Açık Kod yazılımlar ile Ağ ve Güvenlik Çözümleri

Huzeyfe ÖNAL
huzeyfe@EnderUNIX.org

Sunum Planı

- Linux, *BSD, Açık Kod, Özgür yazılım Terimleri
- Linux/UNIX zor mu?
- İhtiyaca yönelik seçim..
- Temel Ağ servisleri
  - DHCP, DNS, Monitoring, mail, web, ftp, file server
- Güvenlik Servisleri
  - Firewall, VPN, IDS/IPS,Proxy, CF, Security Scanner

Tanımlar..

- Linux, Linux dağıtımları.
- BSD
  - FreeBSD, NetBSD, OpenBSD
- Linux mu UNIX mi?
- Linux/UNIX gerçekten zor mu?
  - Kolaylik mi, basitlik(anlaşılırlık)mi ?
- Bilişimci ne iş yapar, ne bilmelidir?
- Bilişim meslek mi hobi mi?

Temel Ağ Servisleri

- DNS Sunucu
  - Internetin temel yapı taşlarından
  - Mail, web ..trafiğini etkiler
  - Yanlış yönetim kurbanı
  - ISC BIND, DJBDNS ...
- WEB, FTP, Mail, File server, DHCP…
  - Apache, PureFTPD, ProFTPD, Samba, ISC DHCP

BIND DNS Sunucu

- Açık kaynak kodlu
- Standartlara uygun
- Ek güvenlik özellikleri sağlar
  - Chroot, dnssec.
- View, blacklist vb ile özelleştirilmiş yönetim
- Kolay, anlaşılır yapılandırma dosyası
- GUI, WEB üzerinden yönetim için onlarca araç..
  - Freshmeat.net, sf.net, Webmin...
- Her eve lazım..☺

