IPcop Linux
release 1.4.x
zum Kennenlernen

Bruno Hopp
Linuxuser der Universität zu Köln:

Jan. 2006
www.uni-koeln.de/themen/linux

Warum ausgerechnet IPcop ??

Vorteile: recycling eines ausgedienten PC möglich. Bislang IPcop auf i386-i686 etabliert, IPcop für Alpha gibt es schon, für Sparc | Ultrasparc nicht geplant.

Standardhardware (NIC) wird unterstützt: alle NIC-driver sind als Module ausgelegt. Interfaces:
Modem: JA *ISDN: JA* *Ethernet: JA*
GB-Ethernet: ist in Arbeit, z.Zt. nur einige wenige Adapter unterstützt.

Dedizierter HW-router kann besser spezialisierte Aufgaben (package filtering) erledigen als eine workstation, auf der "nebenher" noch nameserver (bind9), Samba und ein grafisches Interface laufen.

Software

- bis release 1.3 auf RedHat Linux basierend, Installation ncurses-basiert
- Grundlegende Überarbeitung ab release 1.4.x LSB conform, Linux from Scratch, angepasste Smoothwall-Skripte
- aktuelle IPcop releases 1.4.9/1.4.10 mit **Kernel 2.4.31**, kernel 2.6.x in Planung
- **iptables** 1.4.1; **OpenSSH** 3.9p1; **OpenSSL** 0.9.7e-fips; **Apache** 1.3.33 (build oct.2005) **Perl** 5.8.5; **GRUB** 0.9.5; **vim** 6.3

IPcop basics

- ***unterliegt der GNU/GPL***
- Routing: forwarding & NAT
- Was kann/soll ein Router neben dem reinen „Routing“ noch tun?
- Package filtering: **iptables**
- Web traffic: Proxy Squid – SquidGuard – DansGuardian – URL-filter
- Pop3/Imap: Copfilter u.a.
- Logging lokal oder via **Log-server**

Voraussetzungen zur Installation

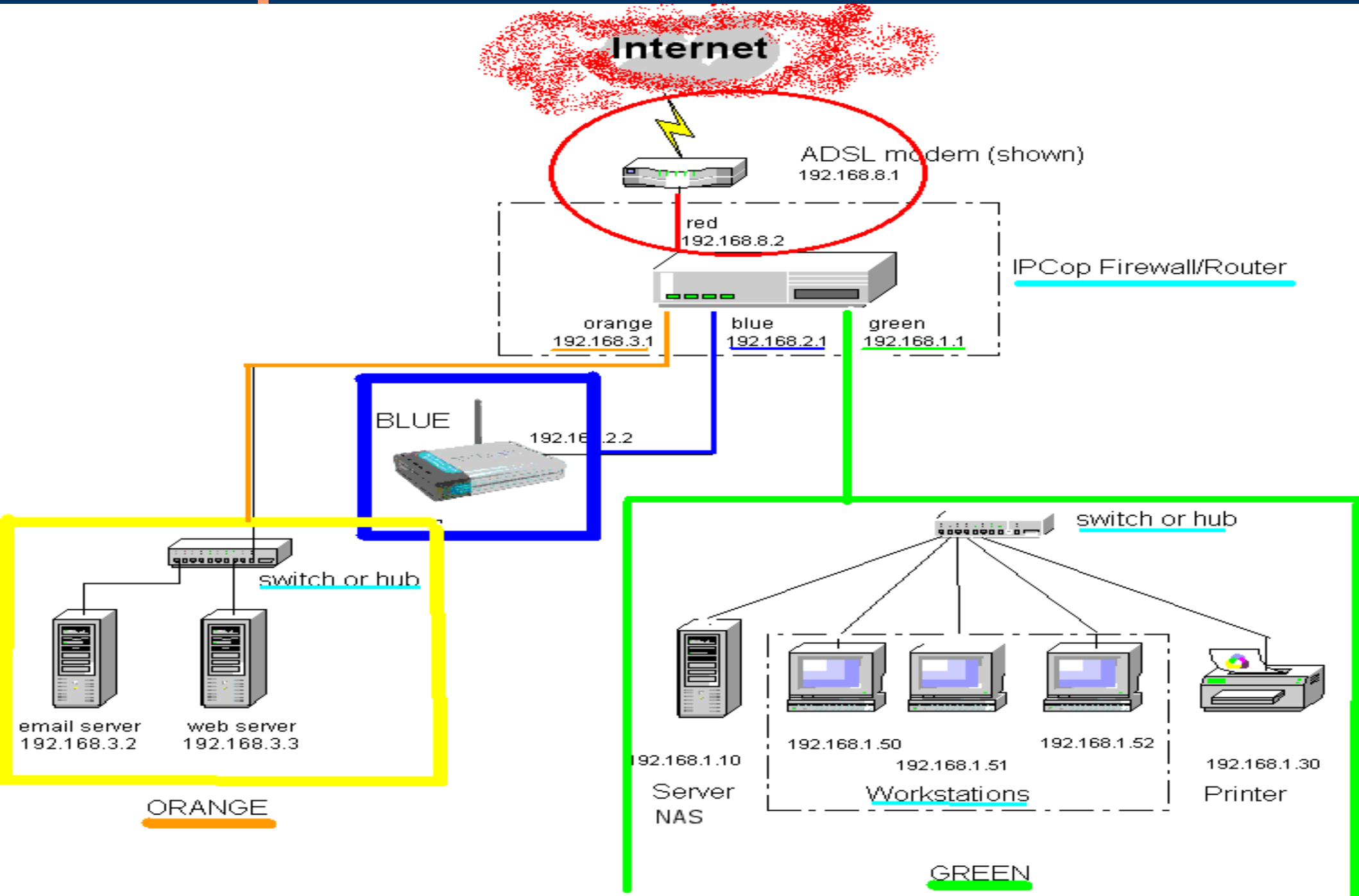
- **Download des ca. 42 MB großen iso-images**
- **von CD booten oder Startdiskette+ image von Webserver**
- **hda wird kpl neu formatiert mit *ext3* (egal ob 500 MB oder 10 GB - Partitionierung nicht beeinflussbar)**
- **486/DX2 mit 16 MB mindestens, 586 (Pentium1)+ 64 MB erlaubt normales Arbeiten - abhängig von Zahl der Requests, der Clients, der Addons etc.**
  Einschätzung für DSL: 200 Mhz P1 mit 128 MB sollte tun, mit Squid und mehreren Addons sind 256 MB ausreichend auch bei 100 Clients.

