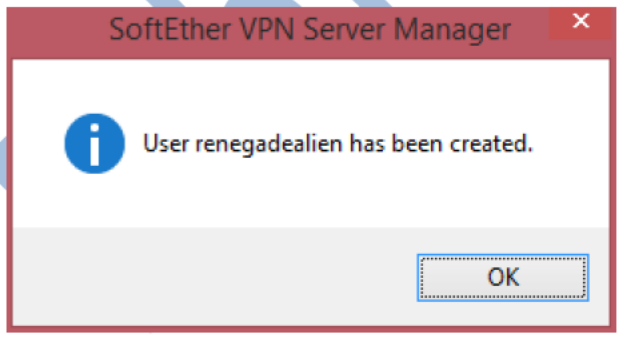


12. Kullanıcı adı giriyoruz, Auth Type kısmından Password Authentication'ı seçiyoruz. Password Authentication Settings kısından, giriş için kullanacağımız şifreyi giriyoruz.

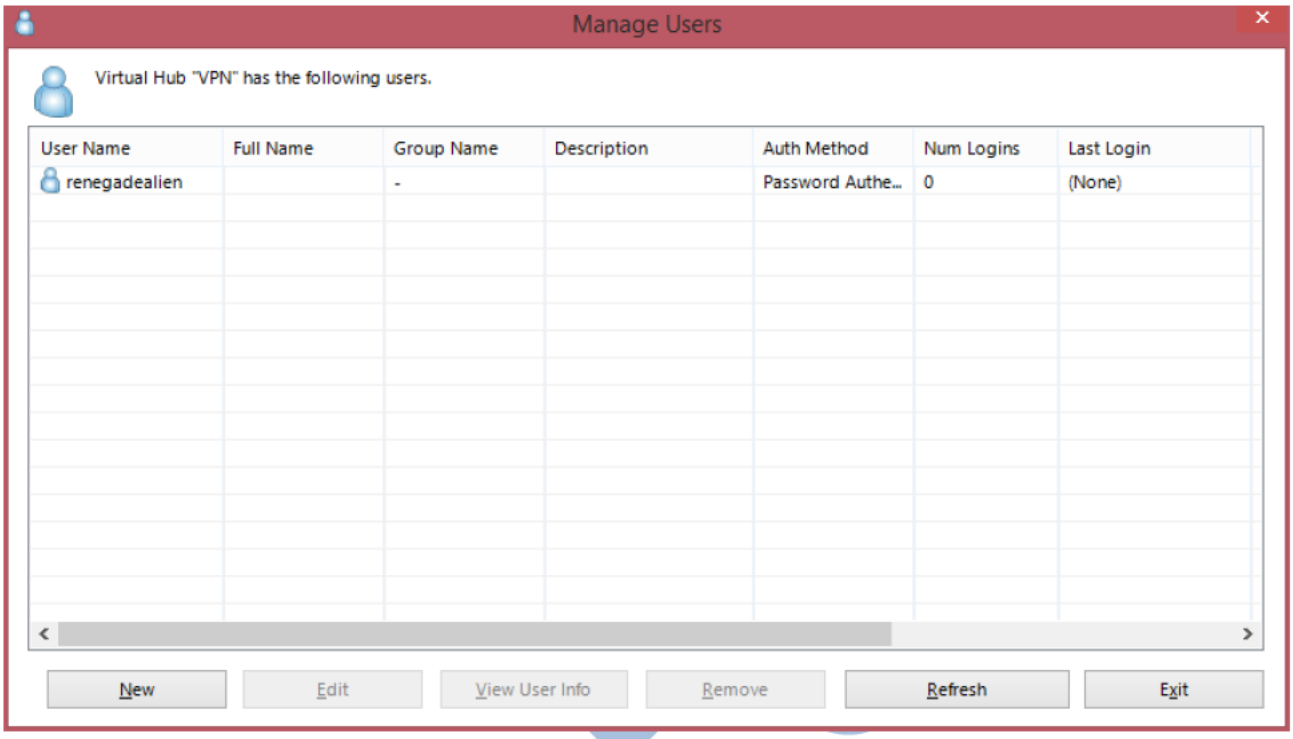
    Ok tuşuna basıyoruz.



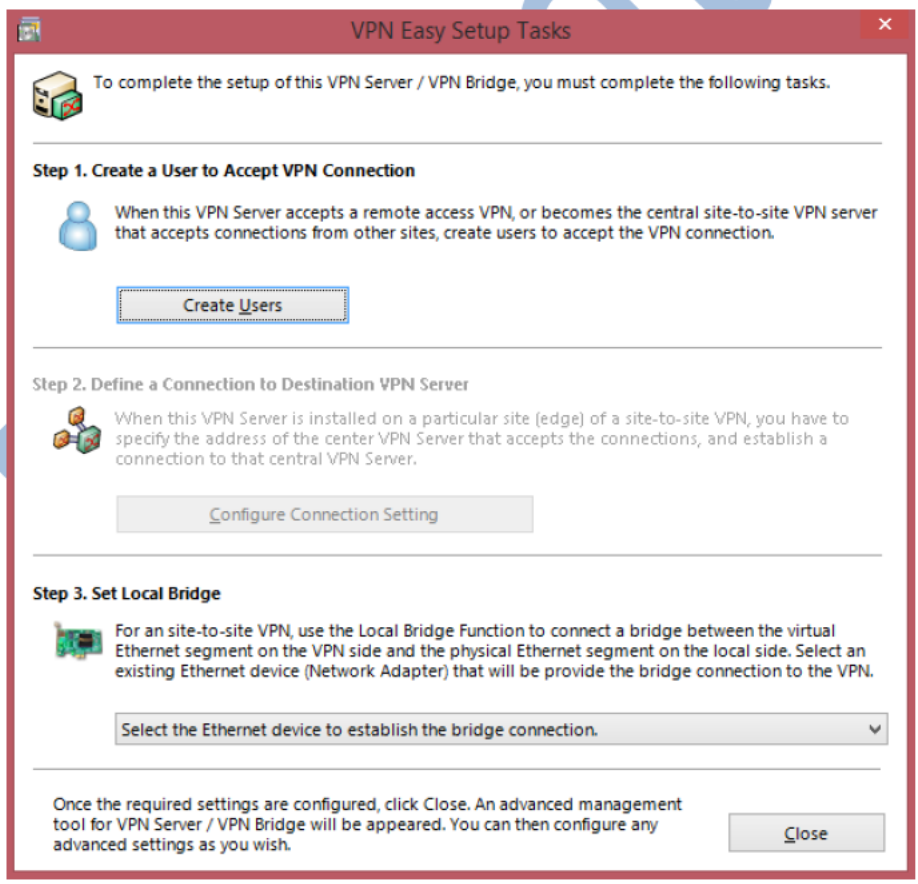
13. Kullanıcı kaydımız başarı ile tamamlandı.