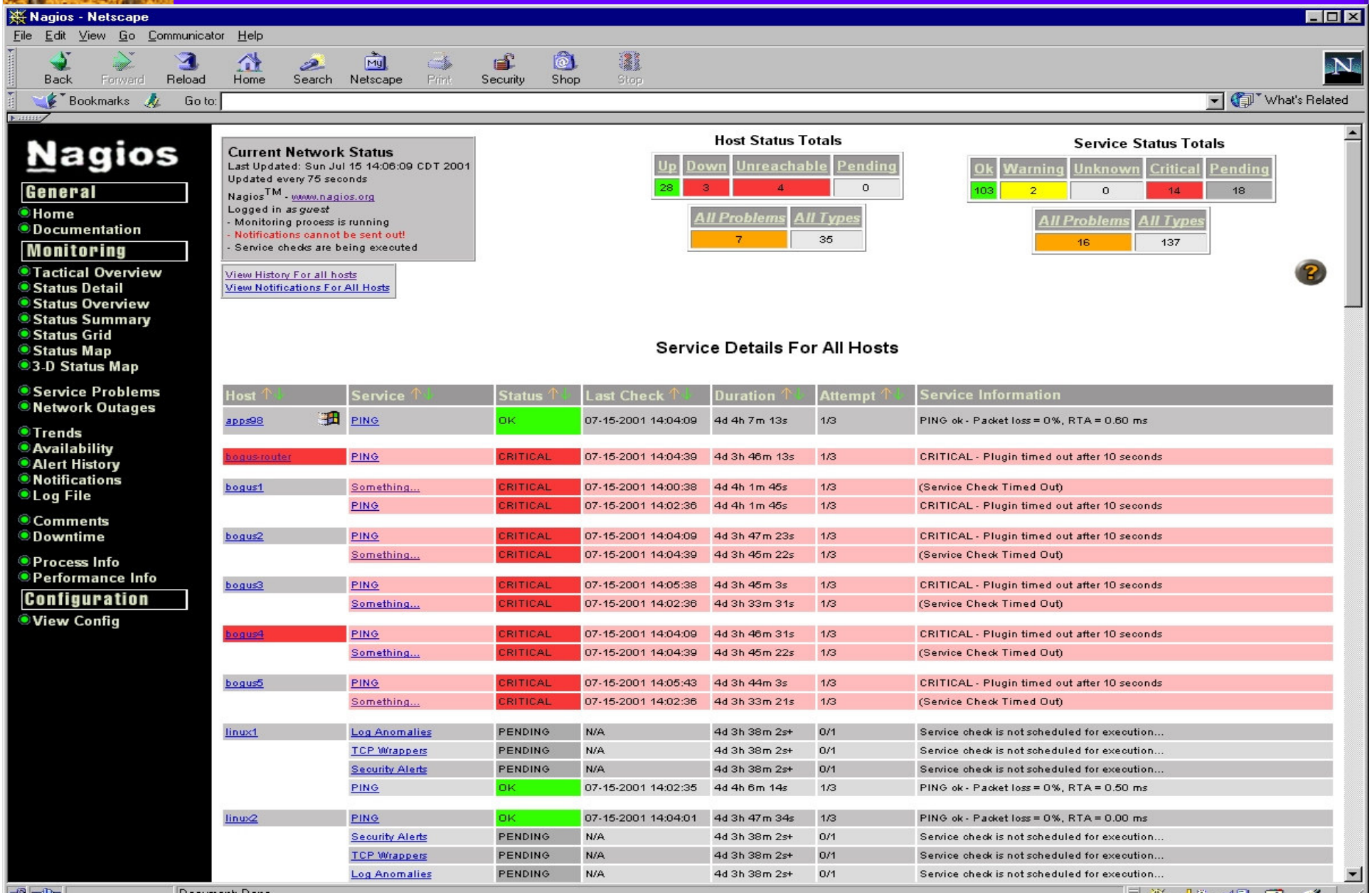
DHCP Hizmeti

- DHCP(Dynamic Host Conf. Protocol) ?
- ISC tarafından yönetiliyor
- Geniş kapsamlı bir proje
- Web ve konsol aracılığı ile kolay yönetim
  - Webmin, Freshmeat ,Sf.net
- Standartlara Uygun
- HA yapısında çalışabilirlik
- Birçok ticari sürümü var

Sistem Gözleme

- Orta ölçekli bir ağ için gerekli
- Nagios, BigBrother …
- Nagios:
- Her tür servis kontrolü
  - Ssh, ftp, dns, telnet,
  - Ajan programlar uzak sistemlere ait disk, cpu, bellek gözleme
  - Gelişmiş uyarı mekanizması
  - Ses, mail, web, sms, Messenger

Nagios servis durumu..



Güvenlik Hizmetleri

- Kime ? Ne derece güvenlik?
- Güvenlik Maliyet ilişkisi
- Güvenlik mi? Paranoya mı?
- Açık sistemler ne kadar güvenli?
  - Kodların açık olması ..
  - Protokollerin açık olması
- Zincirdeki en zayıf halka; insan…

Güvenlik Hizmetleri-II

- Firewall(Güvenlik Duvarı)
  - En temel bileşen, olmazsa olmazlardan
  - Firewall ne işe yarar? Firewall != oyuncak
  - Güvenlik tasarımı.
  - Zone kavramı

    DMZ, iç ağ, internet
- Özgür Firewall yazılımları
  - Linux Iptables, FreeBSD IPF, IPFW, OpenBSD Packet Filter(PF)

OpenBSD PF(Packet filter)

- En gelişmiş açık kod Firewall çözümü
- Aktif gelişim süreci
- Kolay ve anlaşılır yapı
- HA ve Load Balancing
- Ileri düzey trafik kontrolü
- Bandwith Shaping
- Bridge mode çalışma yeteneği
- Üstün performans
  - Gerçek hayattan örnekler

OpenBSD PF -II

- GUI aracılığı ile yönetim
  - Fwbuilder
  - PFW
- Örnek kural söz dizimi

Filtreleme;

