



Açık Kod VPN Çözümleri: OpenVPN

Huzeyfe ÖNAL
huzeyfe@enderunix.org
EnderUNIX Yazılım Geliştirme Ekibi



Sunum Planı

- VPN Tanımı
- VPN Çeşitleri
 - VPN terimleri
 - VPN Teknolojileri
- AçıkKod VPN Projeleri
- OpenSSH ile VPN Çözümü
- OpenVPN Kurulumu
- OpenVPN Yapılandırması
- OpenVPN Yönetim Araçları

VPN Nedir?

- VPN, public ağlar üzerinden güvenli haberleşme amaçlı geliştirilmiş bir teknoloji çeşididir
- VPN Öncesi/harici güvenli haberleşme nasıl sağlanıyordu??
- VPN Ne sağlar.
 - Maliyetten kazanç
 - Güvenlik
- 1995 yılında ilk standart VPN çözümü :
Ipsec

VPN Ne Sağlar?

- Gezgin kurum çalışanlarını şirket ağına güvenli ve ekonomik ulaştırma
- Kurumlar arası güvenli iletişim
 - Kurum-banka , Kurum bayiler gibi
- Dağınık kurumlar için merkezi yapı
 - İzmir bölgesi, Atina bölgesi, Usa bölgesi...
- Bireysel kullanıcılar arasında güvenli iletişim
- Wireless ağlarda güvenlik

VPN Çeşitleri

- Remote Access

- Gezgin kullanıcıların şirket ağına bağlanması için
- VPDN(**virtual private dial-up network (VPDN)**) olarak da adlandırılır

