OpenVPN ile VPN Uygulamaları

- VPN Nedir?
- VPN Çeşitleri
- Açık kod VPN çözümleri
- OpenVPN Nedir?
  - Temel özellikleri
- Kurulum
  - Linux
  - FreeBSD
  - OpenBSD
- Kurulum Sonrası Genel Yapılandırma
- OpenVPN Çalışma Yapısı
  - Routing mode
  - Bridge mode
- Sunucu tarafı VPN yapılandırması
- İstemci tarafı VPN yapılandırması
- Windows XP için OpenVPN istemci ayarları
- Alternatif kimlik doğrulama Yöntemleri

Huzeyfe ÖNAL <Huzeyfe@EnderUNIX.ORG>

EnderUNIX Yazılım Geliştirme Takımı - Şubat 2006

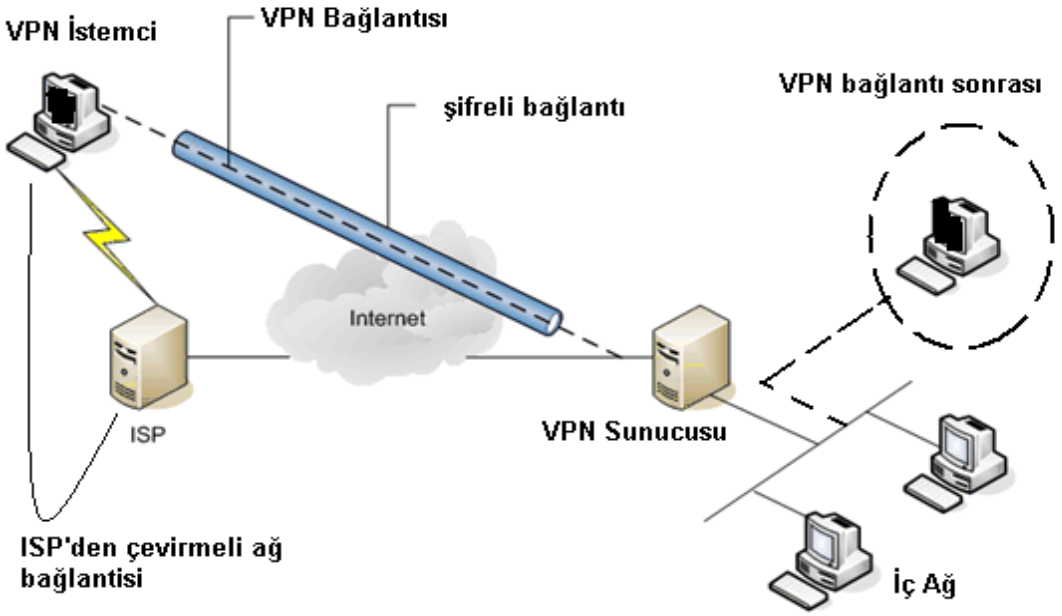
VPN Teknolojisi

VPN(Virtual Private Network/Sanal Özel Ağ) internet üzerinden şifreli ve güvenli veri iletişimi sağlamak için düşünülmüş bir teknolojidir. Kiralık hatlar(Lease-line) gibi daha güvenli, sağlam çözümlerin yerine VPN kullanilmasinin temel nedeni, maliyet ve kolay yapılandırmadır.

Temelde iki tip VPN teknolojisi vardır. Amacımıza gore bu iki VPN teknolojisinden birini seçebiliriz. Bu teknolojiler "Remote Access VPN " ve "Site-to-site VPN" olarak geçer.

Remote Access olarak tanımladığımız VPN türü, firmaların gezgin çalışanlarının firma ağına heryerden güvenli iletişimlerini sağlamak için kullanılır. Ya da büyük bir firmanın farklı lokasyonlardaki şubelerini merkeze bağlamak için kullanılır.