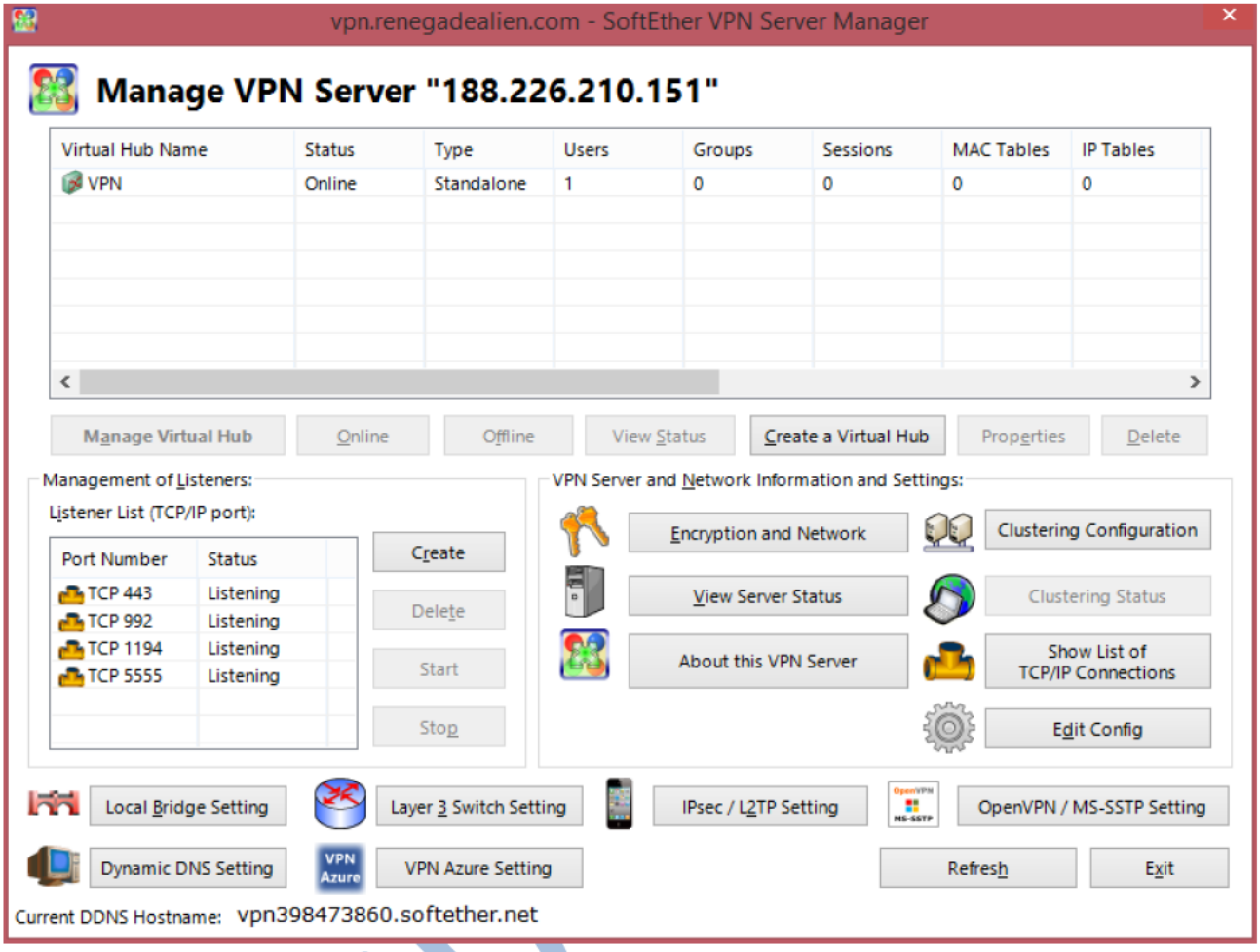
14. Ekranda VPN adlı HUB'a bağlı kullanıcılar görüntüleniyor. Exit diyerek çıkıyoruz.



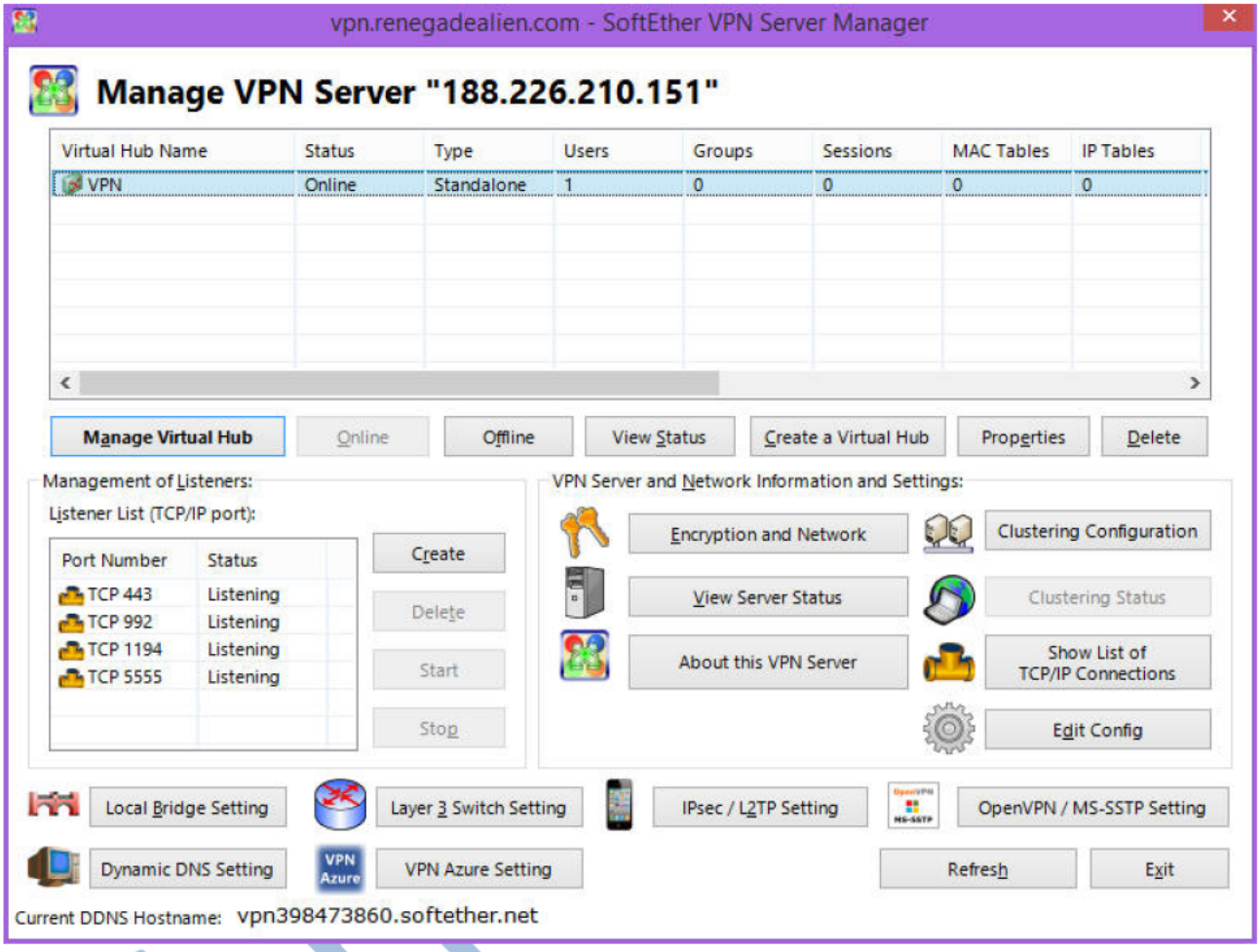
15. Close diyerek ekranı kapatıyoruz.