Profil eines IPcop (einfachster Fall)

- Routing mit NAT
- Paketfilter (iptables)
- DNS caching only

- **Optional**
  - dhcpd
  - DynDNS
  - ntpd
  - sshd (nur nach Grün!)
  - Squid Proxy (web content)
  - SNORT intrusion detection
  - Traffic shaping mit "*WonderShaper*"

IPcop im Netz: krass bunt hier



Steuerung: security first

- Steuerung per Browser (https) + CGI-skripte

  https://rechnername:445

  http://rechnername:81

- SSH

  ssh -4 -p 222 root@rechnername

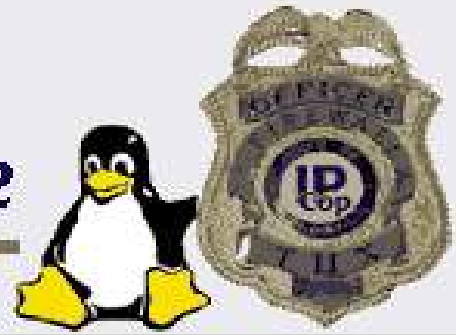
Bootmanager Grub

```
GNU GRUB  version 0.95  (638K lower / 804800K upper memory)

 IPCop
 IPCop SMP
 IPCop (ACPI enabled)
 IPCop SMP (ACPI HT enabled)

   Use the ↑ and ↓ keys to select which entry is highlighted.
   Press enter to boot the selected OS, 'e' to edit the
   commands before booting, 'a' to modify the kernel arguments
   before booting, or 'c' for a command-line.
```

The Bad Packets Stop Here



nightcity.localnet - Startseite - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

https://192.168.1.100:445/cgi-bin/index.cgi

Go

nightcity wiki Linux press Sci Google local Gudrun .de

IPCop 1.4.9

SYSTEM STARTSEITE

The bad packets stop here.

SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS

- STARTSEITE
- UPDATES
- PASSWÖRTER
- SSH-ZUGRIFF
- EINSTELLUNGEN DER BENUTZEROBERFLÄCHE
- DATENSICHERUNG
- HERUNTERFAHREN
- DANK AN ..

calnet

Verbinden Trennen Aktualisieren

Aktuelles Profil: FREENET

Leerlauf - FREENET

1. Für Ihr System sind Updates verfügbar. Im Abschnitt "Updates" erhalten Sie weitere Informationen dazu.

19:25:44 up 4 min, 0 users, load average: 0.44, 0.29, 0.12

Leerlauf - FREENET

19:25:44 up 4 min, 0 users, load average: 0.44, 0.29, 0.12

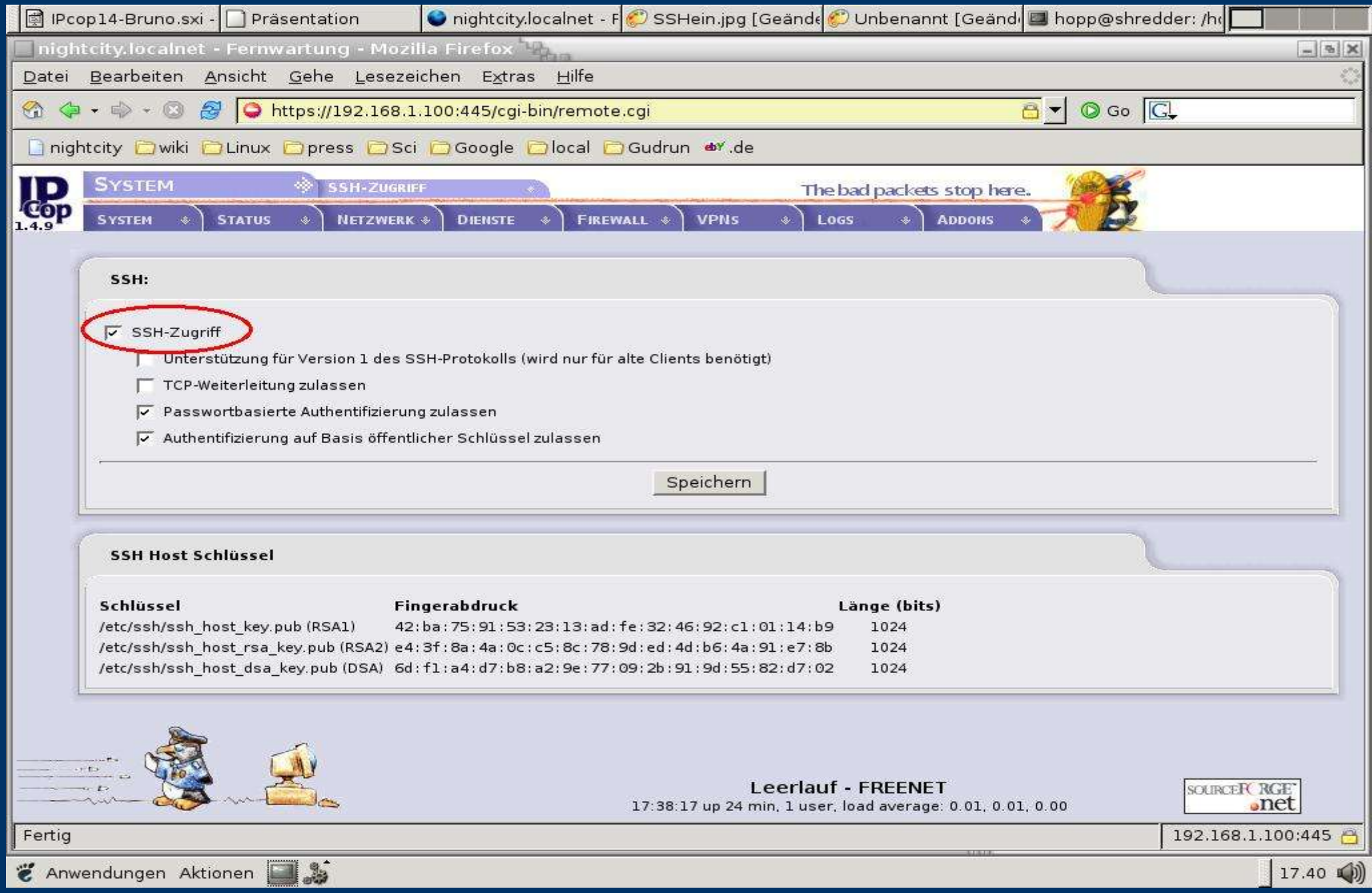
SOURCEFORGE.net

Fertig

192.168.1.100:445

und wie wird ausgeschaltet?

erst Mal SSH ...