- Site to Site

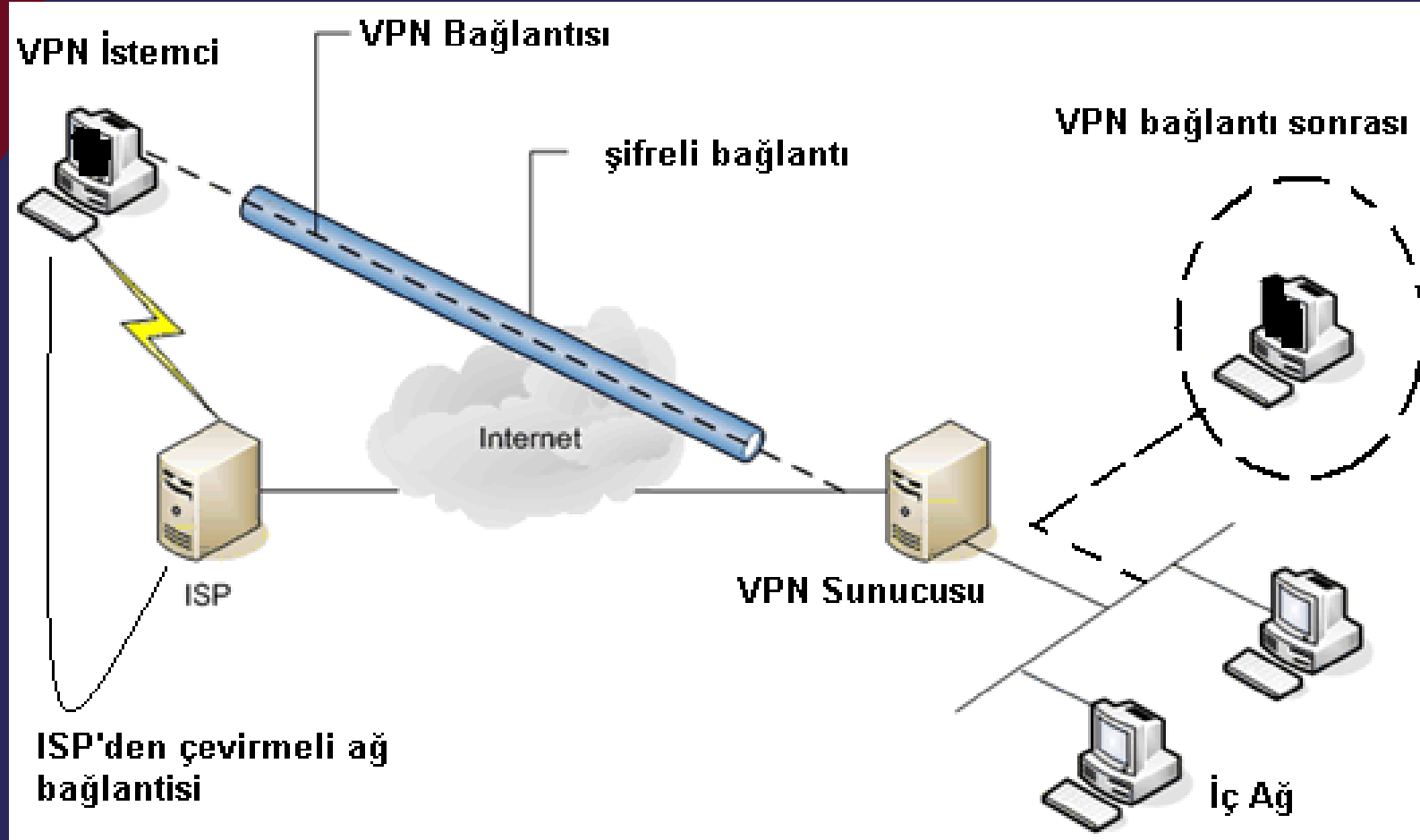
- Intranet tabanlı
- Extranet tabanlı

- Client to client

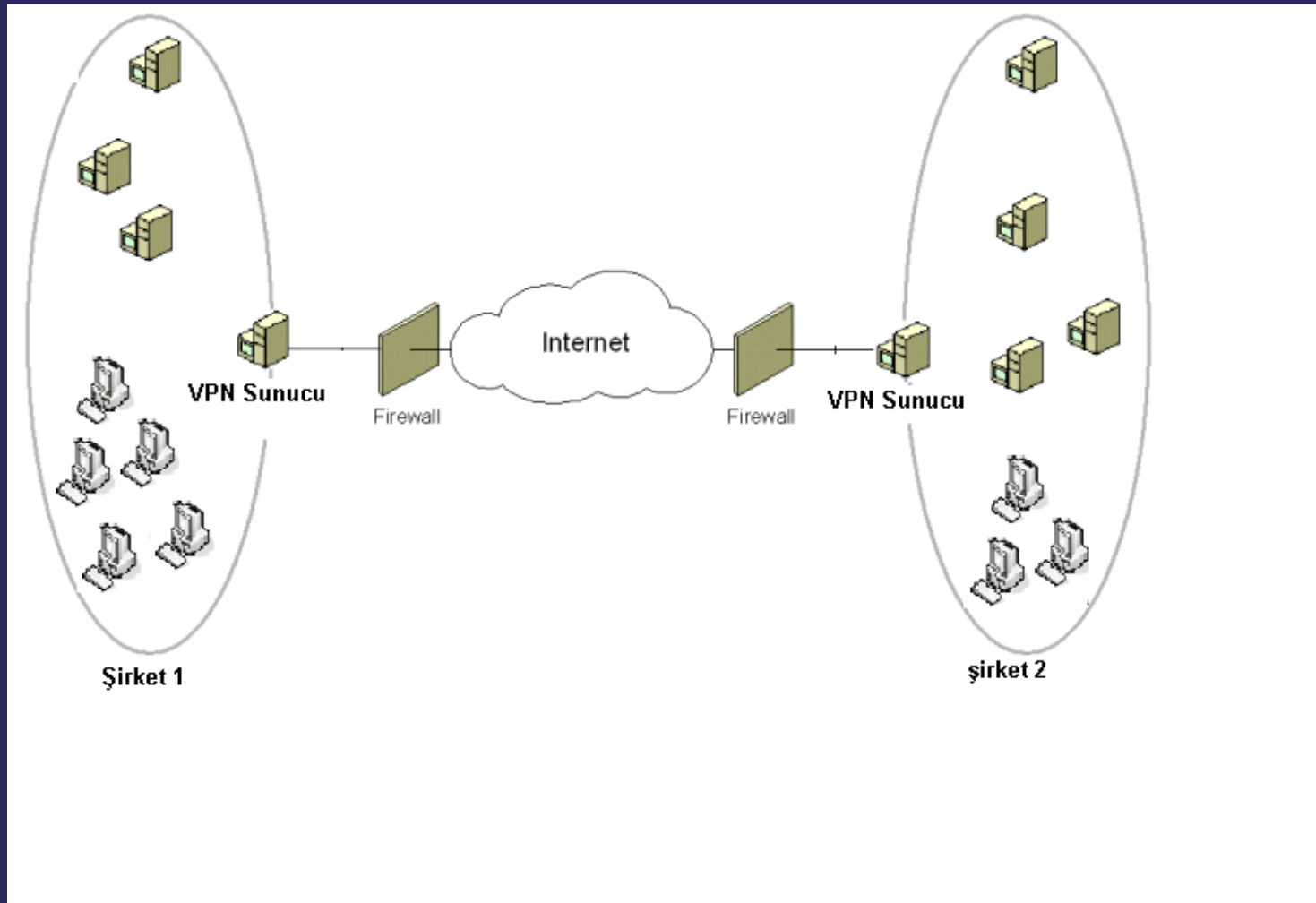
- Günümüz popüler VPN Protokolleri

- Ipsec VPN, PPTP, L2TP, SSH, SSL VPN

Remote Access VPN..



Site-toSite VPN..





Açık Kod VPN Çözümleri..

- PPTP Çözümü: PopTop
- L2TP Çözümü: OpenL2tp
- SSH ile VPN
- SSL VPN: SSLExplorer, OpenVPN
- Ipsec VPN: OpenBSD Ipsec, OpenSwan

OpenSSH ile Gerçek VPN Çözümü!

- OpenSSH 4.3 ve sonrası tun(4)
- Layer 2 ve Layer 3 VPN imkanı
- TCP üzerinden çalışır (-)
- Sunucu tarafı(sshd_config)
 - PermitTunnel yes
- VPN için kullanıcı kısıtlama
 - Authorized_keys kullanılır
 - tunnel="1",command="sh /etc/netstart tun1" ssh-rsa ... huzeyfe@enderunix.org

OpenSSH ile Gerçek VPN Çözümü-II

- İstemci tarafı basit yapılandırma..
- /etc/hostname.tun0
 - inet 192.168.5.1 255.255.255.252
192.168.5.2
 - inet 192.168.1.78 255.255.255.0
192.168.1.255 link0 /Layer 2 VPN...
 - Host **ssh.enderunix.org**
Tunnel yes
TunnelDevice 0:any
PermitLocalCommand yes
LocalCommand sh /etc/netstart tun0
 - ssh **ssh.enderunix.org**

OpenVPN Nedir?

- OpenVPN, multi platform bir SSL VPN çözümüdür