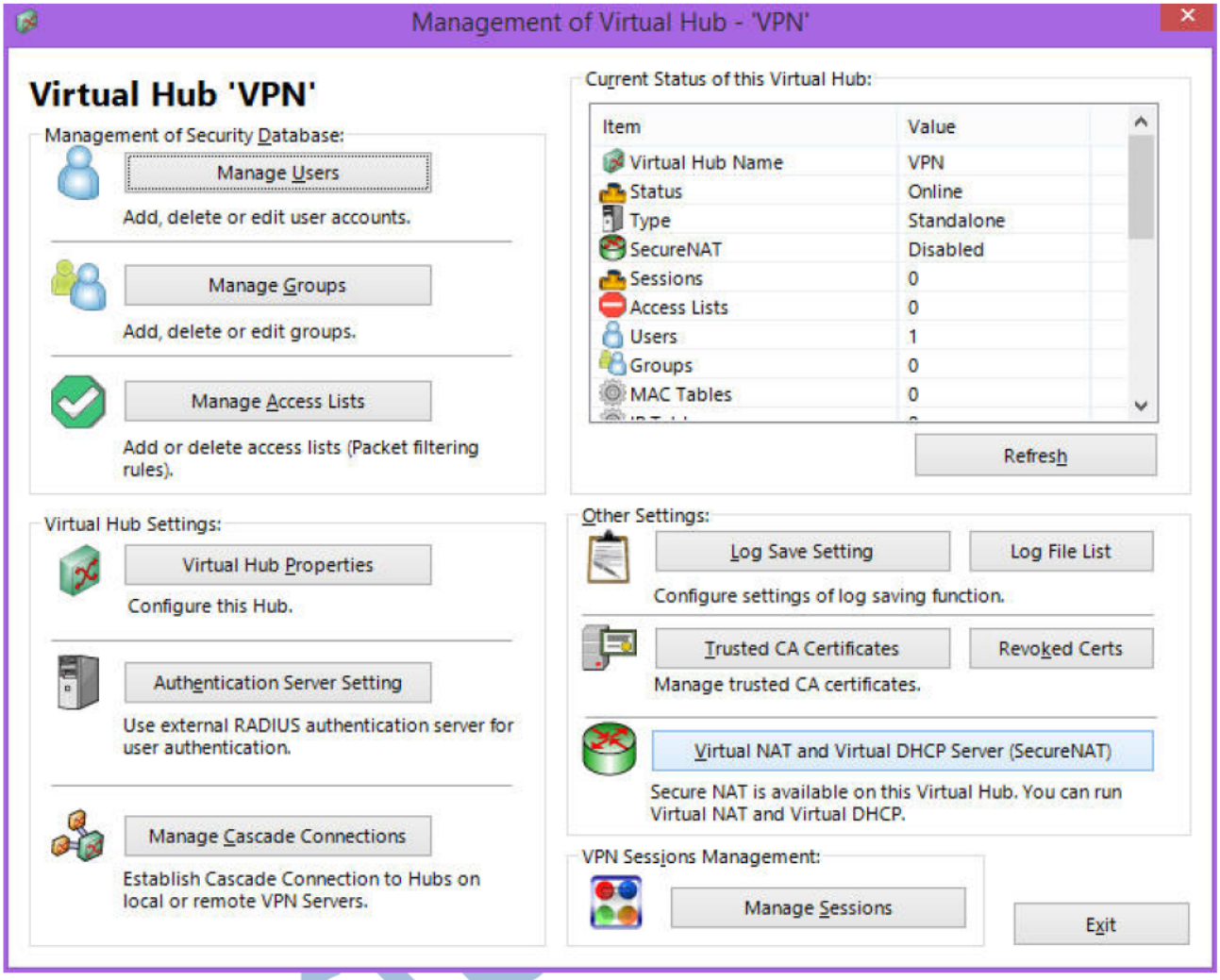
16. Şu anda VPN'imiz kuruldu.



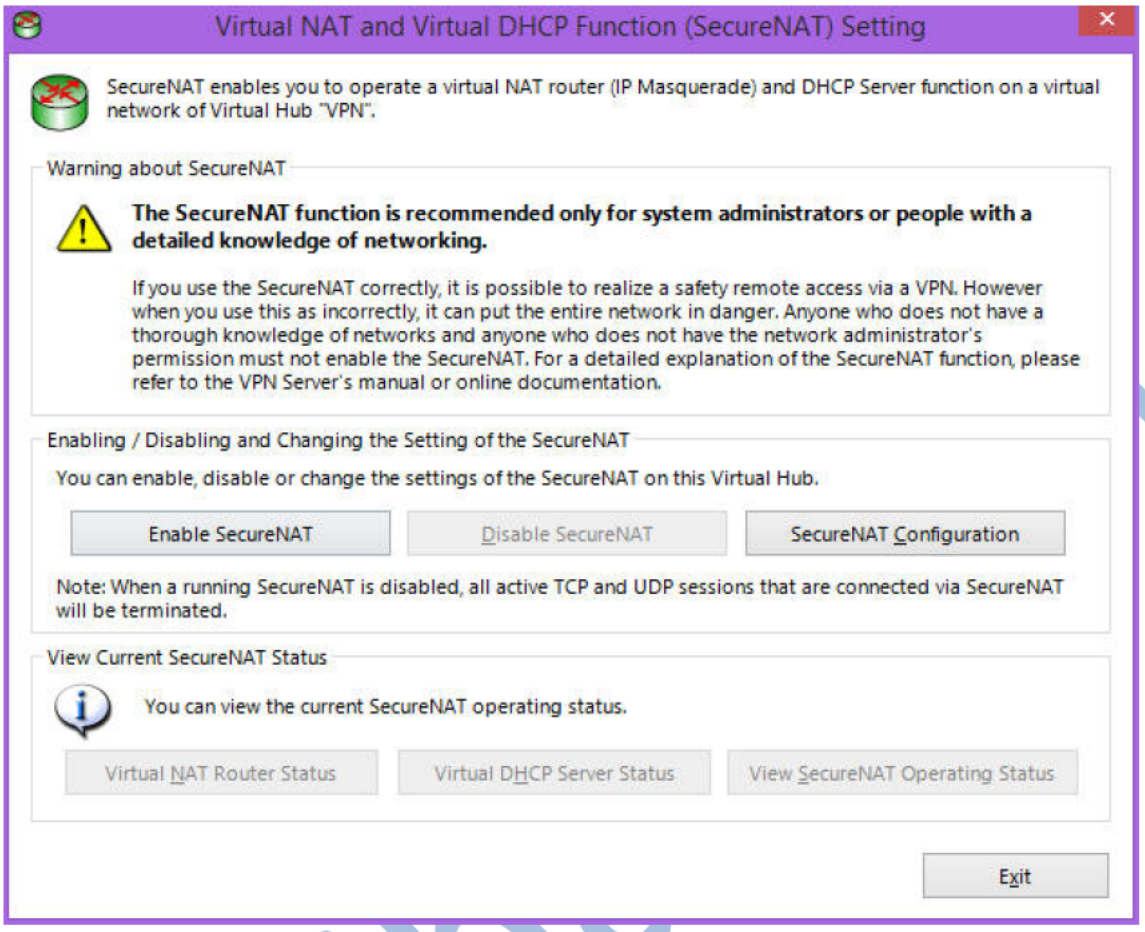
17. Kurulumun ardından, şu anda aslında network bağlantısı yapabilecek durumdayız. Fakat, sunucuya bağlanacak clientların IP alabilmesi için DHCP ve bağlanan kullanıcıların internete cıkarken sunucunun reel IP'sini kullanabilmeleri için NAT kurulumu yapacağız. Bunu için virtual hubımızı seçiyoruz ve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