IPcop14-Bruno.sxi -
Präsentation
nightcity.localnet - F
SSHein.jpg [Geände
Unbenannt [Geänd
hopp@shredder: /h
nightcity.localnet - Fernwartung - Mozilla Firefox
Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe
https://192.168.1.100:445/cgi-bin/remote.cgi
Go
nightcity wiki Linux press Sci Google local Gudrun .de
IPCop 1.4.9
SYSTEM
SSH-ZUGRIFF
The bad packets stop here.
SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS
SSH:
SSH-Zugriff
Unterstützung für Version 1 des SSH-Protokolls (wird nur für alte Clients benötigt)
TCP-Weiterleitung zulassen
Passwortbasierte Authentifizierung zulassen
Authentifizierung auf Basis öffentlicher Schlüssel zulassen
Speichern
SSH Host Schlüssel
Schlüssel Fingerabdruck Länge (bits)
/etc/ssh/ssh_host_key.pub (RSA1) 42:ba:75:91:53:23:13:ad:fe:32:46:92:c1:01:14:b9 1024
/etc/ssh/ssh_host_rsa_key.pub (RSA2) e4:3f:8a:4a:0c:c5:8c:78:9d:ed:4d:b6:4a:91:e7:8b 1024
/etc/ssh/ssh_host_dsa_key.pub (DSA) 6d:f1:a4:d7:b8:a2:9e:77:09:2b:91:9d:55:82:d7:02 1024
Leerlauf - FREENET
17:38:17 up 24 min, 1 user, load average: 0.01, 0.01, 0.00
SOURCEFORGE.net
Fertig
192.168.1.100:445
Anwendungen Aktionen
17.40

Dienste: | Speicher: | Festplattenbelegung: | Uptime und Benutzer: | Geladene Module: | Kernel-Version:

Dienste:

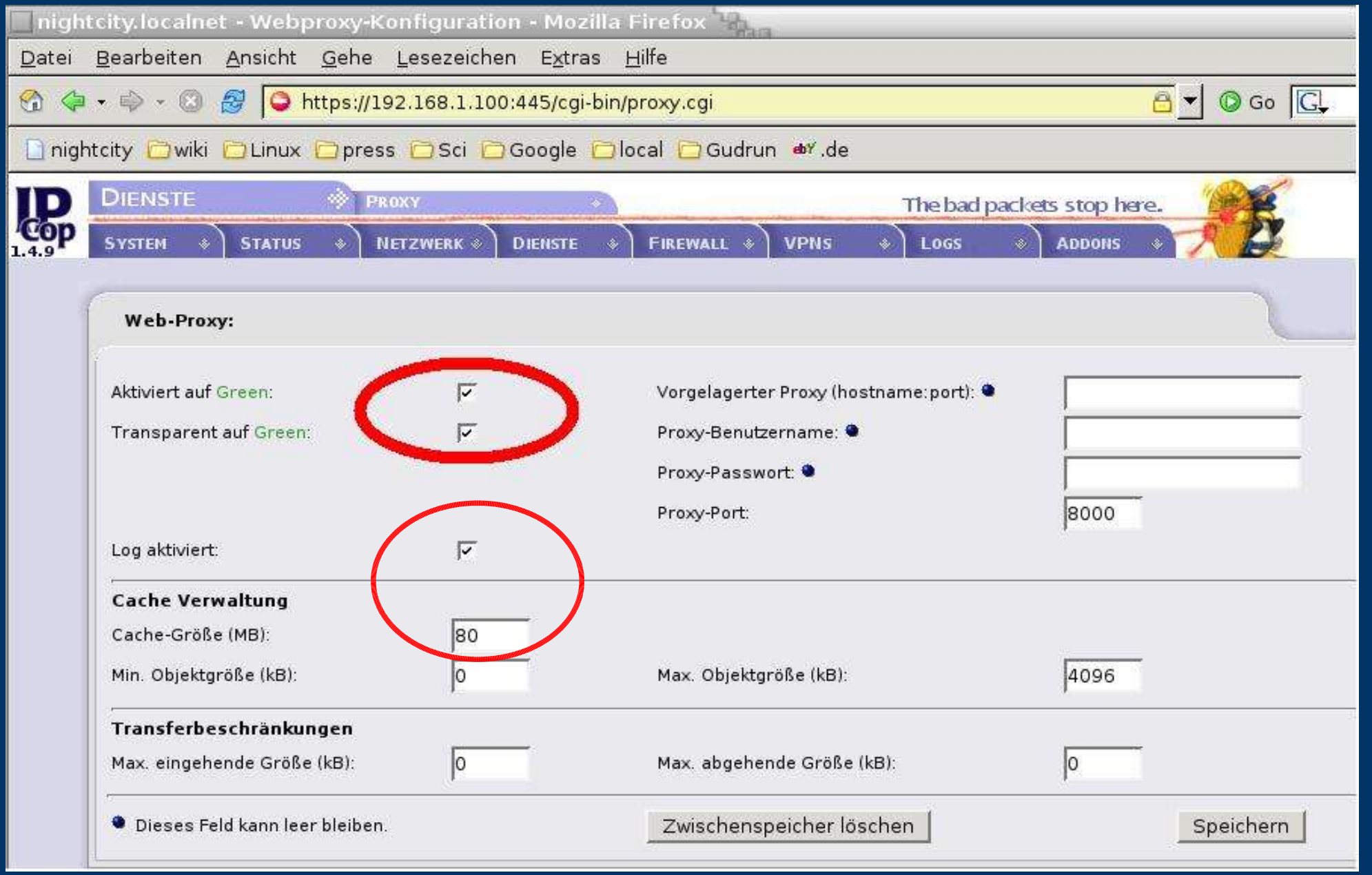
Cron-Server	LÄUFT
DHCP-Server	ANGEHALTEN
DNS-Proxyserver	LÄUFT
Intrusion Detection System (GREEN)	LÄUFT
Intrusion Detection System (RED)	ANGEHALTEN
Kernel-Protokollierungs-Server	LÄUFT
NTP-Server	ANGEHALTEN
Protokollierungs-Server	LÄUFT
Secure Shell Server	LÄUFT
VPN	ANGEHALTEN
Web-Proxy	LÄUFT
Web-Server	LÄUFT