 - !!!SSL VPN kavramı..!!!
 - Linux, Windows 2000/XP ve üzeri, OpenBSD, FreeBSD, NetBSD, Mac OS X ve Solaris
- OpenSSL kütüphanesinin sunduğu encryption, authentication, ve certification özelliklerinin sağladığı herşey..
- User-space bir çözüm..IPsec gibi çekirdekte değişiklik istemiyor
- Site to site, Remote Access, Wifi Security Çözümleri
- Tek port(TCP/UDP) üzerinden VPN Kurulumu
- Eş zamanlı sınırsız(?) VPN desteği



OpenVPN Özellikleri

- Layer 2 ve Layer 3 VPN imkanı
 - Bridge mode, routing mode
- Tun, tap sahte arabirim kullanımı
- Statik, pre-shared, ve dinamik anahtar değişimi destekli
- NAT arkasından problemsiz kullanım imkanı
- İsteğe bağlı olarak GUI aracılığı ile yönetim

Routed Mode

- Standart , önerilen çözüm
- Kararlı ve verimli çalışma
- Muhtemel topolojiler
 - Network - Network
 - Network - Host
 - Host - Network
 - Host - Host
- Tun arabirimi kullanılır

Bridge Mode

- WAN üzerinde bir ethernet LAN'I oluşturmak için kullanılır.
- Layer 2 bridge vazifesi görür
- Broadcast vs gerektiren özel uygulamalar için...(DHCP, Samba, IPX)
- Tap arabirimi kullanılır
- Brctl ile çeşitli kısıtlamalar yapılabilir.