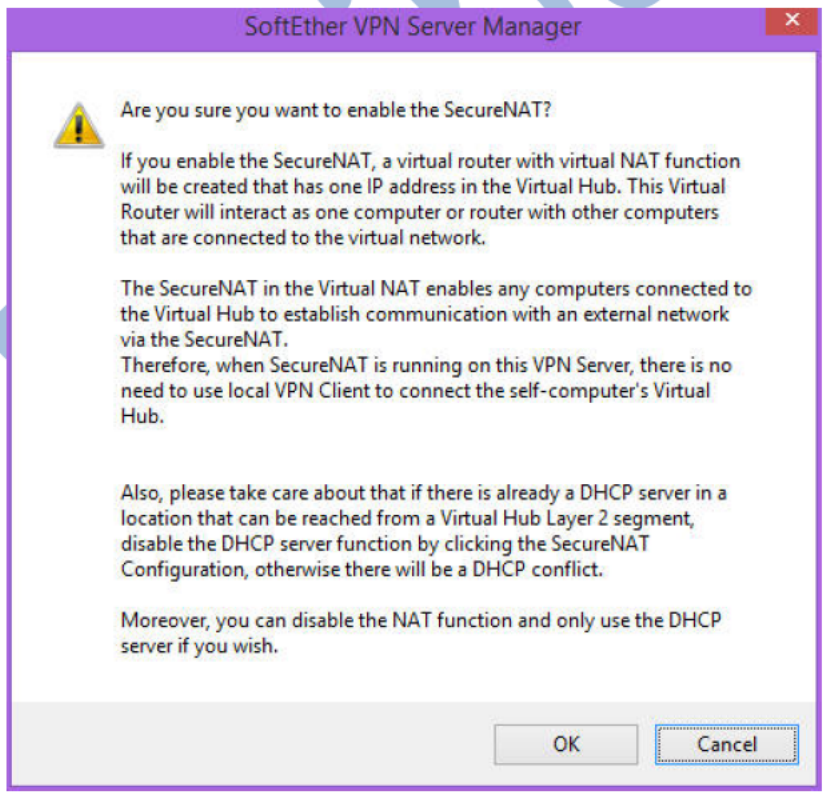


18. Virtual Nat and Virtual DHCP Server butonuna tıklıyoruz.



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

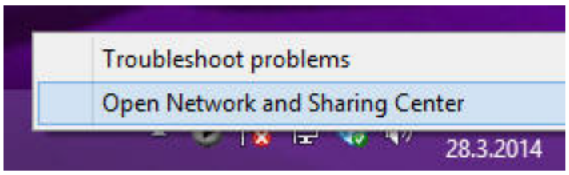




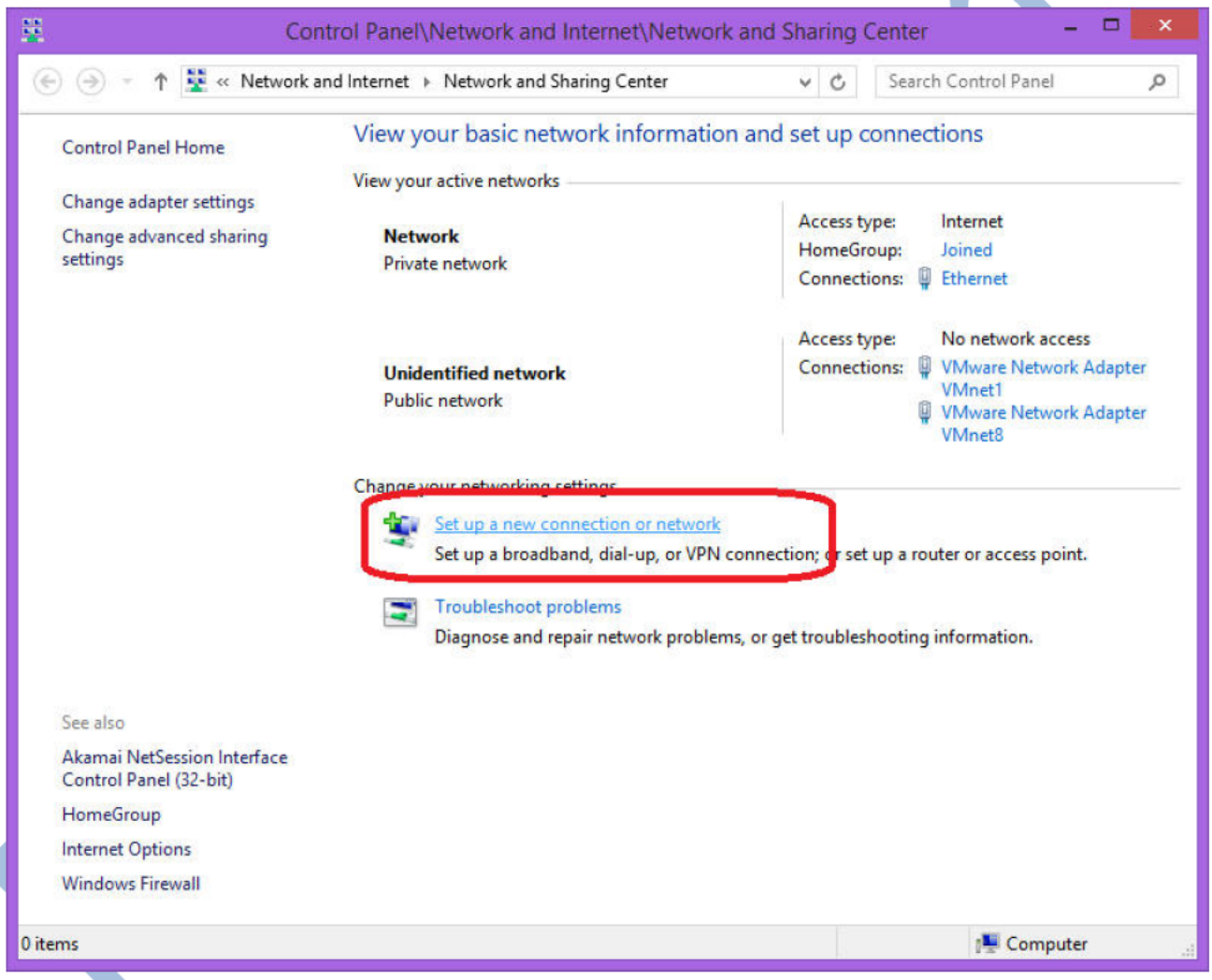
20. Şu anda VPN sunucu kurulumumuz bitti.