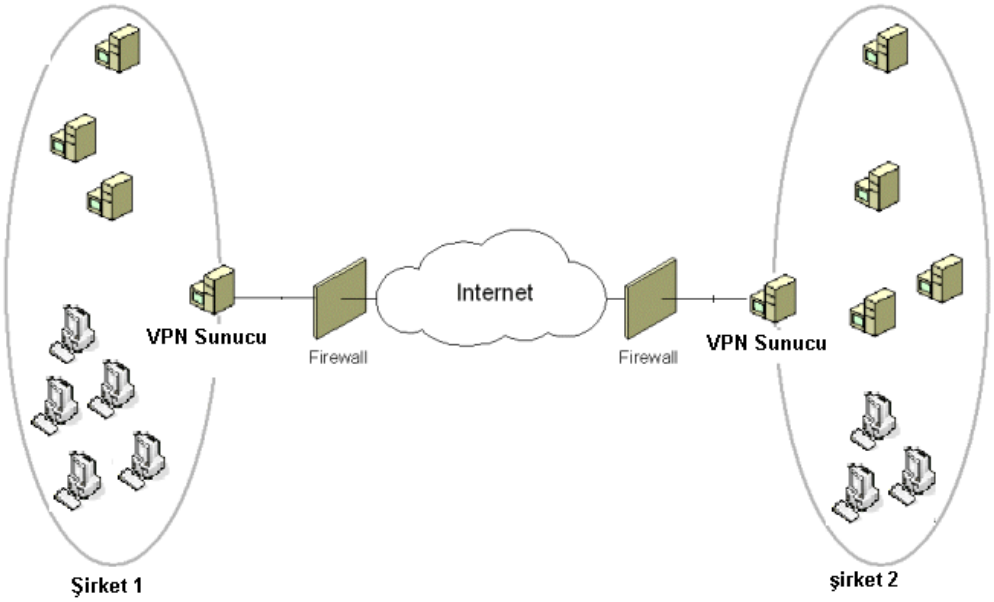
Basitçe resimleyecek olursak: Firmamızın satış elemanı Sivas'da bir görüşme sonrası bazı belgeleri print etmesi ya da ofisteki bir kaynağı kullanması gerekti, bunu normal internet üzerinden yapmak hem riskli hem de bir o kadar zordur. Bunun yerine biz elemanımıza VPN istemcisi kurarak istediği yerden şirket ağına bağlanarak "belirli" işlemleri gerçekleştirebilmesini ve "belirli" kaynaklara erişimi sağlayabiliriz -ki tercih edilmesi gereken yöntem de budur-.



Şekil-1

Site-to-site VPN

Bu tip VPN genellikle farklı firmaların birbirleri ile VPN aracılığı ile güvenli iletişim kurmaları için düşünülmüştür. Aynı zamanda firmanın farklı lokasyonlardaki şubelerinin merkeze bağlanmasını da sağlar. Remote Acces VPN'den temel farkı VPN işlemini gören iki uçta VPN sunucu olması.



Şekil-2

VPN teknolojileri hakkında daha detaylı bilgi edinmek için **Penguence Sayı 2**'deki "Sanal Özel Ağ, Kriptoloji ve PKI Teknolojileri" yazısına gözatmanızı tavsiye ederim. Kısaca VPN teknojisine değindikten sonra bu teknolojiyi en etkin ve ucuz bir sekilde uygulamanın yollarına bakalım.

Açık Kod VPN Çözümleri

Açık kod dünyasında her amaca yönelik çeşitli çözümler vardır. Bu çözümlerin bazıları diğerlerine göre daha fazla tutulur, kullanılırlar ve o teknolojinin adı anıldığında insanların aklına gelir. Mesela bugün port tarama konusunun geçtiği her kitap/yazıda açık kodlu port tarama programı Nmap'den bahsedilir. Nmap ya da benzer diğer popüler açık kodlu yazılımlar, bunu basitlik, projeyi sahiplenme ve bol dökümantasyon özellikleri ile başarmışlardır denilebilir.

VPN çözümlerinde de öne çıkmış bir iki Açık kod yazılım vardır. Bunlardan biri OpenVPN, diğeride Linux OpenSWAN(Ya da daha kararlı bir çözüm olarak OpenBSD Ipsec).

AçıkKod VPN çözümleri ile ilgili olarak detay bilgiyi kaynaklar kısmından edinebilirsiniz**[ref 4]**

Bunun yanında açıkkod dünyasında farklı VPN teknolojilerini kullanarak benzer amaçları gerçekleştiren çeşitli VPN yazılımları da vardır. Bunlardan en sık kullanılanları;

PPTP Çözümü : Poptop
Ipsec Çözümü : Linux OpenSWAN, OpenBSD Ipsec
SSL VPN Çözümü : SSLExplore, OpenVPN
L2TP Çözümü : OpenL2tp

Gerçek bir VPN Çözümü Olarak OpenVPN

OpenVPN multi platform SSL VPN çözümüdür. Endüstri standardı SSL/TLS protokollerini kullanarak OSI 2. ve 3. katman seviyesinde şifreli ağ erişimi sağlar.

NOT:SSL VPN denilince akla gelen bir browser aracılığı ile ek bir program gerektirmeksizin VPN yapmaktır. Fakat buradaki SSL VPN tanımı farklıdır.

OpenVPN ile yapılabilecekler;

- Linux, Windows 2000/XP ve üzeri, OpenBSD, FreeBSD, NetBSD, Mac OS X ve Solaris işletim sistemlerinde çalıştırılabilir.