OpenVPN Kurulum

○ Gereksinimler

- OpenSSL kütüphanesi
- LZO (real-time compression library)
- Pthread library

○ Genel Kurulum

`./configure && make && make install`
`(./configure --help)`

○ BSD'ler için port sistemi

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

○ Windows için "Next, Next, Stop!" Kurulum adımları

OpenVPN Temel Yapılandırma

- **CA(Certificate Authority) Kurulumu**
 - `# cd /usr/src/openvpn/openvpn-2.0/easy-rsa`
 - `# . ./vars`
 - `# ./clean-all`
 - `# ./build-ca`
- **Sunucu Sertifikası oluşturma**
`# ./build-key-server server`
- **Istemciler için anahtar oluşturma**
`# ./build-key laptop`
- **Diffie Hellman parametrelerini oluşturma**
`# ./build-dh`
- **Oluşan sertifika dosyaları;**
 - **ca.crt** Root sertifikası sunucu ve tüm istemcilerde olmalı
 - **ca.key** sadece CA makinede olmalı
 - **laptop.crt** sadece istemci makinede
 - **laptop.key** sadece istemci makinede /gizli
 - **server.crt** sadece sunucu makinede.
 - **server.key** sadece sunucu makinede /gizli
- **openvpn [server config file]**

OpenVPN Yapılandırma(sunucu)-I

- **Hangi IP adresini dinlesin**
local 212.123.34.56
- **Hangi Port üzerinden çalışsın**
port 1194
proto udp , proto tcp
- **Bridge mode mu Tunneling mode mu**
dev tap
dev tun
- **IP Pool**
server 10.10.10.0 255.255.255.0
- **ifconfig-pool-persist ipp.txt**
 - Openvpn yeniden başladığında istemcilerde ip adresi değişikliği yaşanmasın
- **Max. İstemci sayısı**
max-clients 100

OpenVPN Yapılandırma(sunucu)-II

- **VPN İstemcileri Ağ Yapılandırması**
 - `server 10.8.0.0 255.255.255.0`
- **Özel yönlendirme tanımlama**
 - `push "route 192.168.20.0 255.255.255.0"`
- **VPN Kullanıcının Tüm Trafiğini Yönlendirmek**
 - `push "redirect-gateway"`
- **Aynı sertifika ile birden fazla İstemci**
 - `duplicate-cn`
- **Loglama**
 - `log /var/log/openvpn.log`

İstemci Tarafı Yapılandırma

- VPN Sunucu

- remote 194.27.72.88 1194
- Route mod? Bridge mode seçimi?
 - dev tun0
- Sıkıştırma
 - comp-lzo

Örnek Yapılandırma Dosyası- Sunucu

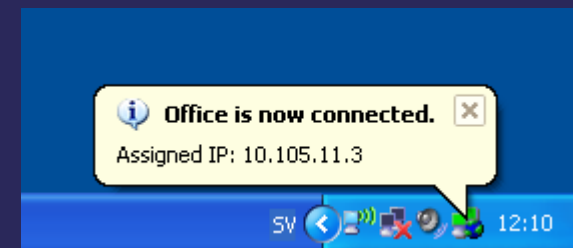
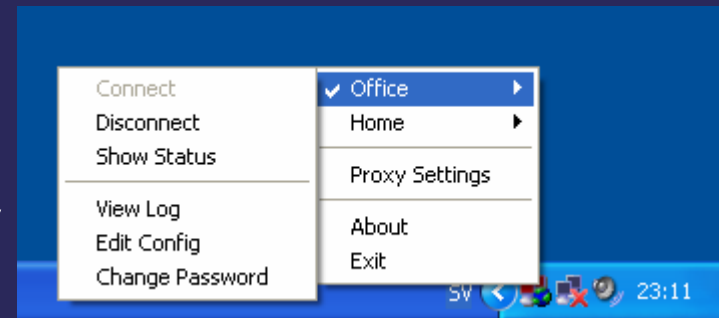
```
local 14.2.2.8
port 1194
proto udp
dev tun0
ca easy-rsa/keys/ca.crt
cert easy-rsa/keys/sunucu.crt
dh easy-rsa/keys/dh1024.pem
server 100.100.100.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "redirect-gateway"
keepalive 10 120
comp-lzo
persist-key
persist-tun
status openvpn-status.log
log /var/log/openvpn.log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

Örnek Yapılandırma Dosyası- İstemci