Pass in log on $ext_if proto tcp from 1.2.3.4 to 4.5.6.7

Block in log on $ext_if proto tcp ftom any to 172.16.10.1 port 23

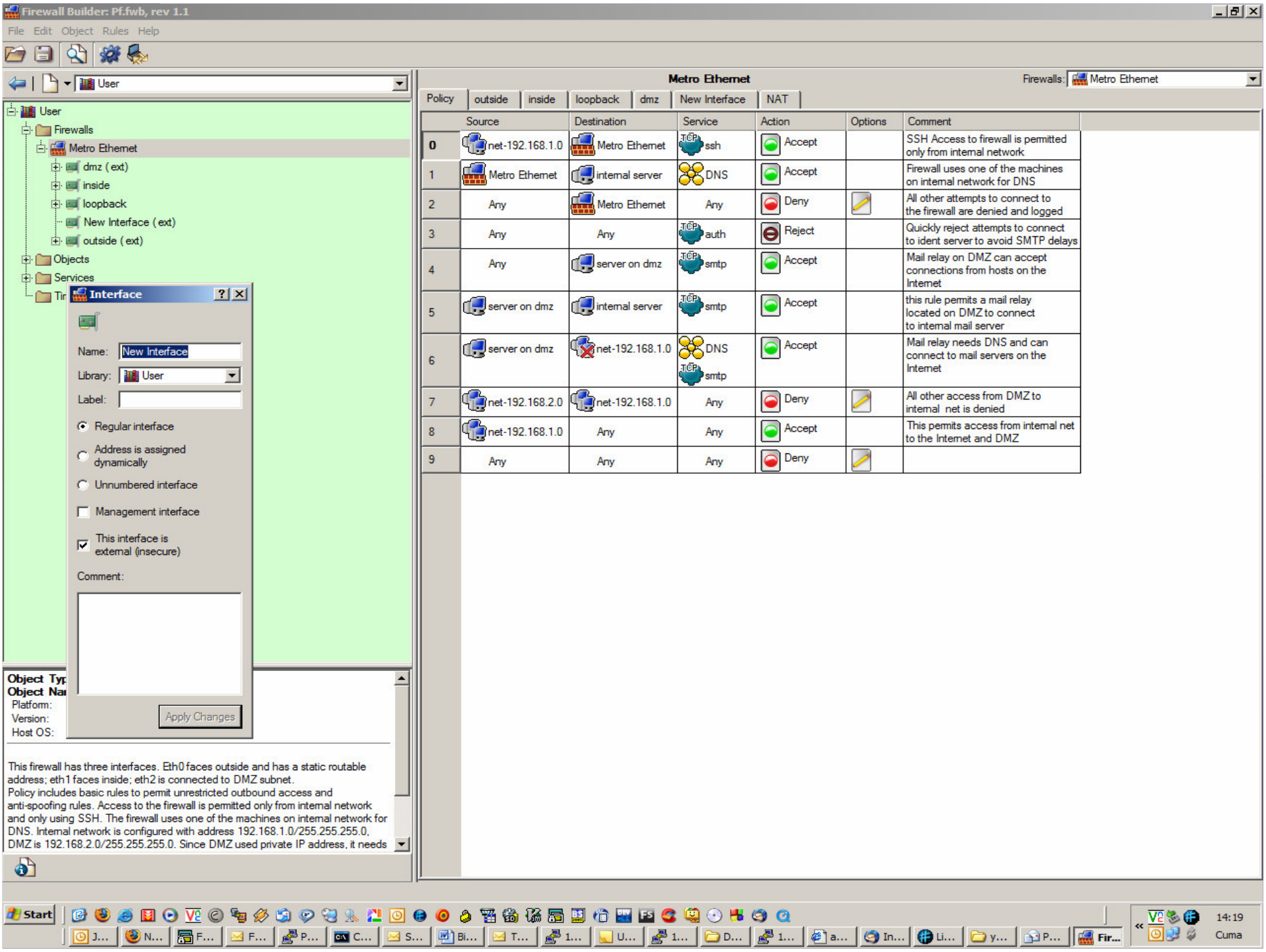
Nat

Nat on $ext_if from $ic_ag to any -> 11.22.33.44

- Basit, performanslı, anlaşılır log yapısı
- Tcpdump kullanılarak izlenebilir.

Dec 02 17:20:31.046452 rule 15/(match) pass out on fxp0: 15.1.5.74.52741 > 83.41.39.166.4672: tcp

- Web arabiriminden rapor alınabilir


Firewall Builder: Pf.fwb, rev 1.1
File Edit Object Rules Help
User
User
Firewalls
Metro Ethernet
dmz (ext)
inside
loopback
New Interface (ext)
outside (ext)
Objects
Services
Interface
Name: New Interface
Library: User
Label:
Regular interface
Address is assigned dynamically
Unnumbered interface
Management interface
This interface is external (insecure)
Comment:
Apply Changes
Platform:
Version:
Host OS:
This firewall has three interfaces. Eth0 faces outside and has a static routable address; eth1 faces inside; eth2 is connected to DMZ subnet.
Policy includes basic rules to permit unrestricted outbound access and anti-spoofing rules. Access to the firewall is permitted only from internal network and only using SSH. The firewall uses one of the machines on internal network for DNS. Internal network is configured with address 192.168.1.0/255.255.255.0, DMZ is 192.168.2.0/255.255.255.0. Since DMZ used private IP address, it needs
Metro Ethernet
Firewalls: Metro Ethernet
Policy outside inside loopback dmz New Interface NAT
Source Destination Service Action Options Comment
0 net-192.168.1.0 Metro Ethernet ssh Accept SSH Access to firewall is permitted only from internal network
1 Metro Ethernet internal server DNS Accept Firewall uses one of the machines on internal network for DNS
2 Any Metro Ethernet Any Deny All other attempts to connect to the firewall are denied and logged
3 Any Any auth Reject Quickly reject attempts to connect to ident server to avoid SMTP delays
4 Any server on dmz smtp Accept Mail relay on DMZ can accept connections from hosts on the Internet
5 server on dmz internal server smtp Accept this rule permits a mail relay located on DMZ to connect to internal mail server
6 server on dmz net-192.168.1.0 DNS smtp Accept Mail relay needs DNS and can connect to mail servers on the Internet
7 net-192.168.2.0 net-192.168.1.0 Any Deny All other access from DMZ to internal net is denied
8 net-192.168.1.0 Any Any Accept This permits access from internal net to the Internet and DMZ
9 Any Any Any Deny
Start
14:19
Cuma

