

Huzeyfe ÖNAL

AçıkKod VPN Çözümleri

huzeyfe@EnderUNIX.org

EnderUNIX Yazılım Geliştirme Ekibi

Sunum Planı

- VPN Tanımı
- VPN Çeşitleri
 - Vpn terimleri
 - VPN Teknolojileri
- AçıkKod VPN Projeleri
- OpenVPN Kurulum ve Yönetimi
- VPN Çözümleri Karşılaştırma

VPN Nedir?

- VPN, internet üzerinden güvenli haberleşme amaçlı geliştirilmiş bir teknoloji
- 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

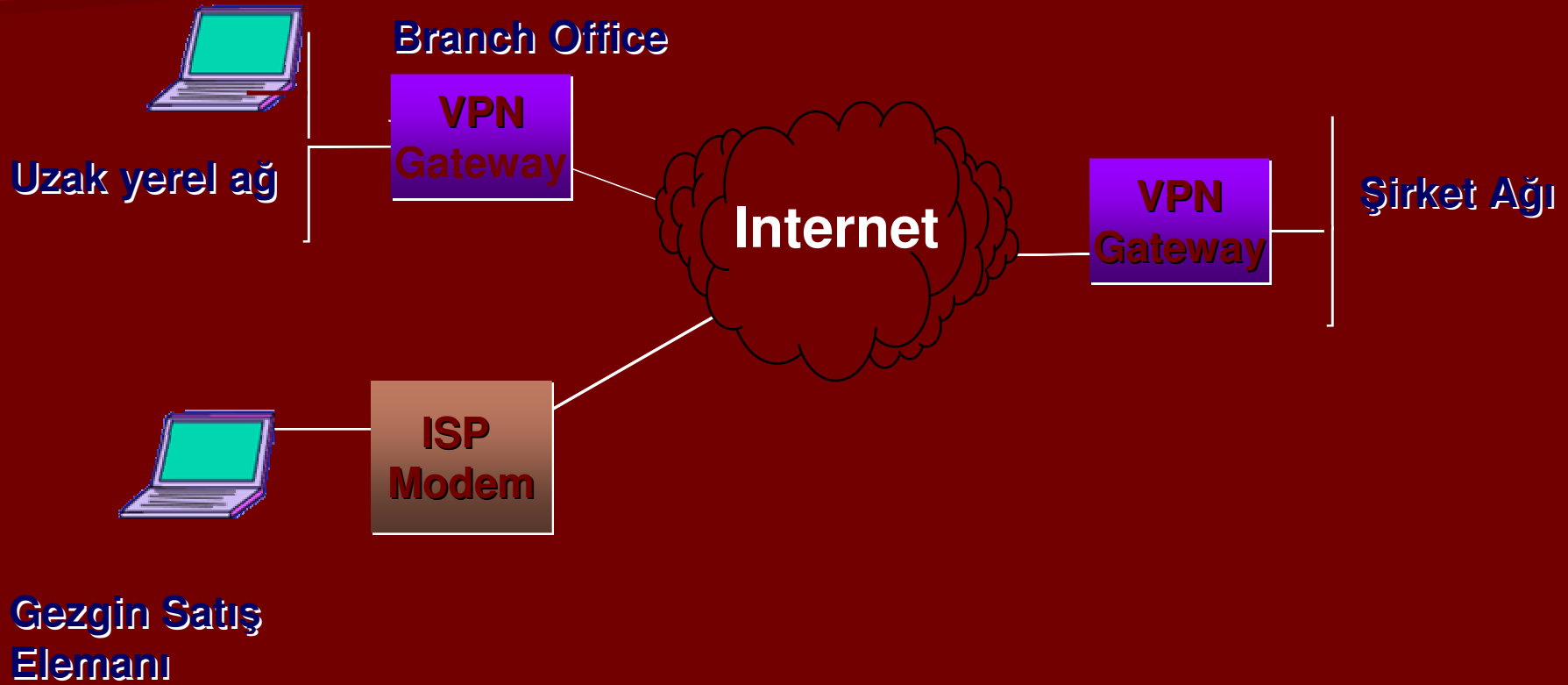
- Intranet tabanlı
- Extranet tabanlı

■ Client to client

■ Günümüz popüler VPN Protokolleri

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

VPN Gösterimi



PPTP VPN Çözümü

- PPTP(Point to Point Tunneling Protocol) uçtan uca tünelleme/şifreleme sunar
- PPTP Forum(Microsoft, 3COM, Ascend) tarafından
- MPPE 40 bit ve 128 RC4 bit şifreleme desteği, PPP destekli Kimlik doğrulama ..
- NETBEUI and IPX/SPX gibi IP tabanlı olmayan protokolleri de destekler..
- Kolay kurulum ve yönetim avantajı
 - Win95 sonrasında işletim sistemi ile birlikte geliyor
 - Linux için pptpclient.sf.net
- Güvenlik sorunsalı
- PopTop yazarları PPTP yerine OpenVPN ya da Ipsec kullanimini tavsiye etmektedir.
 - <http://poptop.sourceforge.net/dox/protocol-security.phtml>
- MS-CHAPv2 ile aktif ataklara çözüm getirildi fakat hala offline brute force karşı zayıf

PopTop



- GPL Lisanslı özgür bir PPTP Çözümü