- OpenSSL kütüphanesinin sunduğu encryption, authentication, ve certification özelliklerini kullanabilir.
- Nat üzerinden sorunsuz tünelleme imkanı
- İsteğe bağlı olarak GUI ile yönetim.
- Kablosuz ağlar için güvenli erişim imkanı

OpenVPN'in kısa sürede bu kadar popüler olmasının nedeni hem güvenli bir altyapı sunması hem de kurulum ve

yönetiminin basit olması denilebilir. OpenVPN, Ipsec gibi işletim sisteminin çekirdeğinde temel değişiklikler gerektirmez.

OpenVPN Kurulumu

Yaygın kullanılan üç işletim sistemi için kurulum adımları;

OpenVPN dosyalarinin taşınacağı ortak alanı oluşturalım

```
#mkdir /usr/local/etc/openvpn
```

OpenBSD için Kurulum Adımları

OpenBSD üzerinde OpenVPN kurulumu icin ister OpenBSD paket sistemi(ports) ister kaynak koddan kurulum yöntemi izlenebilir. Biz burada kaynak koddan kurulum ile ilerleyeceğiz

OpenBSD Kurulumu: OpenBSD 3.8 kurulumu icin http://www.enderunix.org/docs/openbsd.avi adresindeki kurulum videosu takip edilebilir.

Kaynak Koddan kurulum

Kaynak koddan kurulum için sistemde wget programı kurulmalıdır.

OpenBSD için wget kurulumu;

```
#pkg_add -v
ftp://ftp.enderunix.org/pub/OpenBSD/3.7/packages/i386/wget-
1.8.2.tgz
```

```
Lzo Kurulumu

#cd /usr/ports/archivers/lzo
#make && make install
```

```
# mkdir /usr/src/openvpn
# cd /usr/src/openvpn/
```

Son sürüm openvpn paketi indirilerek açılır

```
# wget http://openvpn.net/release/openvpn-2.0.5.tar.gz

# md5 openvpn-2.0.5.tar.gz
MD5 (openvpn-2.0.tar.gz) = ***
```

Not: http://openvpn.net/sig.html adresinden MD5 SHA1 imzalari kontrol edilebilir.

```
#tar zxvf openvpn-2.0.5.tar.gz

#cd openvpn-2.0.5

# ./configure --with-lzo-lib=/usr/local/lib --with-lzo-
headers=/usr/local/include/

#make

#make install

#mv easy-rsa sample-scripts sample-config-files plugin
contrib/    /usr/local/etc/openvpn/
```

OpenBSD paket yonetim sistemi kullanarak kurulum

```
#cd /usr/ports/net/openvpn
#make install
```

Kurulum sonrasında örnek yapılandırma ve gerekli scriptler

/usr/local/share/examples/openvpn/ dizini altına atılmaktadır. Bu dizini /usr/local/etc/openvpn dizini olarak kopyalayalım.

FreeBSD için Kurulum

NOT: FreeBSD için port ağacından Kurulum için

```
#cd /usr/ports/security/openvpn
#make
#make install
```

Komutları verilmelidir.

NOT: Sistemin açılışında otomatik başlaması için /etc/rc.conf dosyasına
openvpn_enable="YES"
satırı eklenir

Standart kurulum için OpenBSD kurulum adımları takip edilebilir.

Red Hat Linux Enterprise için Kurulum

```
# mkdir /usr/src/openvpn
# cd /usr/src/openvpn/
#wget http://openvpn.net/release/openvpn-2.0.5.tar.gz
#tar zxvf openvpn-2.0.5.tar.gz

#cd openvpn-2.0.5

#./configure --with-lzo-lib=/usr/local/lib --with-lzo-
headers=/usr/local/include/

#make

#make install

#mv easy-rsa sample-scripts sample-config-files plugin
contrib/    /usr/local/etc/openvpn/
```

Kurulum sonrası genel yapılandırma

Her üç işletim sistemi için kurulum sonrasında yapılandırma dosyalarını ana bir dizine taşıyarak bunda sonraki işlemlerin üç işletim sistemi için de aynı olmasını sağladık(**usr/local/etc/openvpn).**

CA(Certificate Authority) Kurulumu ve sunucu/istemciler icin gerekli sertifikalari olusturma

CA bir yetki merkezidir. Sertifika ile güvenliği sağlanmaya çalışılan taraflar için güven onayı veren bir merkezdir. Güvenilir bir CA tarafından imzalanmış sertifika ile yapılan şifreleme işlemlerinin güvenliği sağlanmış olur.

Eğer kullanılan CA herkes tarafından kabul görmemiş ise CA tarafından imzalanan sertifikalar için güvenlikden söz edilemez.

OpenVPN ile birlikte kullanılacak sertifikalar için bir adet CA ihtiyacı vardır. Bu CA'I kendiniz oluşturabileceğiniz gibi, internet üzerinden güvenilirliği kanıtlanmış CA'leri de kullanılabilirsiniz.