Saldırı Tespit/Engelleme

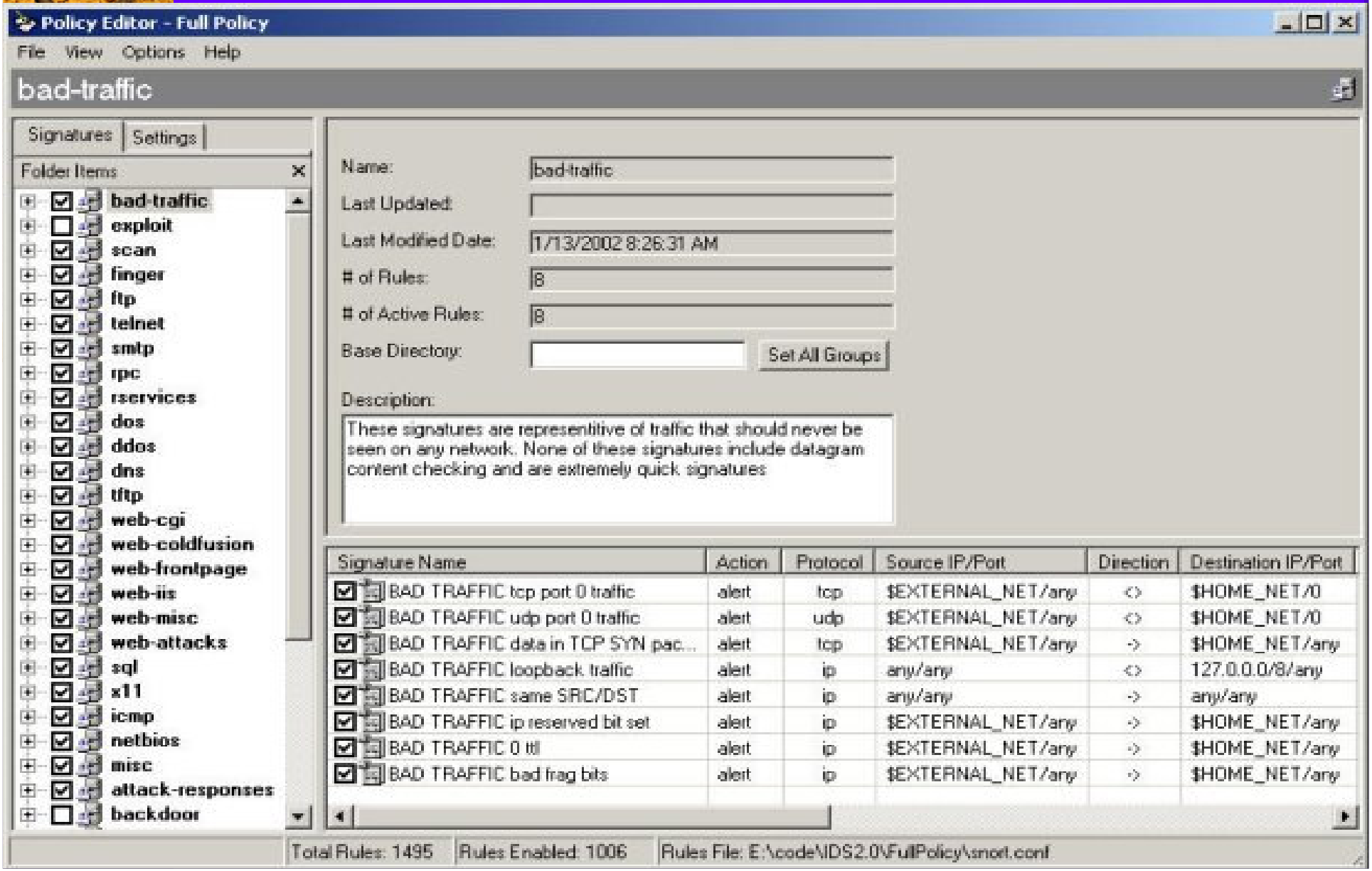
- Normal trafik -saldırgan trafigi ?
- Anormal trafiği izlemek işe yarar mı?
- Snort, Snortsam, snort-inline en bilinen çözümler
- En bilinen özgür (N)IDS Snort
  - Kurucu firma Checkpoint tarafından 85k$ alındı
  - SourceFire firmasi ***OpenBSD+Snort+..*** BOX ürünü
- Snortsam ve snort-inline Snort için engelleme eklentisi olarak kullanılabilir.