6. Windows7 / Windows 8 Üzerinden VPN'e Bağlanmak

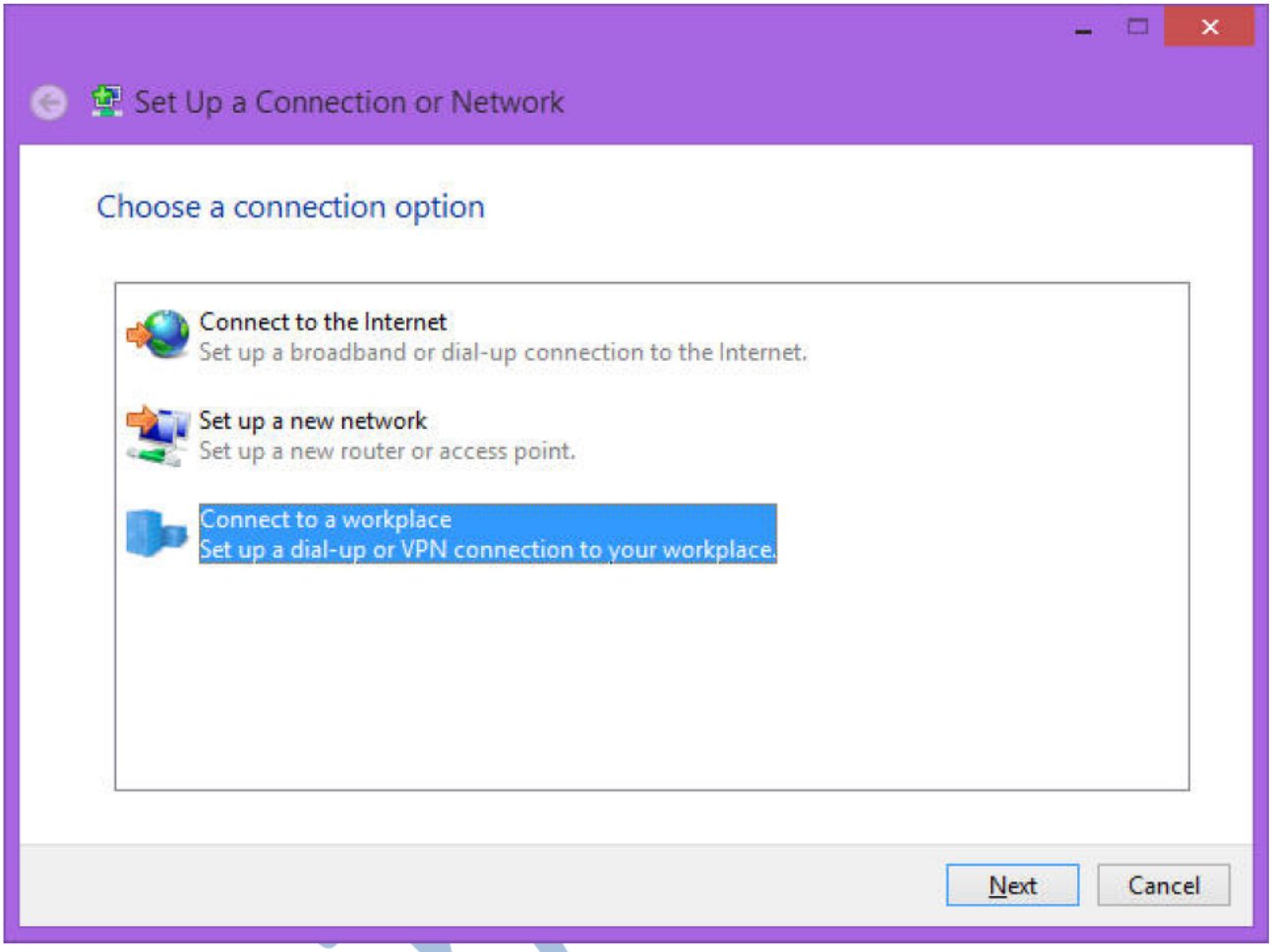
1. Open Network and Sharing Center butonuna tıklıyoruz.



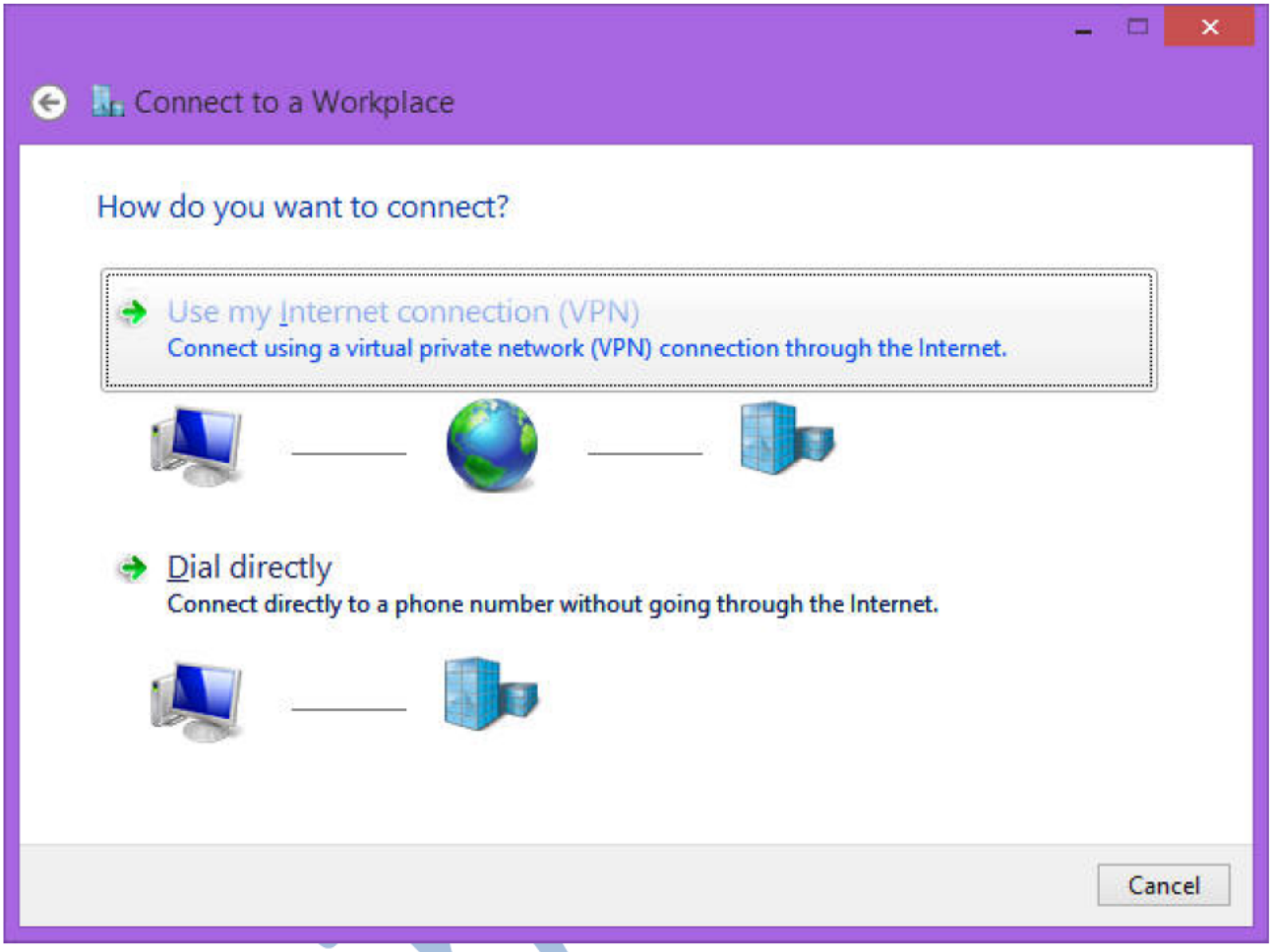
2. Set up a new connection or network linkine tıklıyoruz.