Her sunucu istemcisi ikilisi için birer adet public ve private key olusturulur. OpenVPN'nin güzel bir yanı da çift tarafli onaylama desteklemesidir, yani hem kullanici sunucuyu hem de sunucu kullaniciyi denetleyebilir.

Aşağıdaki komutlar kendi CA'nizi oluşturmanıza yardımcı olacaktır.

```
#cd /usr/local/etc/openvpn/easy-rsa/

# . ./vars
NOTE: when you run ./clean-all, I will be doing a rm -rf on
/usr/src/openvpn/openvpn-2.0/easy-rsa/keys
# ./clean-all
#./build-ca
Generating a 1024 bit RSA private key
....++++++
..........++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:TR
State or Province Name (full name) [NA]:
Locality Name (eg, city) [BISHKEK]:KOCAELI
Organization Name (eg, company) [OpenVPN-TEST]:ENDERUNIX
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname)
[]:vpn-gateway
Email Address [me@myhost.mydomain]:huzeyfe@enderunix.org
```

Sunucu için sertifika ve anahtar olusturma

sunucu için sertifika ve gizli anahtar oluşturma

```
#./build-key-server server
Generating a 1024 bit RSA private key
```

```
.....................................................
..++++++
.......++++++
writing new private key to 'server.key'
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a
Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:TR
State or Province Name (full name) [NA]:
Locality Name (eg, city) [BISHKEK]:KOCAELI
Organization Name (eg, company) [OpenVPN-TEST]:ENDERUNIX
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname)
[]:server
Email Address [me@myhost.mydomain]:server@enderunix.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/local/etc/openvpn/easy-
rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TR'
stateOrProvinceName   :PRINTABLE:'NA'
localityName          :PRINTABLE:'KOCAELI'
organizationName      :PRINTABLE:'ENDERUNIX'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'server@enderunix.org'
Certificate is to be certified until Dec 12 19:43:11 2015
GMT (3650 days)
Sign the certificate? [y/n]:y

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

Istemciler için anahtar olusturma

```
#  ./build-key istemci
./build-key istemci
Generating a 1024 bit RSA private key
..........++++++
.....................................................++++
++
writing new private key to 'istemci.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished
Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [KG]:TR
State or Province Name (full name) [NA]:
Locality Name (eg, city) [BISHKEK]:KOCAELI
Organization Name (eg, company) [OpenVPN-TEST]:ENDERUNIX
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:istemci
Email Address [me@myhost.mydomain]:istemci@enderunix.org

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
Using configuration from /usr/local/etc/openvpn/easy-
rsa/openssl.cnf
DEBUG[load_index]: unique_subject = "yes"
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'TR'
stateOrProvinceName   :PRINTABLE:'NA'
localityName          :PRINTABLE:'KOCAELI'
organizationName      :PRINTABLE:'ENDERUNIX'
commonName            :PRINTABLE:'istemci'
emailAddress          :IA5STRING:'istemci@enderunix.org'
Certificate is to be certified until Dec 12 19:45:15 2015 GMT
(3650 days)
Sign the certificate? [y/n]:y


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

NOT: VPN kullanacak her istemci için farklı adlarda istemci

sertifikası oluşturulmalıdır. Oluşturulan bir sertifika tüm VPN kullanıcıları tarafından kullanılabilir fakat böyle bir kullanım güvenlik açısından uygun değildir.

Diffie Hellman parametrelerini olusturma

Diffie Hellman Anahtar Değişimi: İki sistem arasında şifreli haberleşme yapılması için önceden bu sistemler arasında şifrelemeyi sağlayacak bir anahtarın güvenli bir şekilde paylaşılmasını sağlamak üzere geliştirilmiş algoritmadır.

```
# ./build-dh
Generating DH parameters, 1024 bit long safe prime,
generator 2
This is going to take a long time
.....+.+.....+.....
...+
.....+.....+.....
.....
.....
.....
.....+.....+.....
.....
.....+...+.....+.....
.....
.....+...+..+.++*++*++*
```

```
# cd keys/

# ls
01.pem              ca.key              index.txt.attr
laptop.crt          serial              server.csr
02.pem              dh1024.pem          index.txt.attr.old
laptop.csr          serial.old          server.key
ca.crt              index.txt           index.txt.old
laptop.key          server.crt
```

ca.crt sunucu ve tum istemcilerde olmali

ca.key sadece CA makinede olmali
laptop.crt sadece istemci makinede
laptop.key sadece istemci makinede
server.crt sadece sunucu makinede.
server.key sadece sunucu makinede

Olusturulan bu dosyalar gerekli makinelere güvenli yoldan aktarilmalidir.

```
# cp -rp /usr/src/openvpn/openvpn-2.0/easy-rsa/keys/
/usr/local/etc/openvpn/

# cd /usr/src/openvpn/openvpn-2.0/sample-config-files/

# ls
README                  home.up                 office.up
server.conf             tls-home.conf           xinetd-server-
config
client.conf             loopback-client         openvpn-
shutdown.sh     static-home.conf        tls-office.conf
firewall.sh             loopback-server         openvpn-
startup.sh      static-office.conf      xinetd-client-config

# cp * /usr/local/etc/openvpn/

#cd /usr/local/etc/openvpn
```

Buraya kadarki adımlarla kurulum sürecini tamamladık. Şimdi de OpenVPN'in çalışma yapısına gözatarak nasıl yapılandırılacağınagözatalım.