Snort ..

- 7 yıl öncesinde basit bir sniffer projesi..
- Günümüzde: Ağ temelli , imza tabanlı saldırı tespit sistemi
- Açık kaynak kodlu, Aktif geliştirici topluluğu
- Bol ve açık dökümantasyon

  Belgeler, kitaplar, e-posta listeleri...
- Snortsam ile Firewall'a kural gönderme
- Onlarca yönetim arabirimi
  - En bilinenleri: Acid-Base, Squil, Ids center.

IDS Policy Manager



VPN hizmetleri

- VPN(Virtual Private Network) ?
- VPN Çeşitleri
  - Ipsec VPN, L2TP, PPTP, SSL VPN
- İhtiyaca göre seçim…

IPsec VPN Çözümleri

- Standart bir Çözüm
- Tam güvenlik
- Kompleks yapı, kurulum kullanım zor(?)
- Linux FreeSWAN/OpenSWAN
- OpenBSD Ipsec altyapısı

PPTP Çözümü

- Uçtan uca tünelleme/şifreleme sağlar
- Microsoft destekli…
- Hızlı, kolay yapılandırma kullanım tercih sebebi
- Windows işletim sistemi ile birlikte istemcisi gelir.
- Linux'lar için pptpclient.sf.net
- Şifreli kullanımı yeter seviyede güvenli