Speicher:

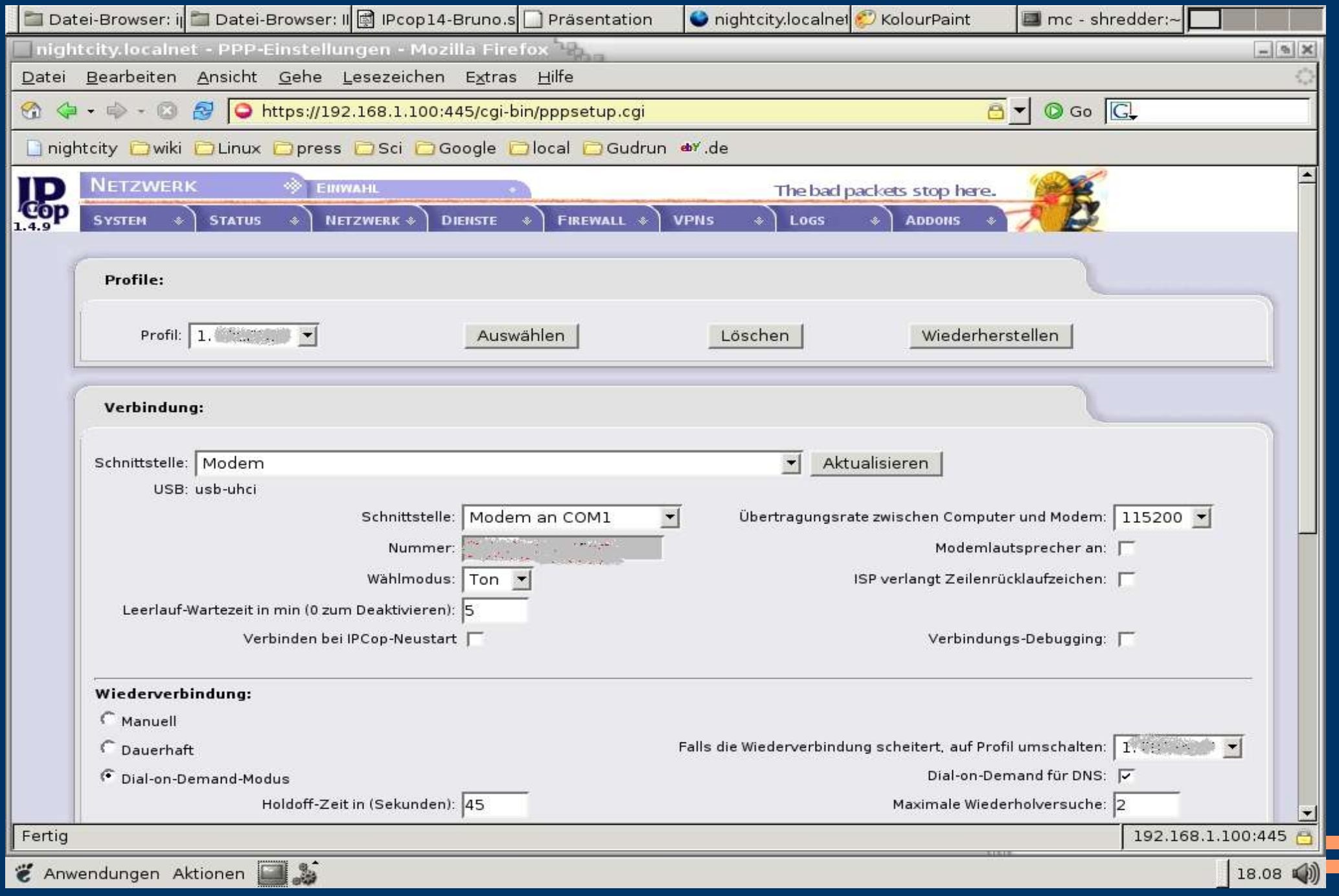
	Größe	Benutzt	Frei	Prozent			
RAM-Speicher	256880	81660	175220		31%	**shared**	0
-/+ Puffer/Zwischenspeicher		39288	217592		15%	**Puffer**	16780
Swap	32764	0	32764		0%	**zwischengespeichert**	25592

Festplattenbelegung:

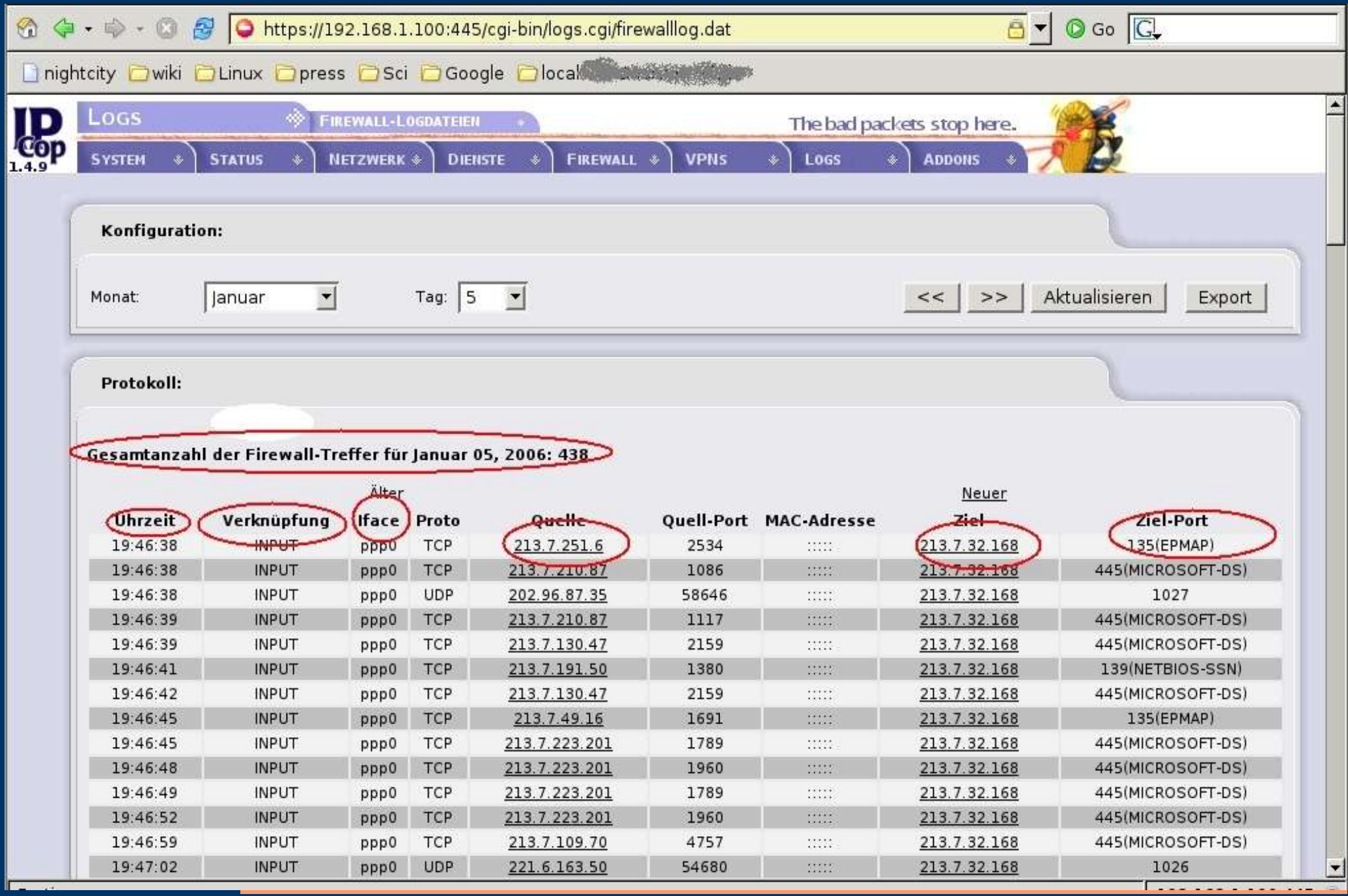
Squid einschalten



wohin verbindet sich der Router?

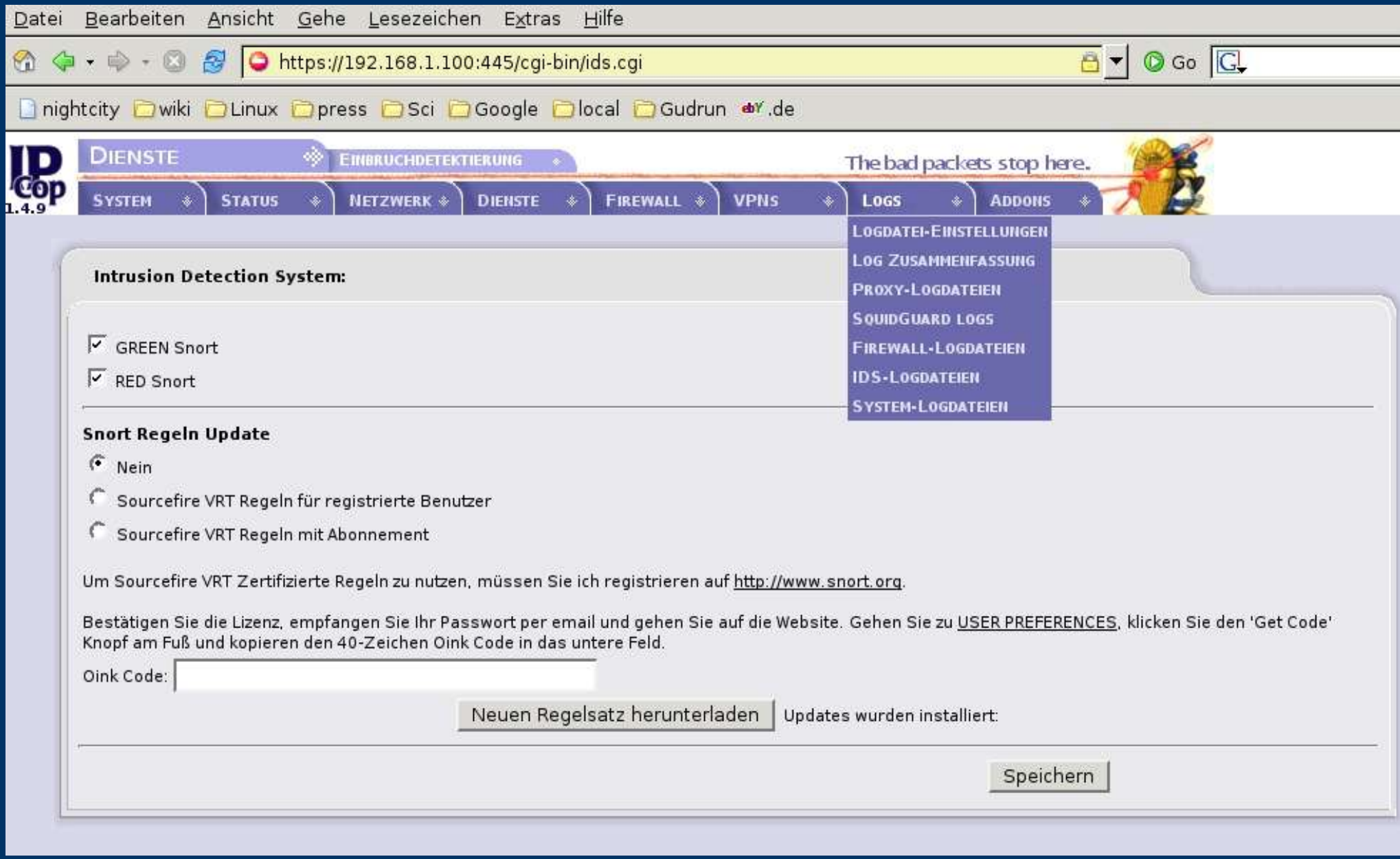


was sieht der Paketfilter?