OpenVPN Çalışma Modları

OpenVPN iki farkli modda çalışabilir. Bridge mod ve route mod. Gereksiniminize gore bu iki çalışma yönteminden birini kullanabilirsiniz.

Bridge Mode Çlışma Yapısı

Bridge mod, WAN üzerinde bir ethernet LAN'I oluşturmak için kullanılır. Yani birbirinden farklı lokasyonlardaki makineleri, ağları tek bir ethernet ağındaymış gibi haberleştirebilirsiniz. Bridge mode daha çok özel gereksinimler için tercih edilmektedir. Mesela broadcast paketler aracılığı ile haberleşen bir uygulamanız varsa bridge mod kullanmanız kazçınılmazdır. Bridge modda tap sahte arabirimleri kullanılır.

Route Mod Çalışma Yapısı

Routing mod biraz daha rahattır ve özel bir gereksinim olmadığı müddetçe(IPX gibi IP tabanlı olmayan protokollerin kullanımı gerektiğinde) routing mod kullanımı tavsiye edilmektedir. Route modda tun sahte arabirimleri kullanılır.

Sunucu Tarafı Yapılandırma Dosyası – server.conf

OpenVPN çalışma parametrelerini komut satırından alabileceği gibi bir dosyaya düzenli bir şekilde yazarak bu dosyadan da okuma yapabilir. Tercih edilen yöntem, tüm yapılandırma parametrelerini bir dosyaya(server.conf) yazarak bu dosyadan okutmaktır.

Öntanımlı olarak bu dosya server.conf'tur. Server.conf dosyasında sık kullanılan bazı parametreler ve anlamları;

NOT: server.conf dosyasında # ya da ; ile başlayan satırlaryorum satırı olarak algılanır ve herhangi bir etkisi yoktur. Bir parametrenin önündeki ;, # işaretlerini kaldırarak o parametreyi aktif hale getirmiş oluruz.

VPN Sunucu hani IP üzerinden çalışsın?

local a.b.c.d

a.b.c.d ile belirtilen IP adresi üzerinden çalışacağını belirtir. Sunucumuzda birden fazla IP adresi varsa bu adresler arasında seçim şansı verir.

VPN sunucu Portu

port 1194

VPN sunucunun hangi port üzerinden çalışacağını belirtir. Aynı makine üzerinde birden fazla OpenVPN çalıştırılacaksa bu parametre her yapılandırma dosyası için farklı olmalıdır.

proto udp

Hangi protokolün kullanılacağını belirtir. Varsayılan ve tavsiye edilen değeri UDP'dir.

Route mod mu Bridge mod mu?

;dev tap0
dev tun0

Layer 2 VPN kullanmayı düşünüyorsanız bu değer tap olmalıdır. Eğer OpenVPN'i route modda kullanmak isterseniz tun arabirimi kullanılmalıdır.

NOT: TAP, Tun Arabirimleri;
Tun Arabirimi: Sanal bir ağ bağdaştırıcısıdır. Üzerinde çalıştığı makine için bir PPTP arabirimden farksızdır. Programcı tun arabirimini herhangi bir dosya gibi kullanarak istediği bilgileri okur ve yazar. Tap arabirimi de Tun'e benzer fakat sadece ethernet arabirimleri simüle edebilir.

ca /usr/local/etc/openvpn/certs/ca.crt

CA Sunucunun sertifikası. Burada tam yol belirtilmelidir. Bu sertifika tüm sunucu ve istemcilerde bulunmak zorundadır.

cert /usr/local/etc/openvpn/certs/server.crt

VPN sunucunun sertifikası. Sadece sunucu tarafında bulunmalıdır.

key /usr/local/etc/openvpn/certs/server.key

bu dosya çok önemlidir. Diğer tüm sertifikaları imzalamada kullanılır.

dh /usr/local/etc/openvpn/certs/dh1024.pem

Diffie hellman parametrelerinin bulunduğu dosya

VPN İstemcileri Ağ Yapılandırması

server 10.8.0.0 255.255.255.0

VPN sunucuya bağlanarak IP alacak istemcilerin IP havuzunu belirler. Havuz içinde ilk IP adresi VPN sunucunun IP adresi olacaktır.

ifconfig-pool-persist ipler.txt

VPN sunucuya bağlanarak IP adresi alan istemcilerin kayıtlarını tutar. VPN sunucuda yaşanacak bir bağlantı kopması sonrasında istemcilerin eski IP adreslerini almalarını sağlar.