- Linux, BSD, Solaris destekli
- PPTP'yi etkileyen güvenlik açıklarını barındırıyor
 - Windows istemcilerle uyumlu olabilmek için
- Kolay kurulum basit yönetim
- Eşzamanlı birden fazla kullanıcı desteği
- Radius eklentisi ile samba ve ldap üzerinden kimlik doğrulama yapabilir.
- www.poptop.org

L2TP

- L2TP(Layer 2 Tunneling Protocol)uçtan uca tünelleme protokolü
- IETF tarafından tasarlanmıştır
- Cisco'nun Layer 2 Forwarding (L2F) ve Microsoft'un Point-to-Point Tunneling Protocol (PPTP) protokollerinin iyi yönleri..
- Ipsec ile şifrelenerek geçerli bir VPN Çözümü olabilir
- Özgür L2TP Çözümü
 - OpenL2TP (<http://opensource.katalix.com/openl2tp/>)

SSH ile VPN

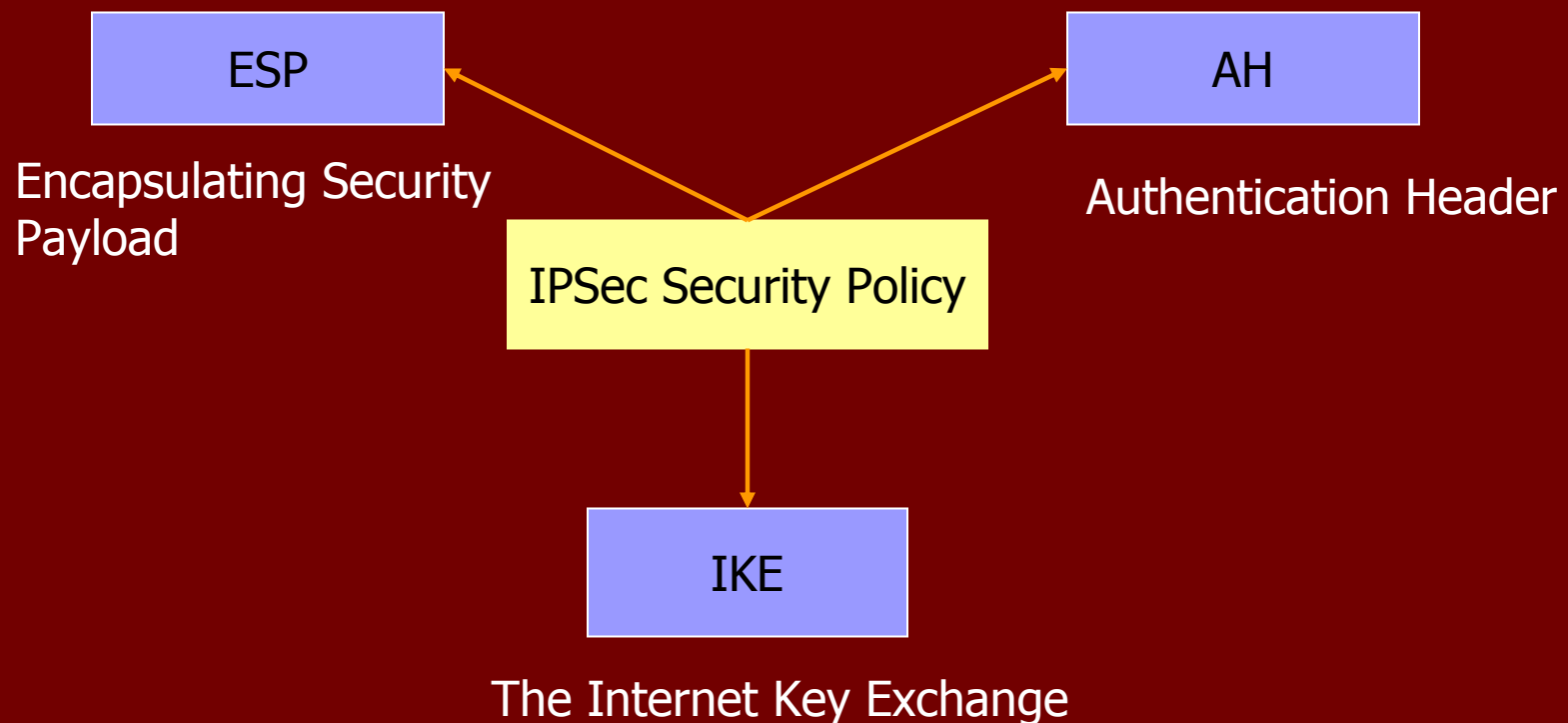
- SSH(Secure SHell), temel amacı ağ üzerinden güvenli iletişim sağlamak
 - authentication (Kimlik denetimi), (encryption /Şifreleme), (Integrity /Bütünlük.)
- Uzak sistemlerde komut çalıştırmak, dosya transferi yapmak amaçlı kullanılabilir
 - Scp, sftp.. (Winscp, Windows tarafında)
- Port Forwarding ile VPN işlevi
- Yerel Yönlendirme(local forwarding)
`$ssh -L5000:localhost:110 mail_sunucu(POP)`
- Uzak Yönlendirme(Remote Forwarding)
`#ssh -R5000:localhost:22 istemci_makine`
 - `telnet localhost 5000(istemci makinede)...ssh ☺`
- Dynamic Port Forwarding
`$ssh -D 8080 ssh.enderunix.org (Socks proxy)`