Uhrzeit	Verknüpfung	Iface	Proto	Quelle	Quell-Port	MAC-Adresse	Ziel	Ziel-Port
19:46:38	INPUT	ppp0	TCP	213.7.251.6	2534	:::::	213.7.32.168	135(EPMAP)
19:46:38	INPUT	ppp0	TCP	213.7.210.87	1086	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:38	INPUT	ppp0	UDP	202.96.87.35	58646	:::::	213.7.32.168	1027
19:46:39	INPUT	ppp0	TCP	213.7.210.87	1117	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:39	INPUT	ppp0	TCP	213.7.130.47	2159	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:41	INPUT	ppp0	TCP	213.7.191.50	1380	:::::	213.7.32.168	139(NETBIOS-SSN)
19:46:42	INPUT	ppp0	TCP	213.7.130.47	2159	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:45	INPUT	ppp0	TCP	213.7.49.16	1691	:::::	213.7.32.168	135(EPMAP)
19:46:45	INPUT	ppp0	TCP	213.7.223.201	1789	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:48	INPUT	ppp0	TCP	213.7.223.201	1960	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:49	INPUT	ppp0	TCP	213.7.223.201	1789	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:52	INPUT	ppp0	TCP	213.7.223.201	1960	:::::	213.7.32.168	445(MICROSOFT-DS)
19:46:59	INPUT	ppp0	TCP	213.7.109.70	4757	:::::	213.7.32.168	445(MICROSOFT-DS)
19:47:02	INPUT	ppp0	UDP	221.6.163.50	54680	:::::	213.7.32.168	1026

SNORT Intrusion detection



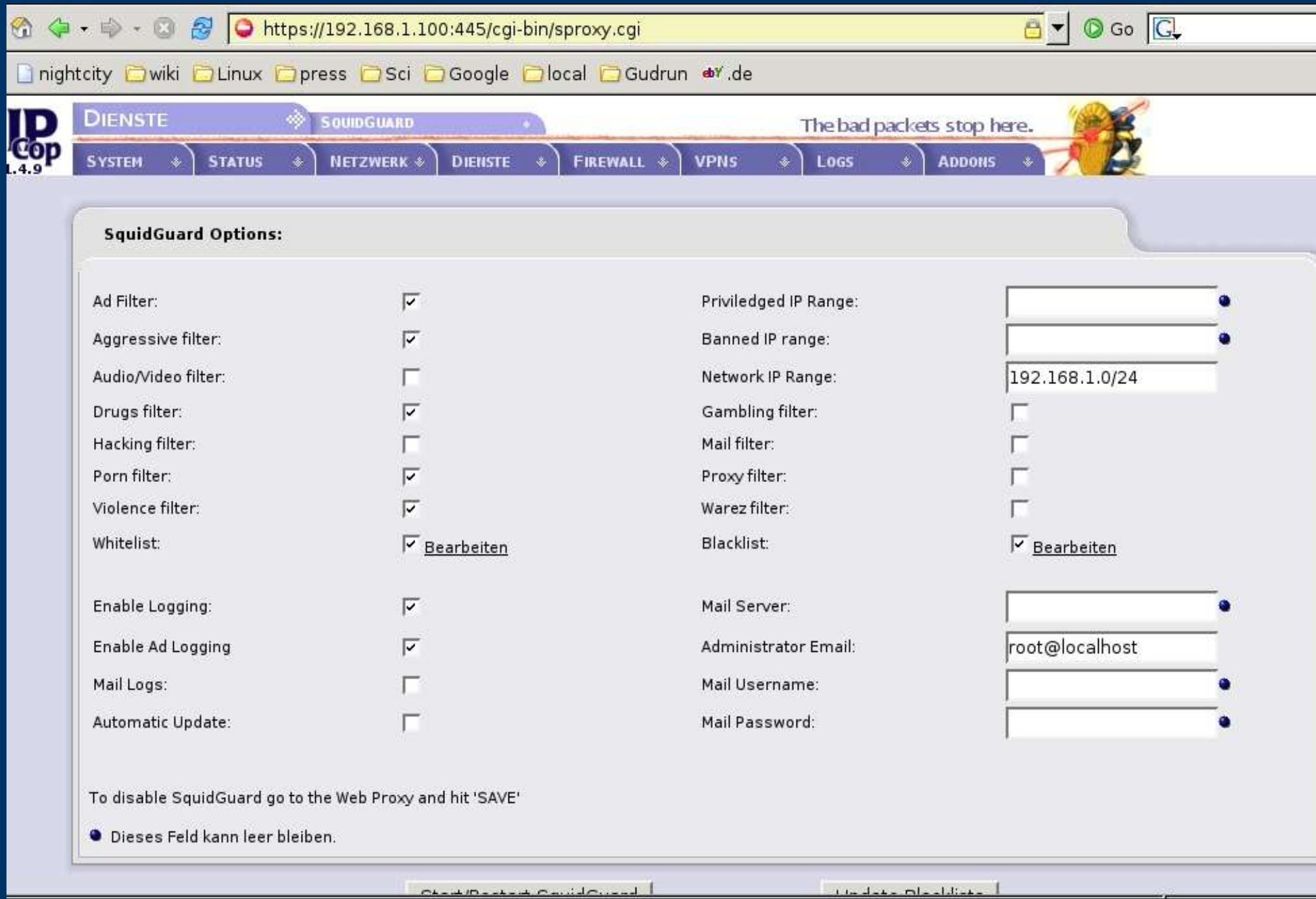
Addons

- addons: AddOn Server 2.3 zuerst installieren "tar xzvf name.tgz ...." und "./setup -i"
- danach *ausgewählte* Module z.B.: SquidGuard, DansGuardian, Midnight Commander 4.6.x, joe, procinfo, AutoShutDown, Rootkithunter, Nmap, etherwake (WOL), hping, ssh-client, LCD-proc (ähnlich lcdproc von fli4l), lanbackup, sarg, webalizer sftp, siriusadmin, tripwire ...
- bitte kein Samba, keine Spiele etc. (warum?)