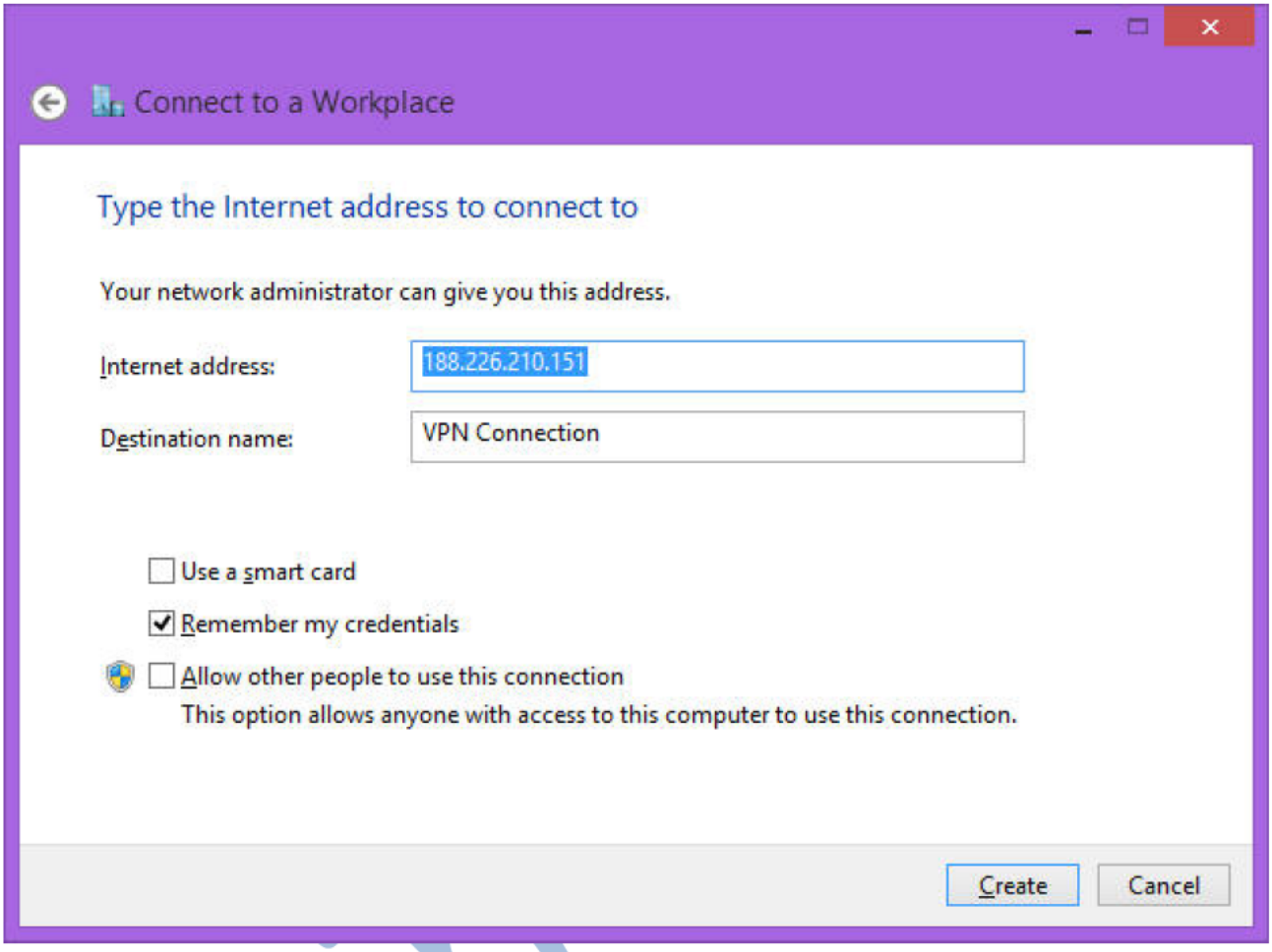
3. VPN bağlantısını seçiyoruz.



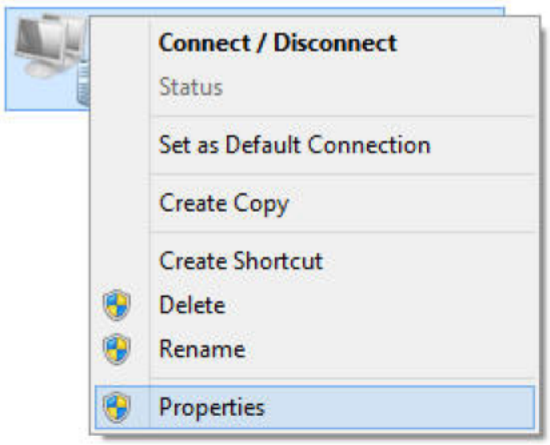
4. Use My Internet Connection botununa tıklıyoruz.