Ipsec

- Kullanılan IP protokolü güvensizdir!
 - Günümüz düşünülerek tasarlanmamış
 - İş halletme amaçlı, küçük ağlar için düşünülmüş
 - Ip spoofing ve veri içeriği korumada etkisiz
- Güvenli iletişim için SSL/TLS bir çözümdür fakat aplikasyon seviyesinde çalışır..
- Ipsec ise network seviyesinde şifreleme yapar ..

Ipsec ..

- IP'ye ek güvenlik özellikleri katar
 - Gelen bilginin doğru kişiden geldiğini onaylar
 - Gelen paket için güvenlik ve bütünlük sağlar



AH & ESP

■ AH

- Veri bütünlüğü, kaynak ip doğrulama
- Veri güvenliği yok!
- Paketin IP başlığını da doğrular(Src/Dst IP)

■ ESP

- AH'nin sağladığı herşey
- Ek olarak şifreleme
- Paketin payload kismini doğrular

■ Ipcomp

- Ip datagram boyutunu azaltmak için
- Sıkıştırma amaçlı...

Ipsec Yapısı

- 2 farklı modda çalışabilir
 - Transport Mode (host-to-host)
 - Tunnel Mode (gw-to-gw)

Original

IP header TCP header data

Transport
mode

IP header **IPSec header** TCP header data

Tunnel
mode

IP header IPSec header **IP header** TCP header data

Ipsec VPN

- İlk standart VPN Çözümü..
- Kullanımı zor, tam olarak bitmemiş
- Özgür Ipsec çözümleri
 - Linux FreeSWAN/OpenSWAN
 - OpenBSD Ipsec altyapısı
 - OpenBSD 3.8 ile birlikte PF benzeri ipsec yapılandırma

flow esp out from 192.168.3.14 to 192.168.3.100

SSL VPN

- Yeni nesil VPN Çözümü
- İstemci tarafında ek bir program gerektirmez
- <https://ssl-vpn.gateway>
- Genellikle Java tabanlı çözümler..
- Özgür SSL VPN Çözümü:SSLExplorer
- Browser tabanlı olmayan SSL VPN Çözümleri
- OpenVPN