;push "route 192.168.20.0 255.255.255.0"

VPN ile bağlanan istemcileri VPN sunucu arkasındaki başka ağlara da erişim izni için yönlendirme tanımı.

Istemciye Özel IP atama

Bazı istemcilerinize özel ip ataması yapmak isterseniz istemcilerin sertifikalarında kullandıklar CN tanımına göre özel ip atamaası yapabilirsiniz.

Örnek;

Sertifikasında CN'si enderunix olan istemciye **10.9.0.1** ip'sinin atanmasını istiyoruz.

client-config-dir *ozel*

route 10.9.0.0 255.255.255.252

/usr/local/erc/openvpn/ozel dizinini oluşturarak içine enderunix adlı bir dosya açılır ve bu dosyaya aşağıdaki satır eklenir.

ifconfig-push 10.9.0.1 10.9.0.2

VPN Kullanıcının Tü mnTrafiğini Yönlendirmek

push "redirect-gateway"

VPN sunucuya bağlanan istemcilerin varsayılan geçit yolunu(default gateway) VPN sunucu olarak ayarla manasıan gelir. Böylece istemcinin özel olarak yönlendirilmemiş tüm trafiği VPN gateway aracılığı ile çıkacaktır. Burada istemcileri internete çıkarmak için VPN sunucu makinesinde NAT yapılması da gerekir. Linux, FreeBSD ve OpenBSD işletim sistemlerinde NAT işleminin nasıl yapıldığı öğrenilmelidir.

OpenBSD PF için nat tanımı:

```
ext_if=”fxp0”
VPN_AGI=”100.100.100.0/24”
nat on $ext_if from VPN_AGI -> ($ext_if)
```

VPN istemcilerinin birbirini görmesi

OpenVPN varsayılan yapılandırımı ile VPN istemcileri sadece VPN sunucuyu görecektir. Birbirlerini görebilmeleri için

;client-to-client

Tanımı girilmelidir. Istemcilerin sadece VPN sunucuyu görmelerini kesin olarak sağlamak için VPN sunucu üzerindeki Güvenlik duvarı uygun şekilde yapılandırılmalıdır.

Aynı sertifika ile birden fazla İstemci

Aynı sertifika ile birden fazla istemcinin VPN yapabilmeleri için

duplicate-cn

tanımı kullanılmalıdır. Aksi takdirde VPN ağına bağlanan her istemci aynı IP adresini alacaktır. Biraz karışık bir özellik ve sadece test amaçlı kullanılması öneriliyor.

keepalive 10 120

Sunucu ve istemcilerin birbirinin durumundan haberdar olmalarını sağlayan bir yapı. Anlamı her 10 saniyede bir kontrol et, 120sn içerisinde cevap gelmezse bağlantıyı kopar.

VPN Hattında Sıkıştırma

comp-lzo

kullanılır. Bu tanım hem sunucuda hem de istemcide kullanılmalıdır.

Eşzamanlı VPN Kullanıcısı

max-clients 100

eşzamanlı 100 kullanıcıya izin ver.

OpenVPN durum Kontrolü

status openvpn-status.log

tanımı ile yapılır. VPN sunucunun durumu hakkında özet bilgi için.

Loglama

log /var/log/openvpn.log

log-append /var/log/openvpn.log

verb 3

 # 0 is silent, except for fatal errors
 # 4 is reasonable for general usage
 # 5 and 6 can help to debug connection problems
 # 9 is extremely verbose

VPN sunucu başlatma ve çalışma zamanı için loglarını atacağı dosya. VPN sunucuda problem yaşandığında ilk bakılması gereken dosyadır.

NOT: Tüm geçerli parametreler için örnek server.conf dosyasının incelenmesi faydalı olabilir.

Örnek Yapılandırma Dosyaları

Aşağıdaki istemci ve sunucu yapılandırma dosyaları temel bir VPN ağı oluşturmak için gerekli yapılandırmaları içermektedir. Kendi ihtiyacınıza göre bu değerlerle oynayabilirsiniz.