```
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
```

OpenVPN GUI (windows)

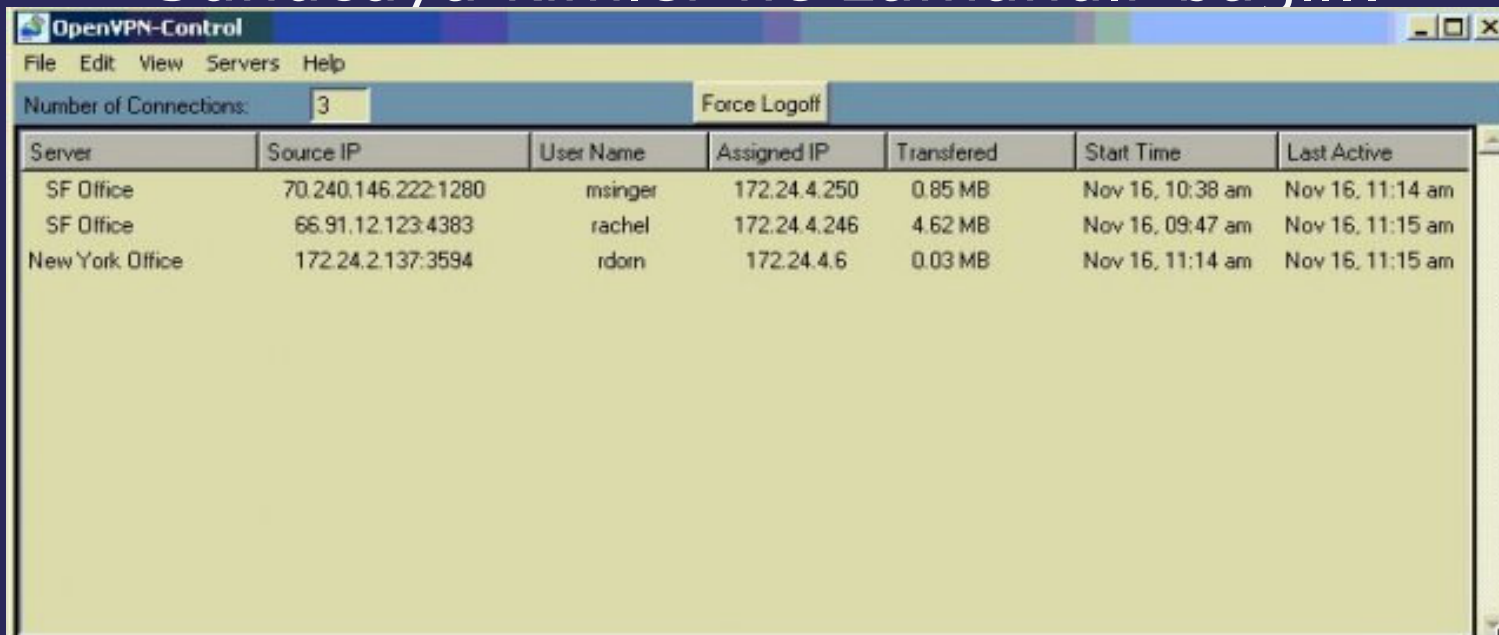
- GPL Lisanslı ile özgür kullanım
- VPN yönetimi(start/stop/restart/
- Log izleme
- Proxy ayarları yapma imkanı
- Config dosyasını düzenleme seçeneği
- <http://openvpn.se/>



OpenVPN Araçları

○ OpenVPN Control

- Multiplatform Openvpn sunucu kontrolü
- Sunucuya kimler ne zamandır bağlı..



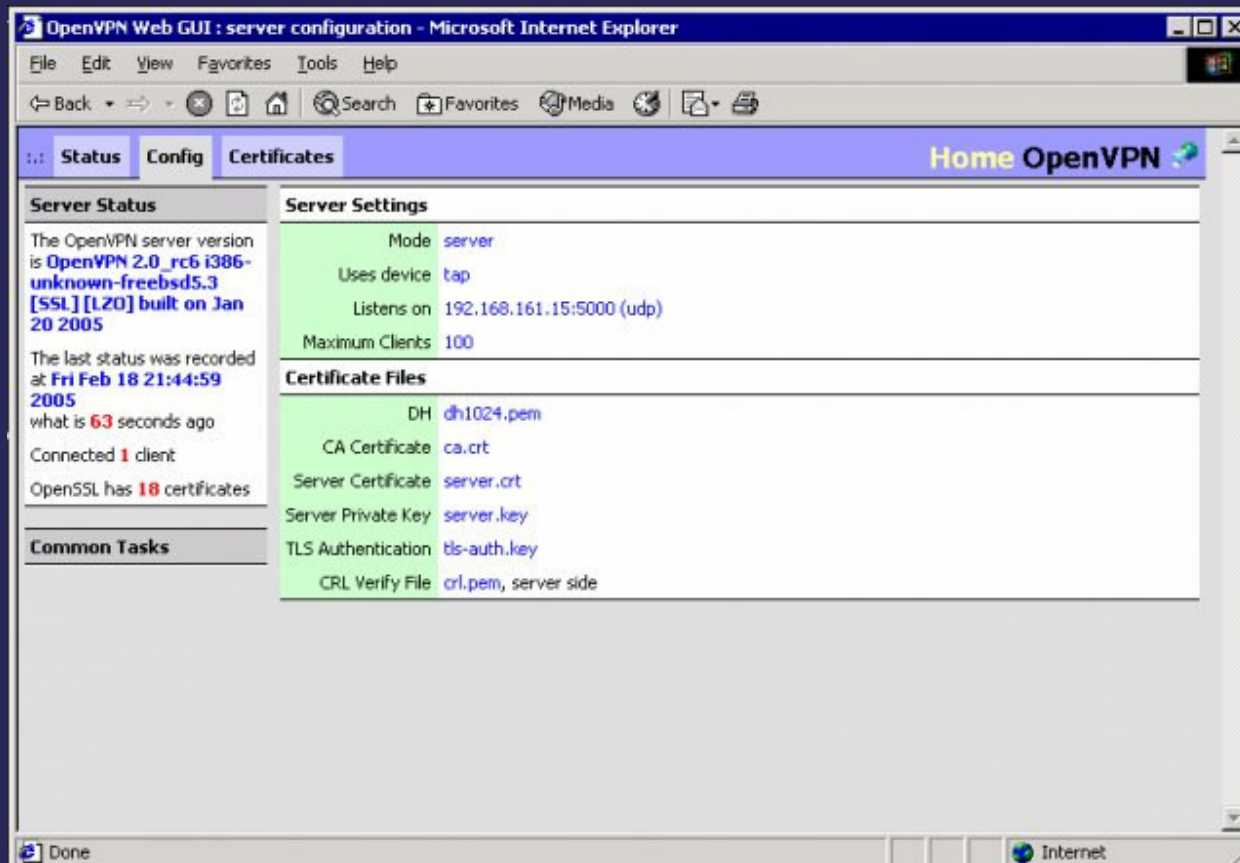