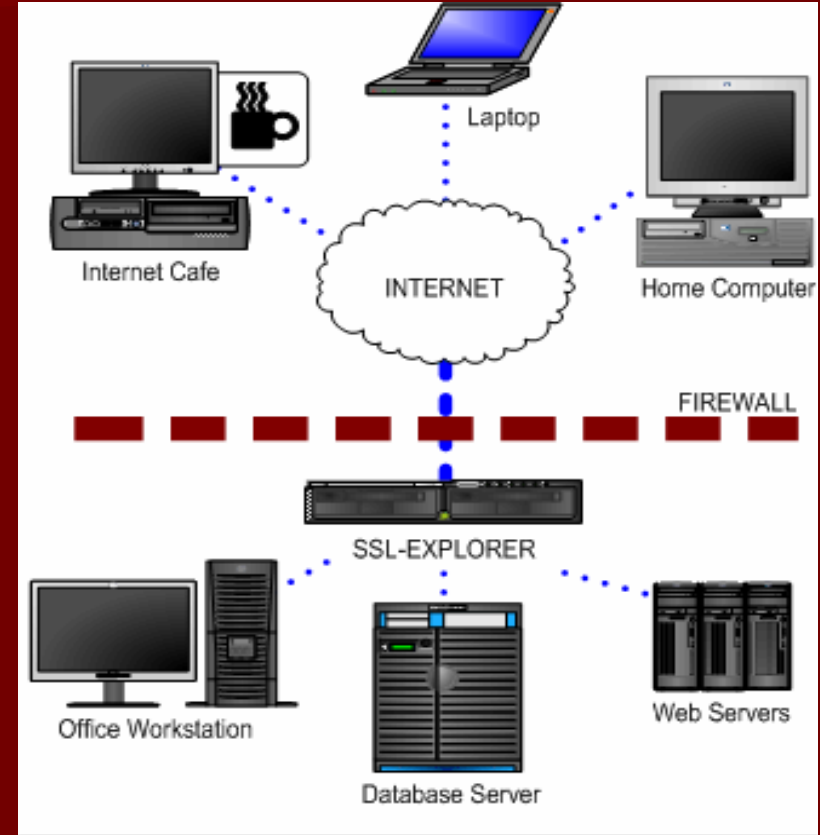


Fig. 1: SSL-Explorer safeguards your network infrastructure through the use of 128-bit SSL encryption across insecure networks

SSLExplorer



- Browser tabanlı özgür SSL VPN Çözümü
- Active Directory, UNIX passwd, Radius Destekli, kendi onay mekanizması
- Linux, Windows destekli
- Sınırsız eş zamanlı kullanıcı desteği
- Role tabanlı kullanıcı
- Ticari eklenti desteği ile çeşitli özellikler
- <http://3sp.com/showSslExplorer.do>

OpenVPN



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

OpenVPN

- Layer 2 ve Layer 3 VPN imkanı
 - Bridge mode, routing mode
 - Broadcast gerektiren uygulamalar, farklı ağ grupları
- Tun, tap sahte arabirimler
- Statik, pre-shared, ve dinamik anahtar değişimi destekli
- IPsec'e göre oldukça basit, anlaşılır..
- NAT arkasından problemsiz kullanım imkanı
- İsteğe bağlı olarak GUI aracılığı ile yönetim

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 sonrası ayarlar

OpenVPN Yapılandırma

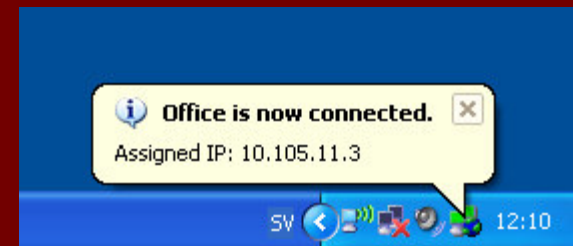
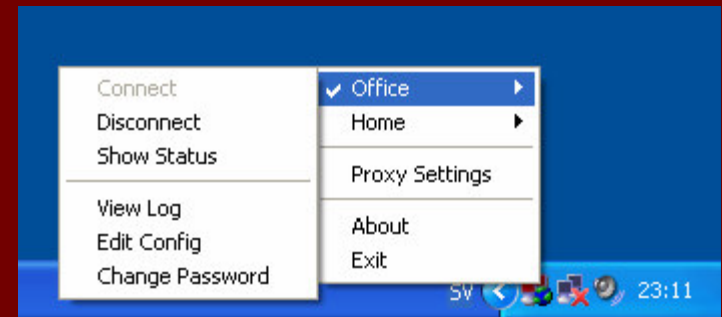
- CA(Certificate Authority) Kurulumu
 - # cd /usr/src/openvpn/openvpn-2.0/easy-rsa
 - # . ./vars
 - # ./clean-all
 - # ./build-ca
- Sunucu Sertifikası oluşturma
 - # ./build-key-server server
- İstemciler için anahtar oluşturma
 - # ./build-key laptop
- Diffie Hellman parametrelerini oluşturma
 - # ./build-dh
- 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)