Örnek istemci dosyası

```
-- -- -- -- -- -- -- -- -- -- --
client
dev tun0
proto udp
remote 194.27.72.88 1194
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert istemci.crt
key istemci.key
ns-cert-type server
comp-lzo
verb 3
-- -- -- -- -- -- -- -- -- -- --
```

Örnek sunucu konfigürasyonu

-- -- -- -- -- -- -- -- -- -- --

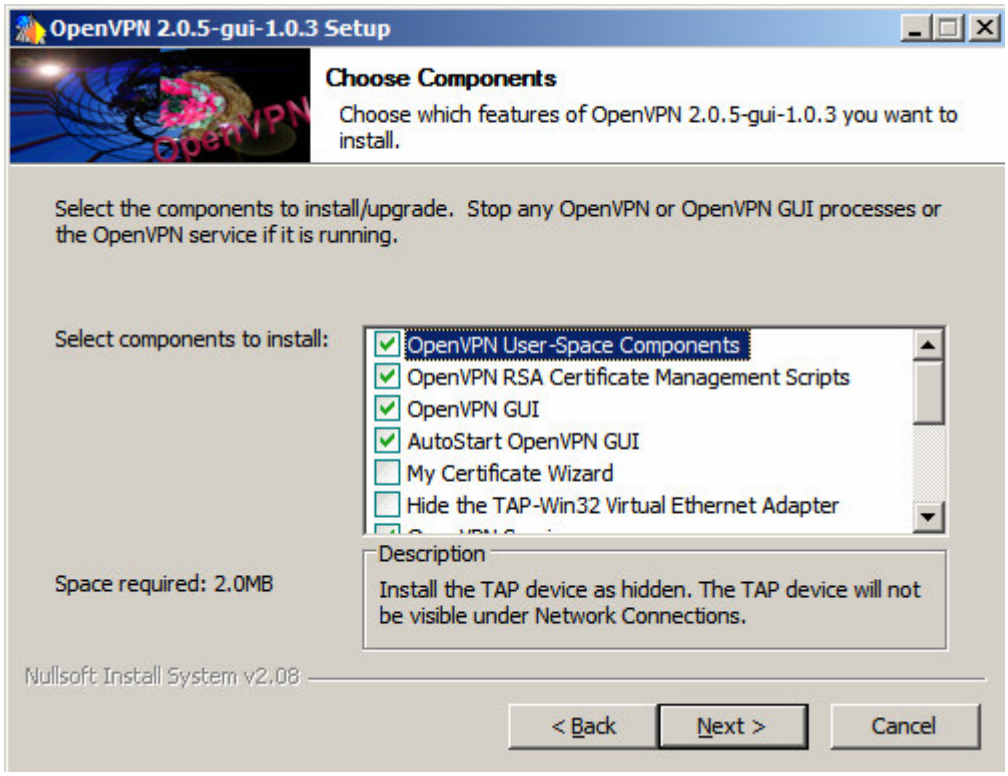
```
local 14.2.2.8
port 1194
proto udp
dev tun0
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/sunucu.crt
dh easy-rsa/keys/dh1024.pem
server 100.100.100.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway"
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log         /var/log/openvpn.log
verb 6
```

-- -- -- -- -- -- -- -- -- -- --

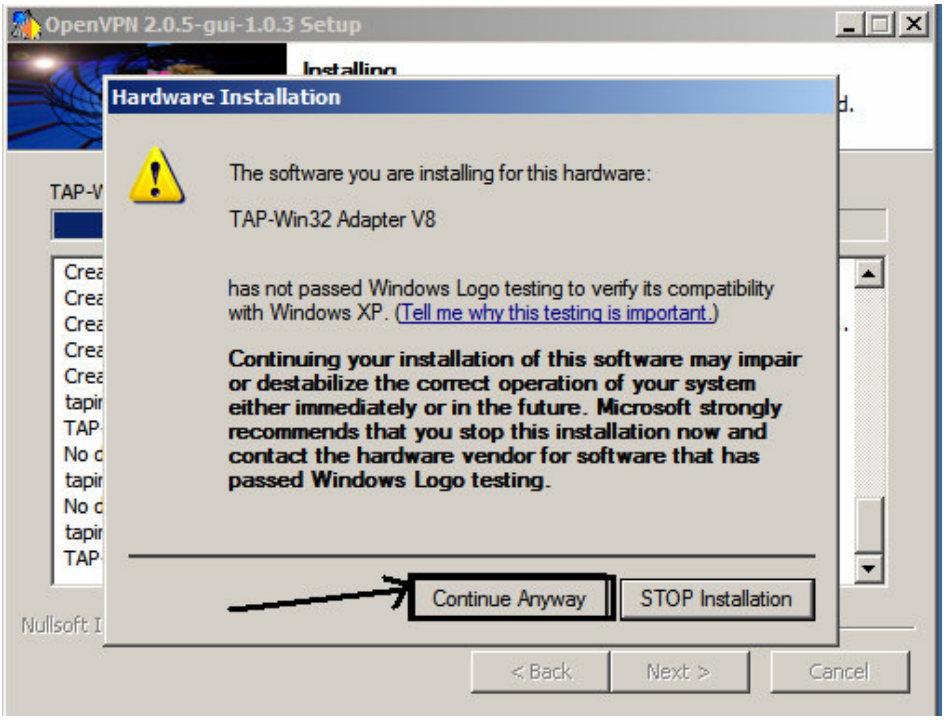
Windows XP OpenVPN istemci Kurulumu

http://openvpn.se/download.html adresinden son sürüm "stable" OpenVPN-gui paketini indirerek işleme başlayalım.