The screenshot shows the OpenVPN-Control web interface. At the top, there's a menu bar with 'File', 'Edit', 'View', 'Servers', and 'Help'. Below the menu, there's a status bar showing 'Number of Connections: 3' and a 'Force Logoff' button. The main content area is a table with the following columns: Server, Source IP, User Name, Assigned IP, Transferred, Start Time, and Last Active. The table contains three rows of data representing active connections.

Server	Source IP	User Name	Assigned IP	Transferred	Start Time	Last Active
SF Office	70.240.146.222:1280	msinger	172.24.4.250	0.85 MB	Nov 16, 10:38 am	Nov 16, 11:14 am
SF Office	66.91.12.123:4383	rachel	172.24.4.246	4.62 MB	Nov 16, 09:47 am	Nov 16, 11:15 am
New York Office	172.24.2.137:3594	rdorn	172.24.4.6	0.03 MB	Nov 16, 11:14 am	Nov 16, 11:15 am

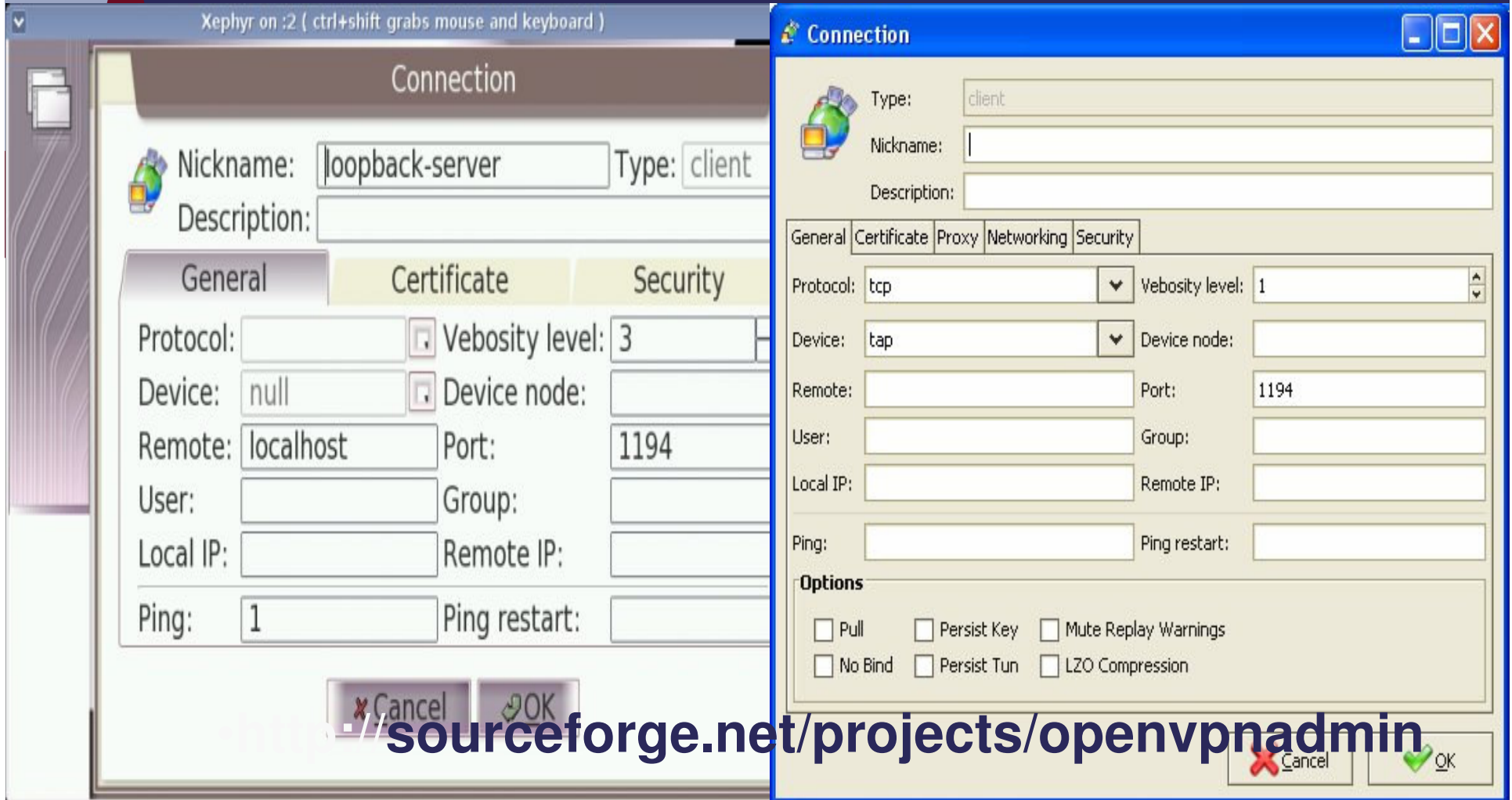
• <http://sourceforge.net/projects/openvpn-control>

OpenVPN Web GUI

- Php5 ile yazılmış yönetim arabirimi
- <http://sourceforge.net/projects/openvpn-web-gui>



OpenVPN Araçları





Teşekkürler...