- **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 degisikligi yasanmasin
- **Max. İstemci sayisi**
max-clients 100

OpenVPN GUI (windows)

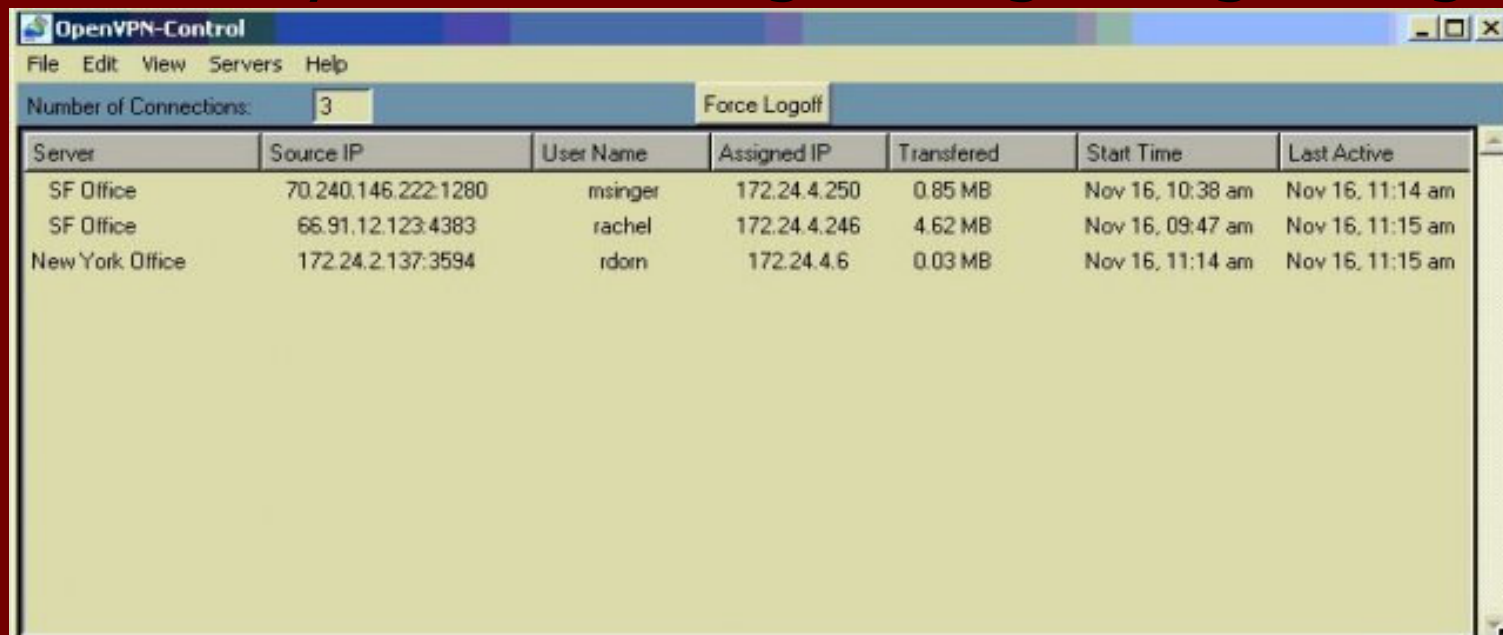
- GPL Lisanslı ile özgür kullanım
- VPN yönetimi(start/stop/restart/
- Log izleme
- Proxy ayarları yapma imkanı
- Config dosyasını düzenleme seçeneği
- <http://openvpn.se/>



OpenVPN Araçları

■ OpenVPN Control

- Multiplatform Openvpn sunucu kontrolü
- Sunucuya kimlerin bağlı olduğu vb gibi bilgiler



The screenshot shows the OpenVPN-Control application window. It has a menu bar with 'File', 'Edit', 'View', 'Servers', and 'Help'. Below the menu bar, there is a status bar showing 'Number of Connections: 3' and a 'Force Logoff' button. The main area contains a table with the following data:

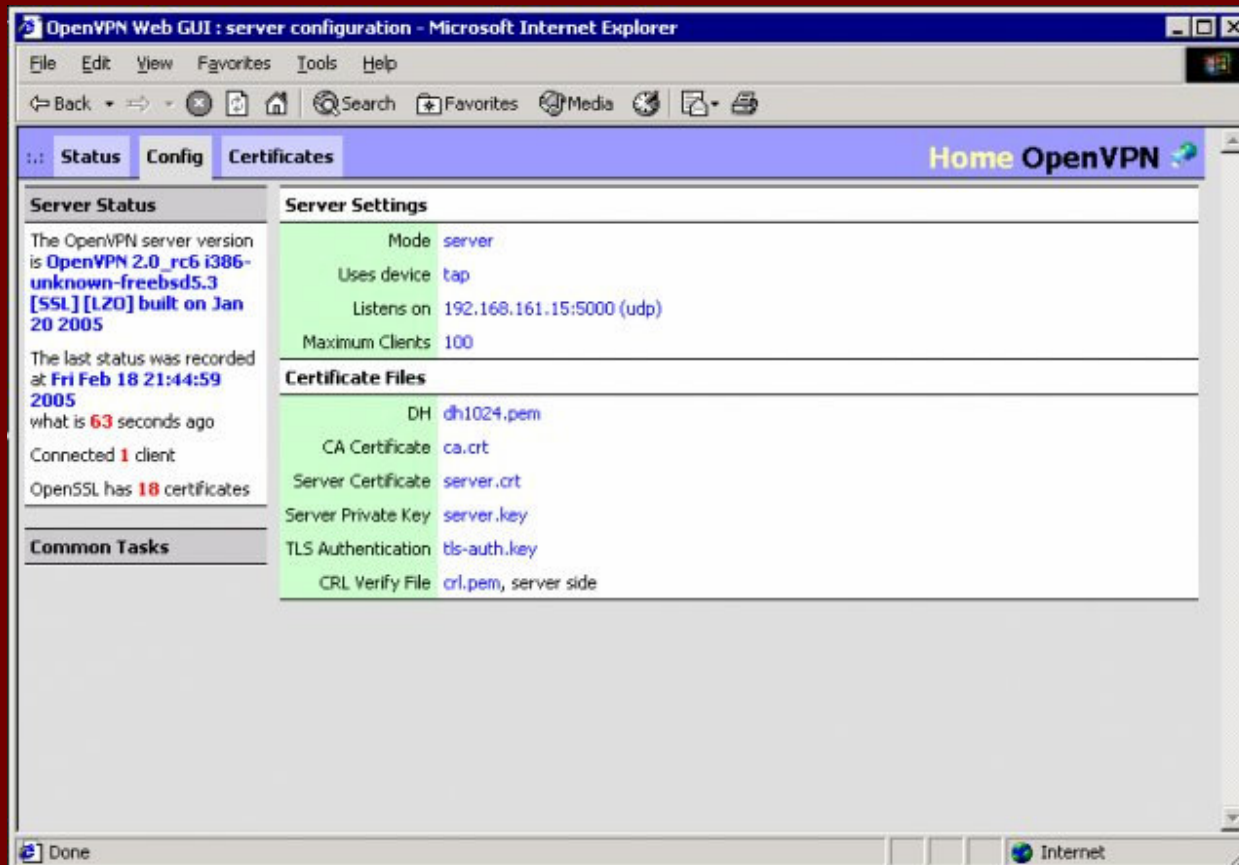
Server	Source IP	User Name	Assigned IP	Transferred	Start Time	Last Active
SF Office	70.240.146.222:1280	msinger	172.24.4.250	0.85 MB	Nov 16, 10:38 am	Nov 16, 11:14 am
SF Office	66.91.12.123:4383	rachel	172.24.4.246	4.62 MB	Nov 16, 09:47 am	Nov 16, 11:15 am
New York Office	172.24.2.137:3594	rdorn	172.24.4.6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