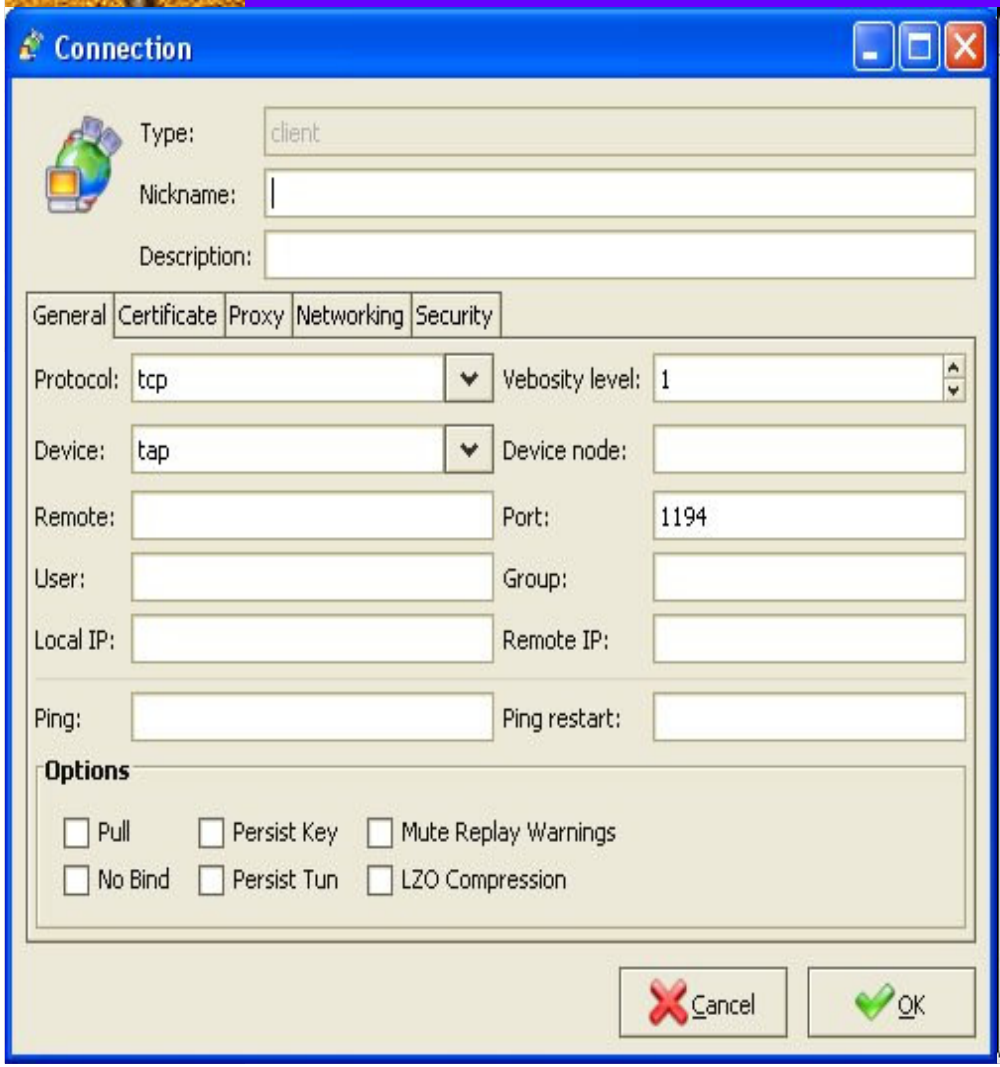
PopToP

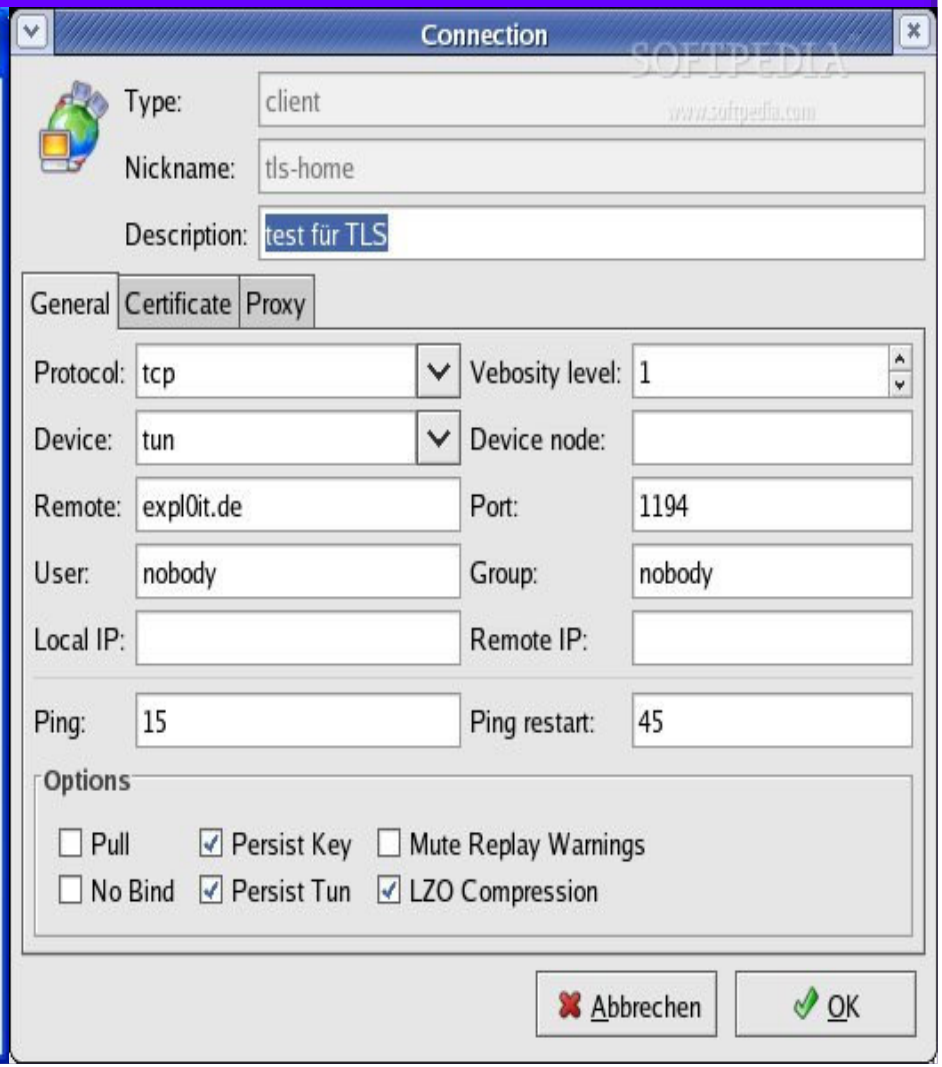
- PopTop (The PPTP server for Linux) BSD, Solaris
- GPL Lisanslı
- Kolay kurulum ve yönetim
- Microsoft uyumlu kimlik denetimi ve şifreleme(MSCHAPv2, MPPE 40 - 128 bit RC4)
- Eşzamanlı birden fazla kullanıcı desteği
- Radius eklentisi ile samba ve ldap üzerinden onaylama yapabilir.
- www.poptop.org