5. Sunucunun adresini giriyoruz ve bir isim veriyoruz.

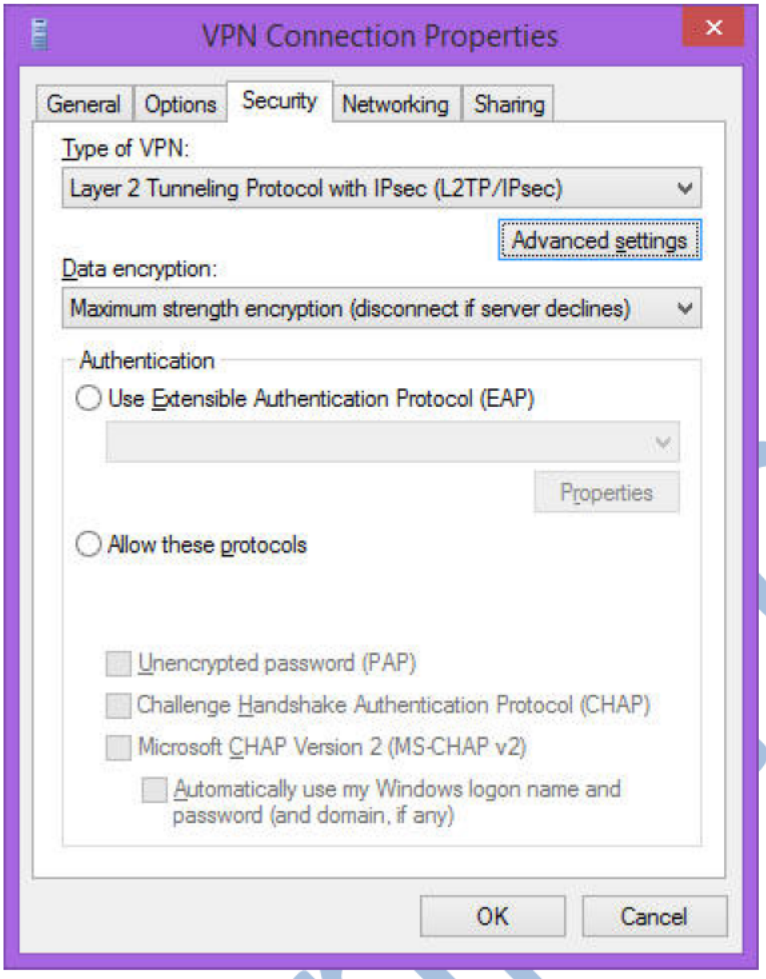


6. Ağ Bağlantılarına giriyoruz. VPN Connection isimli Connection'u bulup sağ tuş, properties penceresini açıyoruz.

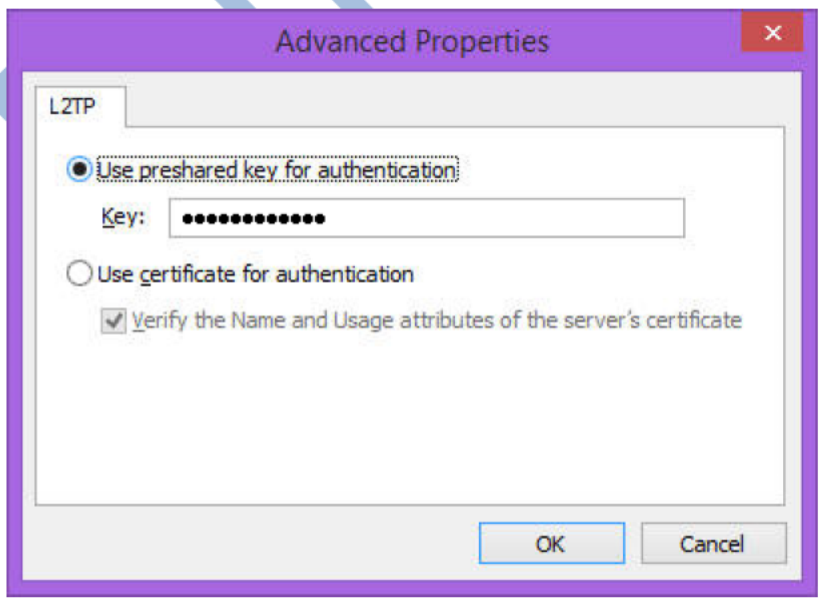


7. Security sekmesinde aynen kurduğumuz gibi Layer2 Tunnelling Protocol Over IPSec'i seçiyoruz.

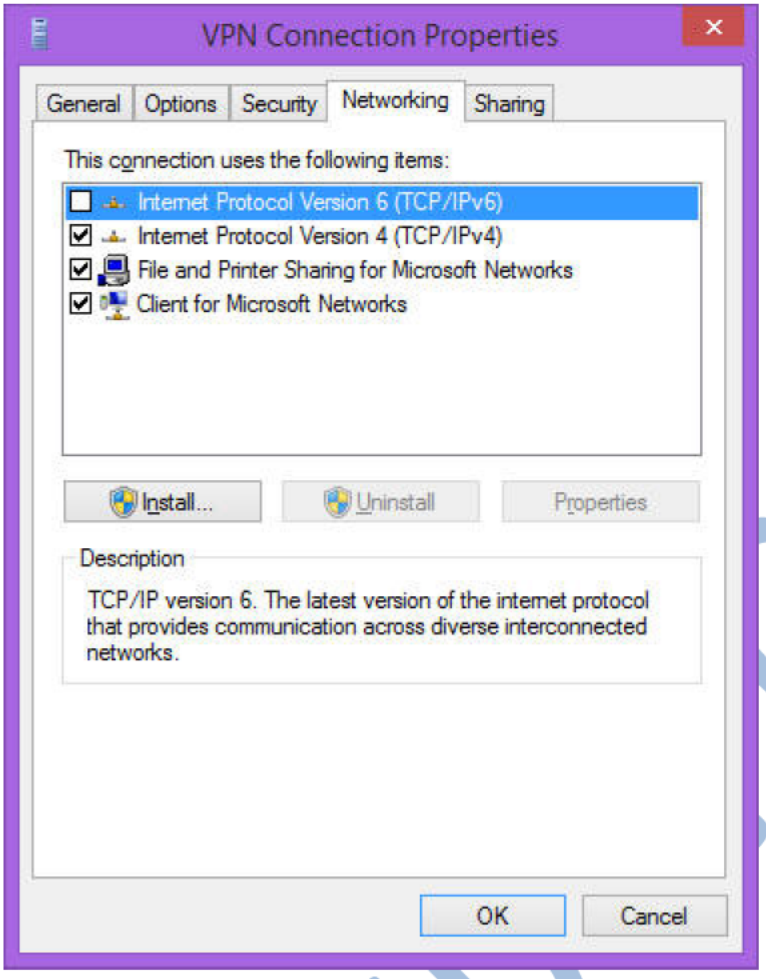
   Data Encryption kısmında, Maximum strength'i seçiyoruz.



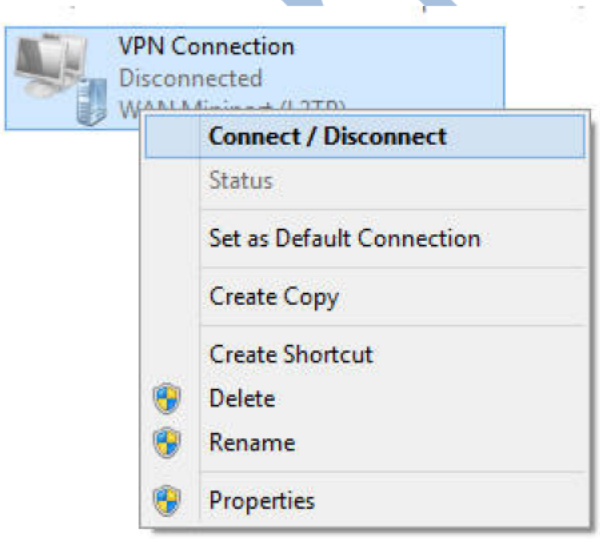
8. Advanced tabına tıklayıp, **4. bölümün 9. adımında belirlediğimiz** şifreyi giriyoruz :) O zaman not alın demiştim:)