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

OpenVPN Araçları

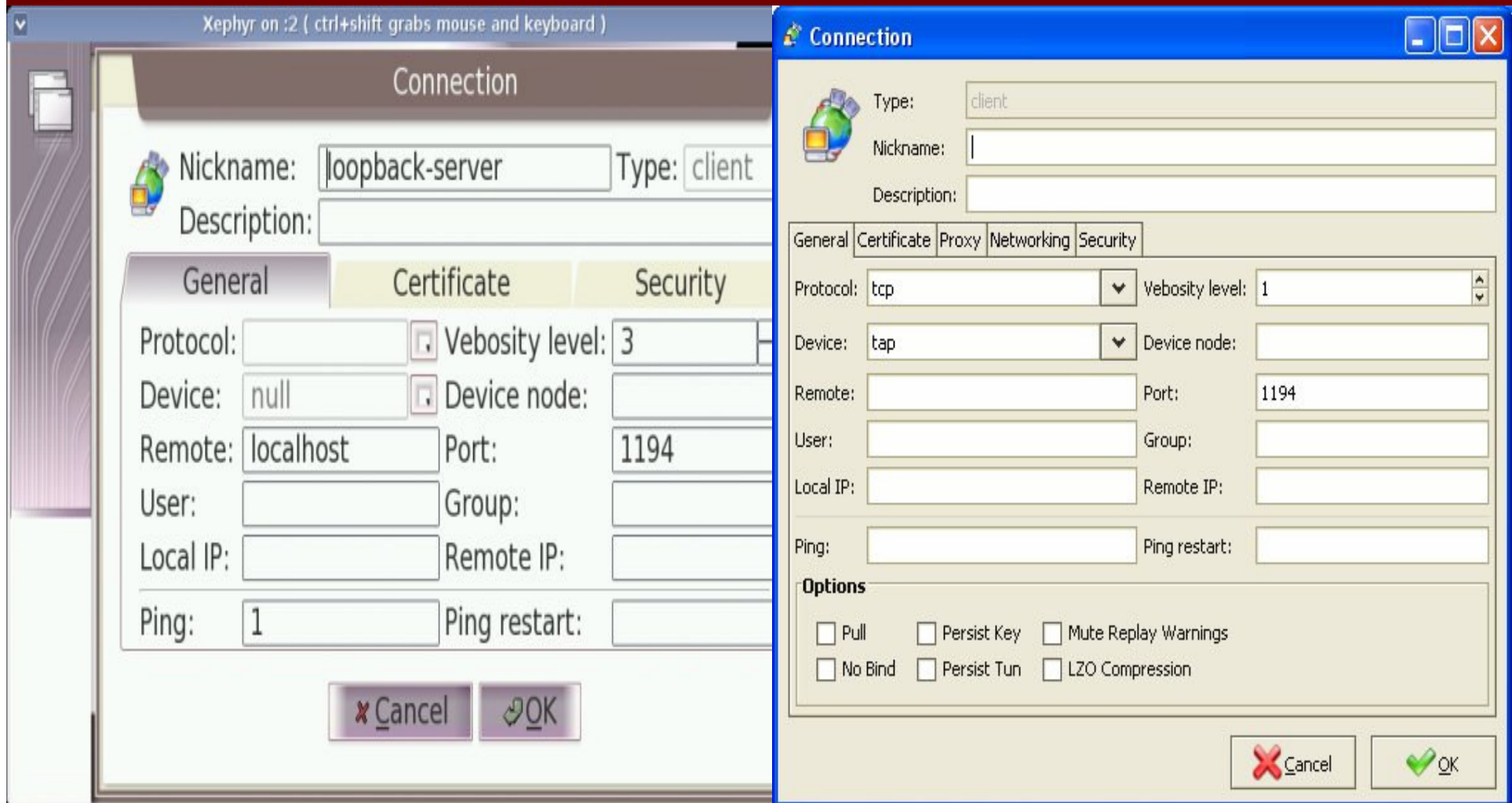
■ OpenVPN Web GUI

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



OpenVPN Araçları

- <http://sourceforge.net/projects/openvpnadmin>



Karşılaştırma

- PPTP güvenlikten sınıfta kalıyor, basit yönetim ve ücretsiz istemci avantajı var
- Ipsec en sağlam, kararlı çözüm fakat yapılandırması ve kullanımı zor, özel istemci gerektiriyor..
- L2TP IPsec olmadan kullanılmıyor
- SSLVPN en gözde çözüm..
- OpenVPN her ölçekte ağ için uygun bir seçim..

Kaynaklar

- www.openvpn.net
- www.vpnc.org (Virtual Private Network Consortium)
- <http://www.microsoft.com/technet/prodtechnol/windowsserver2003/tr/library>
- <http://seminer.linux.org.tr/seminer-notlari/vpn/>

Sunum notlari

- <http://www.enderunix.org/media/acikvpn.pdf>