OpenVPN

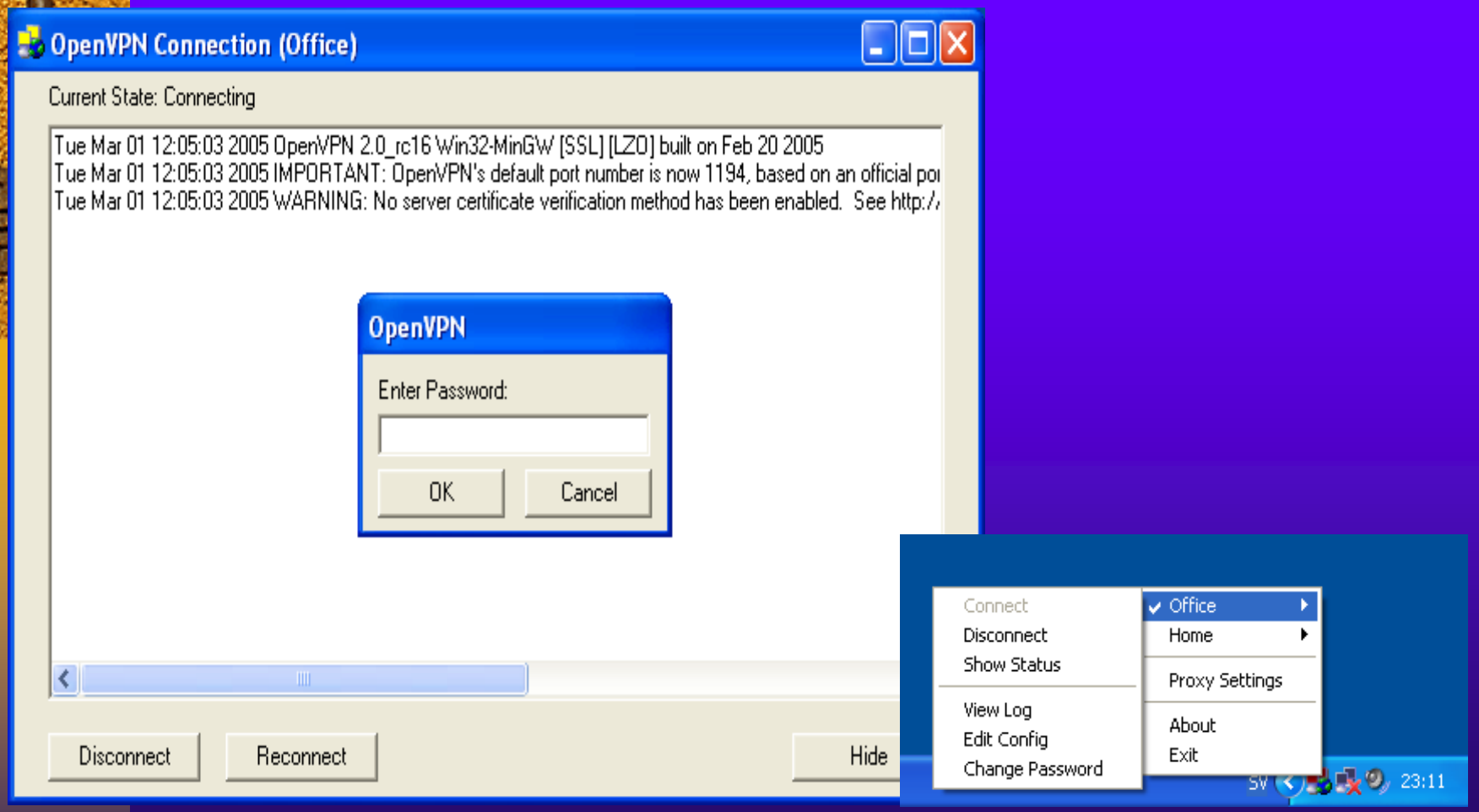
- MultiPlatform SSL VPN Çözümü
  - Linux,*BSD, Solaris, Windows...
- Geniş, anlaşılır dökümantasyon
- TCP/UDP tek port üzerinden çalışır, NAT sorunsuz
- OpenSSL kütüphanesinin sunduğu herşey..
- Kolay kurulum ve yönetim
  - GUI, konsol, Web
  - IPsec kompleskligi yok
- www.openvpn.net

OpenVPNAdmin GUI





OpenVPN GUI..