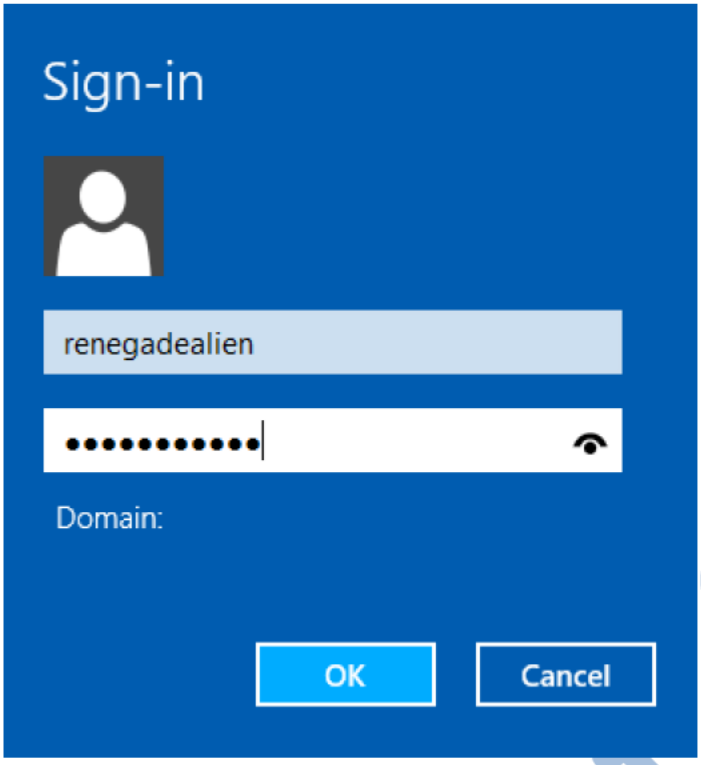
9. Networking sekmesinden IPv6'yı kaldırıyoruz. OK diyerek kapatıyoruz.



10. VPN Bağlantımıza sağ tuş tıklayarak Connect diyoruz.

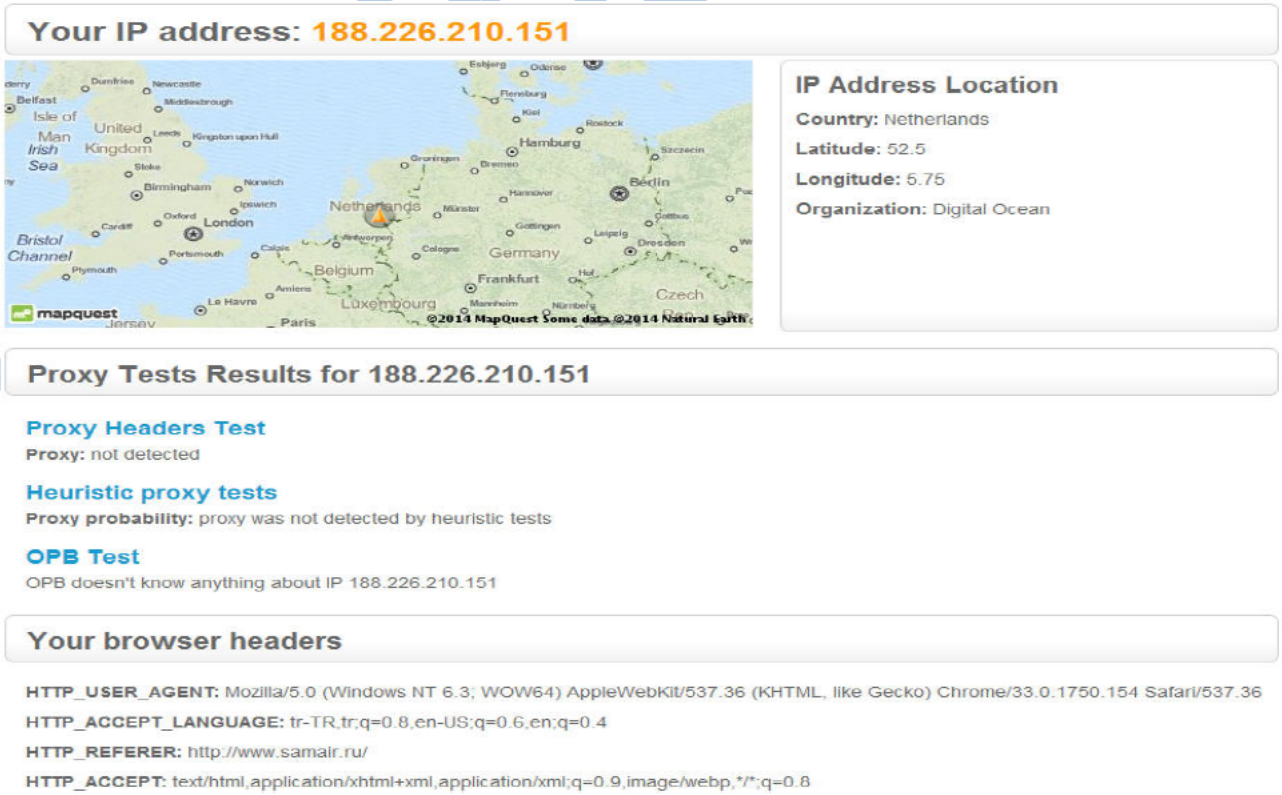


11. **4. bölümün 12. adımında belirlediğimiz** Kullanıcı adı ve şifremizi giriyoruz.

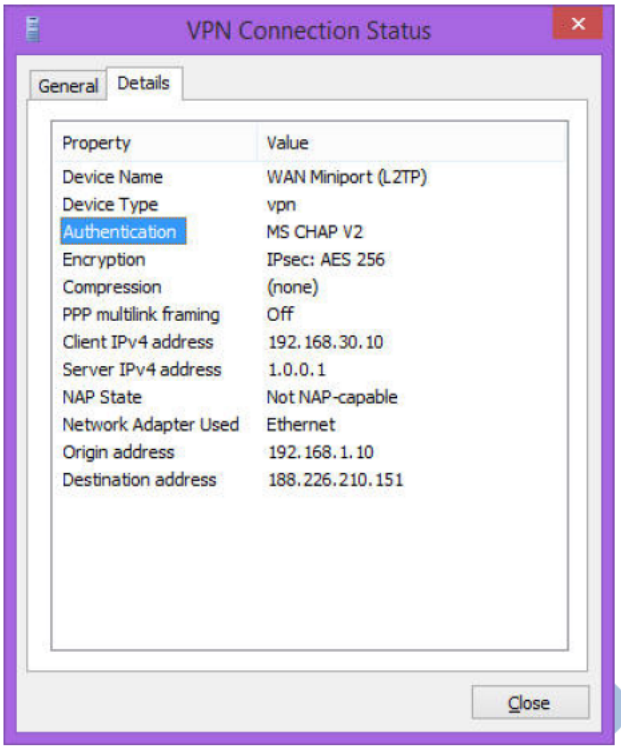


12. Sonunda bitti :) http://ip.proxy.lc/ adresinden anonimliğimizi kontrol ediyoruz.

Hollanda'dayız :) :)



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 olduğunuda üzülerek görmüş bulunmaktayım :)

8. Linux Üzerinden VPN'e Bağlanmak

Linux işletim sistemlerinde, L2TP default olarak gelmiyor. İnternetten L2TP on <linux dağıyımınız > şeklinde aratırsanız, uygun sonuca ulaşacaksınızdır.

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

9. Sonuç

Yukarıdaki adımları sırayla tamamlayarak, yurtdışı kaynaklı, güvenli ve size özel VPN servisinizi kurabilir, arkadaşlarınız ile paylaştırabilirsiniz. Paylaşım yapacağınız tüm arkadaşlarınıza açacağınız kullanıcı adı ve şifre sayesinde, bandwith 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 kullanımınının 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