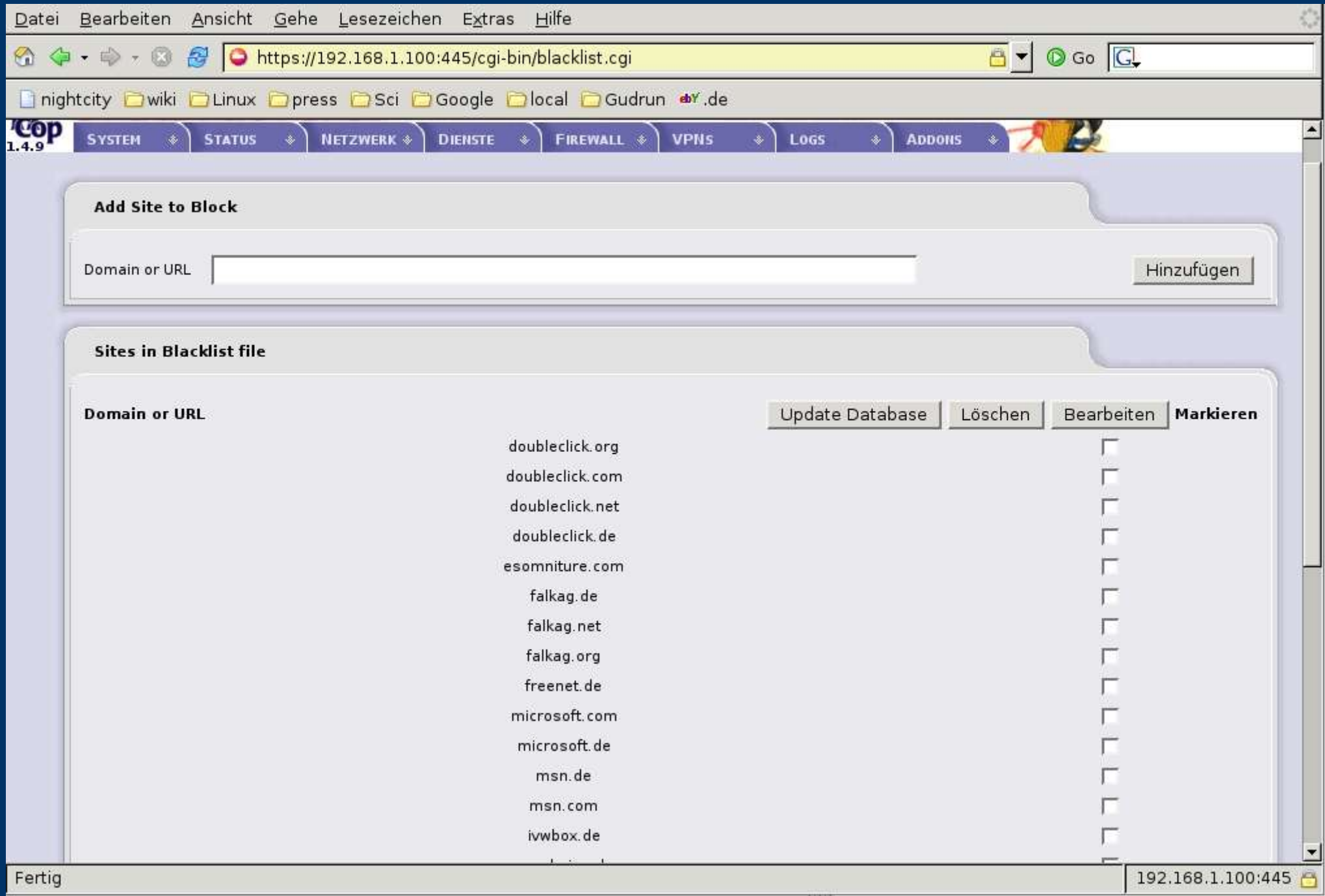
Beispiel – SquidGuard addon

- Squid im *transparenten Modus*?
- sollen ausgewählte Domains weggefiltert werden?
  mircosoft.com, msn.... yahoo, xy.doubleclick.net....
  werbeerfolgskontrolle.de...
- sollen ausgewählte URL-Bestandteile geblockt werden?
  xyz.de/banners/...*.gif .uni-koeln.de/grafik/.....