Yazı hazırlarken son sürüm openvpn-gui: *openvpn-2.0.5-gui-1.0.3-install.exe*



Şekil-3



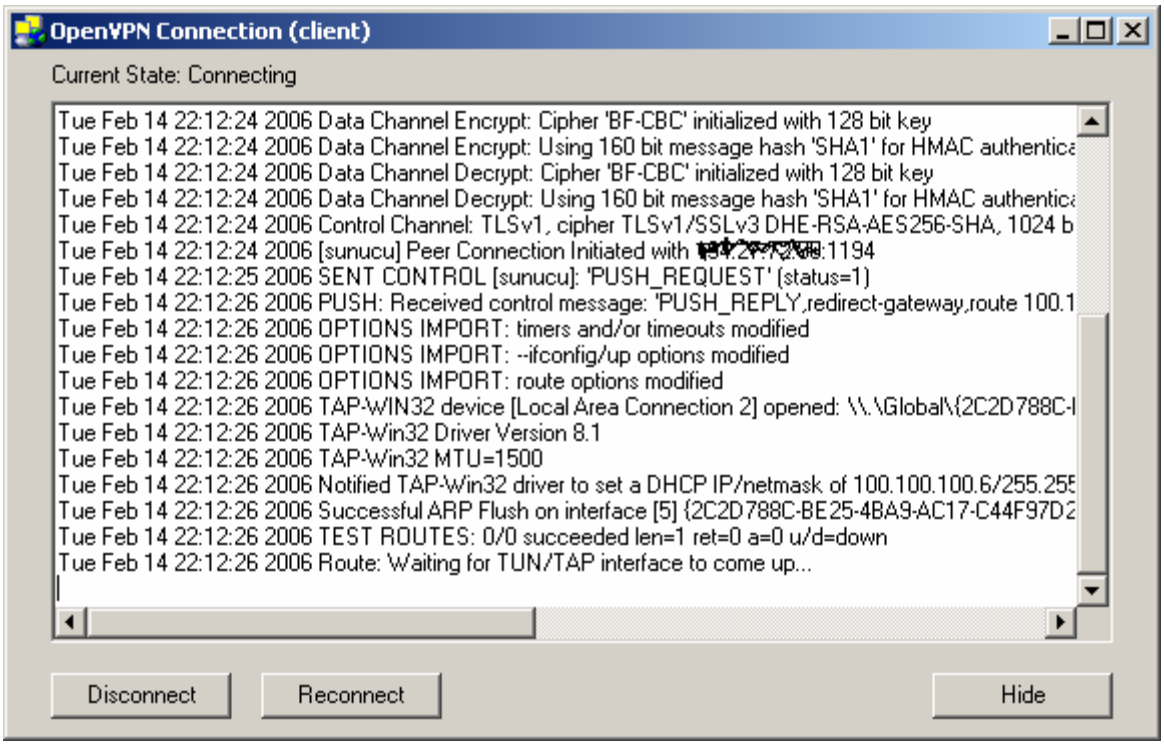
Şekil-4

Kurulum adımları tamamlandıktan sunucu tarafında oluşturduğumuz istemci sertifikalarını **C:\Program Files\OpenVPN\config** dizini altına kopyalayarak istemci tarafı VPN yapılandırma dosyasını uygun şekilde düzenleyelim.

Laptop.ovpn adlı bir dosya oluşturarak içine örnek istemci dosyasındaki gibi değerleri yazarak VPN bağlantısını başlatabilirsiniz.

Şekil-5

Bağlantı kurulumu esnasında aşağıdaki ekrana benzer bir pencere açılarak bağlantı durumunu gösterecektir.



Şekil-6

Kaynaklar

[ref 1] "Implementing OpenVPN". Florin Andresi. Mar 26 2004
http://fedoranews.org/contributors/florin_andrei/openvpn/

[ref 2] OpenVPN Articles.
http://openvpn.net/articles.html

[ref 3] "Sanal Özel Ağ, Kriptoloji ve PKI Teknolojileri". Serkan YILMAZ.
http://penguence.linux.org.tr/?~p=dergi&action=show&which=7
7
[ref 4] "AçıkKod VPN Çözümleri". Huzeyfe ÖNAL.
http://www.enderunix.org/slides/Internet%20Konferanslari/ac
ikkodvpn.pdf

[ref 5] "OpenVPN Howto".
http://openvpn.net/howto.html