OpenVPN Connection (Office)
Current State: Connecting
Tue Mar 01 12:05:03 2005 OpenVPN 2.0_rc16 Win32-MinGW [SSL] [LZO] built on Feb 20 2005
Tue Mar 01 12:05:03 2005 IMPORTANT: OpenVPN's default port number is now 1194, based on an official por
Tue Mar 01 12:05:03 2005 WARNING: No server certificate verification method has been enabled. See http:/
OpenVPN
Enter Password:
OK
Cancel
Disconnect
Reconnect
Hide
Connect
Disconnect
Show Status
View Log
Edit Config
Change Password
Office
Home
Proxy Settings
About
Exit
23:11

Zayıflık inceleme

- Açıklarınızı Hackerler keşfetmeden siz bulun..
- Ethical Hacking: Son yıllarda oldukça popüler
- Nessus, Nmap, nikto…

Nessus

- ’98 yılında Renaud Deraison tarafından GPL olarak başlatıldı
- 2005 Lisans değişikliği…☹
- İstemci sunucu mimarisine göre çalışır
- Uzak ve yerel sistem güvenliği kontrolü
- Uzak ve yerel sistem güvenlik tarama özelliği
  - Nessus yerel güvenlik taraması yapabilen ik ürün
  - Windows, UNIX ve Mac makinelere login olarak gerekli taramaları, eksik yamaları belirleyebilir
- Web, GUI , konsol ile kolay yönetim
- Güncel zayıflık veritabanı(günlük)
- Bulunan açıklar için detaylı bilgi ve referans
- 8000~farklı zayıflık imzası
- NASL ile zayıflık tanımlama özelliği
- Birçok ticari kopyası var

Proxy Hizmeti

- Proxy (Vekil Sunucu) nedir?
- Kullanım amacı
  - internet kullanımı kısıtlama
  - Bandwith ayarlama
  - Raporlama
  - Güvenlik
  - Virus tarama vs
  - Squid, oops

Squid...

- http, https, ftp… için Caching proxy
- Şeffaf proxy (transparent Proxy)özelliği
- ACL yapısı ile gelişmiş kural tanıma imkanı
- LDAP, AD, Mysql üzerinden kullanıcı onaylama
- ClamAv deteği ile birlikte WEB trafiğinde virüs kontrolü
- Redirector desteği ile ek özellikler..

İçerik Filtreleme

- İçerik kontrolu nedir?
- Özgür bir çözüm:DansGuardian
- DansGuardian
  - Herhangi bir Proxy ile çalışabilir
  - Siteleri PICS(http://www.w3.org/PICS/) etiketleme sistemine göre bloklayabilir
  - MIME tipine ve dosya uzantısına göre filtreleme yapabilir.
  - Düzenli ifadeler ile URL filtreleme yapabilir.
  - IP tabanlı URL filtreleme
  - Veritabanına uygun CSV formatında log üretir.
  - Belirli IP ve kullanıcı adına göre filtreleme

Hazır CD'ler

- İhtiyaca yönelik hazırlanmış dağıtımlar
- Disksiz çalışan sürümler oldukça popüler
- Knoppix ile başlayan Live CD serüveni..
- Hemen hemen her ihtiyaca yönelik Live CD
  - Oyun, Matematik, Firewall, Güvenlik, Kurtarma, Router vs vs.
- Knoppix STD, Phlax, Whoppix, MonoWall

FrozenTech's LiveCD List

Display All LiveCDs with a function of Firewall/Router Update

All Functions
Astronomy
Bioinformatics
Clustering
Desktop
Development
Diagnostics
Education
Firewall/Router
Forensics
Gaming
GIS
Hobby
Home Entertainment
Media Production
Medical
OS Replacement
Rescue
Robotics
Science

Votes [go vote]	Name	ISO Size (megabytes) Min	Max	Prin	Download	Links
4	m0n0wall	5	5			
2	redWall Firewall	148	154			
1	NetBoz	53	143			
0	Devil-Linux	88	88			
0	floppyfw	2	2			
0	Linux Live-CD Router	83	83			
0	Public IP ZoneCD	271	271			
0	Sentry Firewall CD	288	288			
0	Trx Live Firewall	653	653			
0	XORP Live CD	132	132	Firewall		

CLEAR SETTINGS

Currently displaying 10 LiveCD/DVDs

Key:
Primary Functions:

Türkiye'den..

- Linux Kullanıcıları Derneği
  - Linux.org.tr, www.lkd.org.tr
- EnderUNIX Yazılım geliştirme ekibi
  - EnderUNIX.org
- Mutasyon.net
- Belgeler.org
- Fazlamesai.net
- Ceviz.net Linux Forumu
- www.huzeyfe.net

Teşekkürler..

Sunum adresi

http://www.enderunix.org/slides/acikkod_sec.pdf

Eskiz.NET'e teşekkurler...