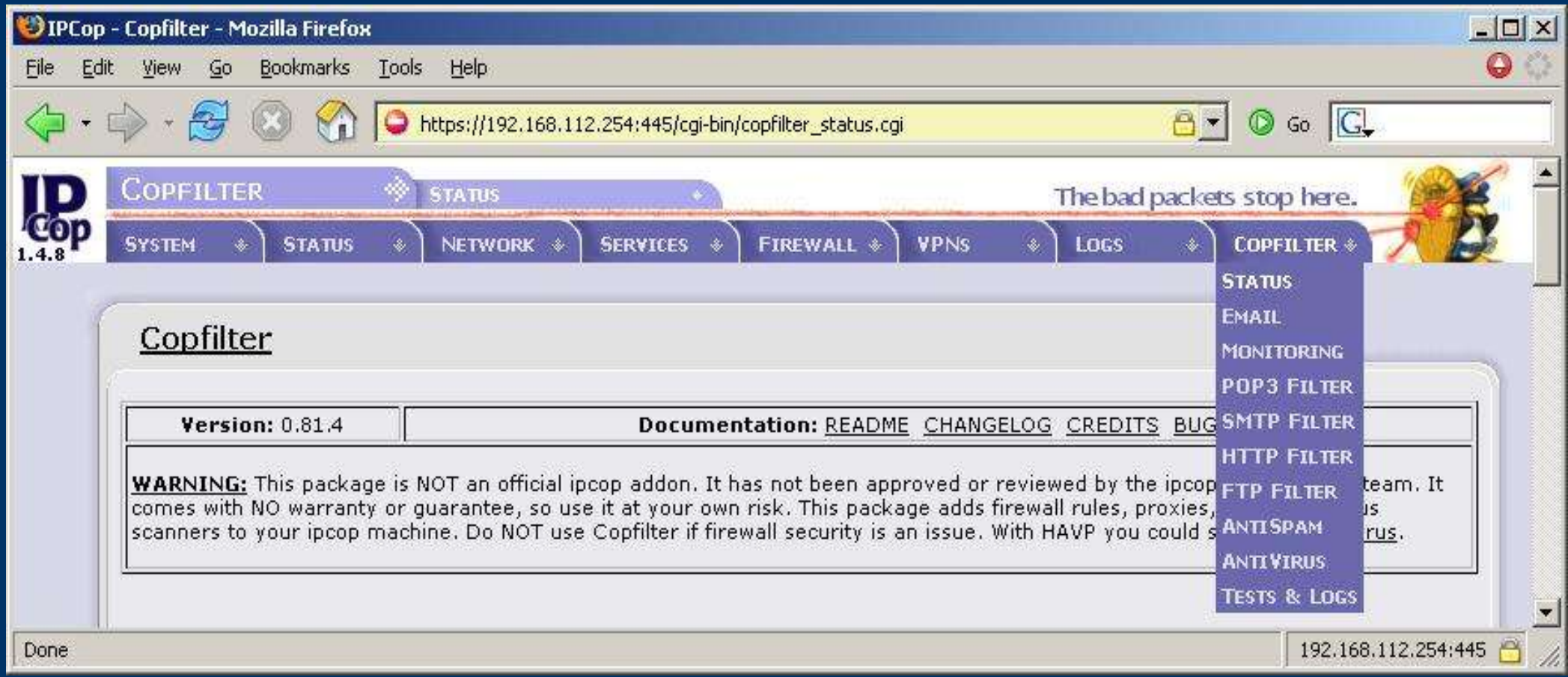
SquidGuard (1)



SquidGuard (2): *blacklist*



und noch'n Addon: URLfilter



Treffer, versenkt

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

http://www.freenet.de/customerindex.html

Go

nightcity wiki Linux press Sci Google local Gudrun .de

Laden... | 302 Access denied

Access to the page:

http://www.freenet.de/customerindex.html
... has been denied for the following reason:
blacklist

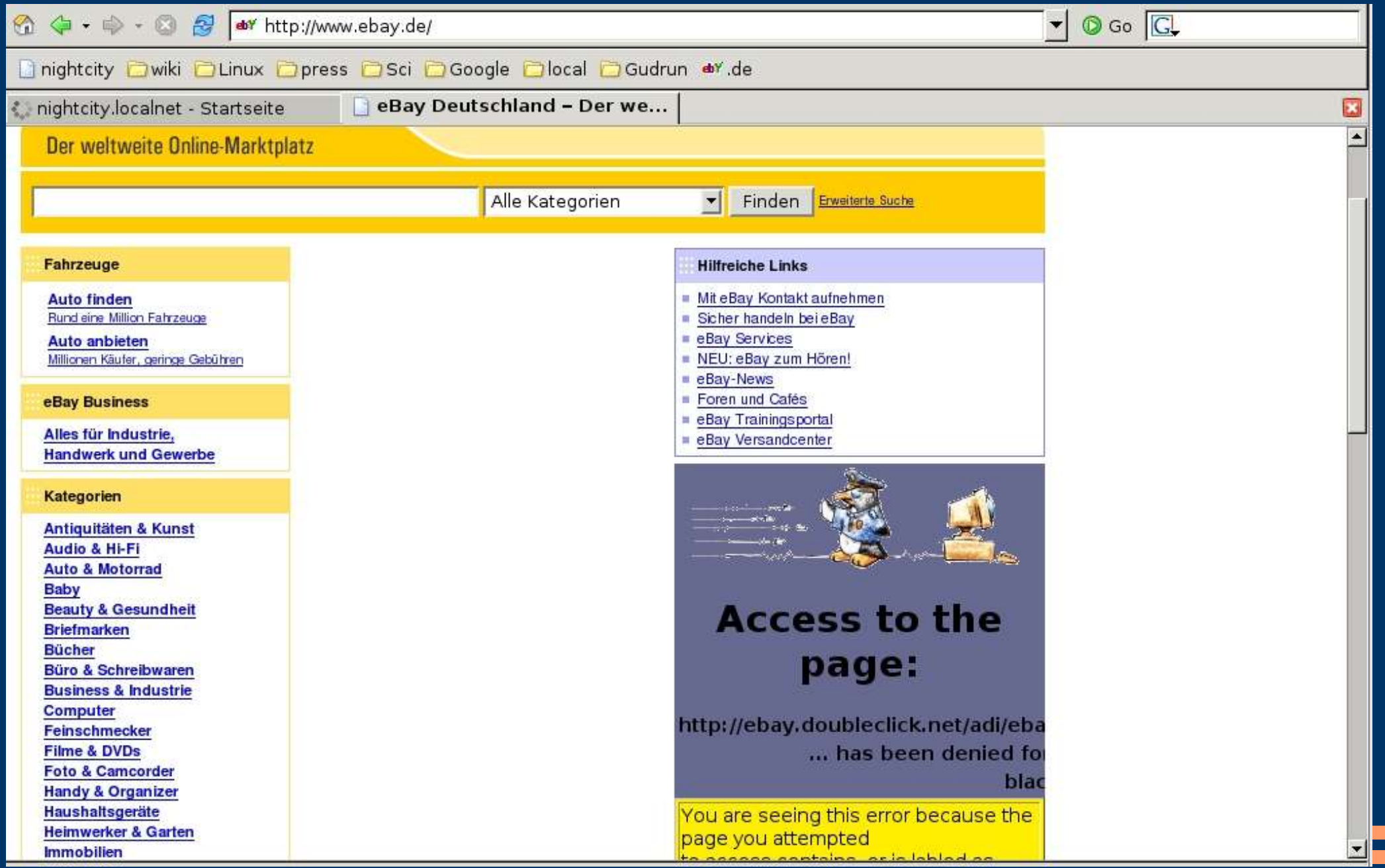
You are seeing this error because the page you attempted to access contains, or is labled as containing, material that has been deemed inappropriate.

If this is wrong, contact your
Network Administrator

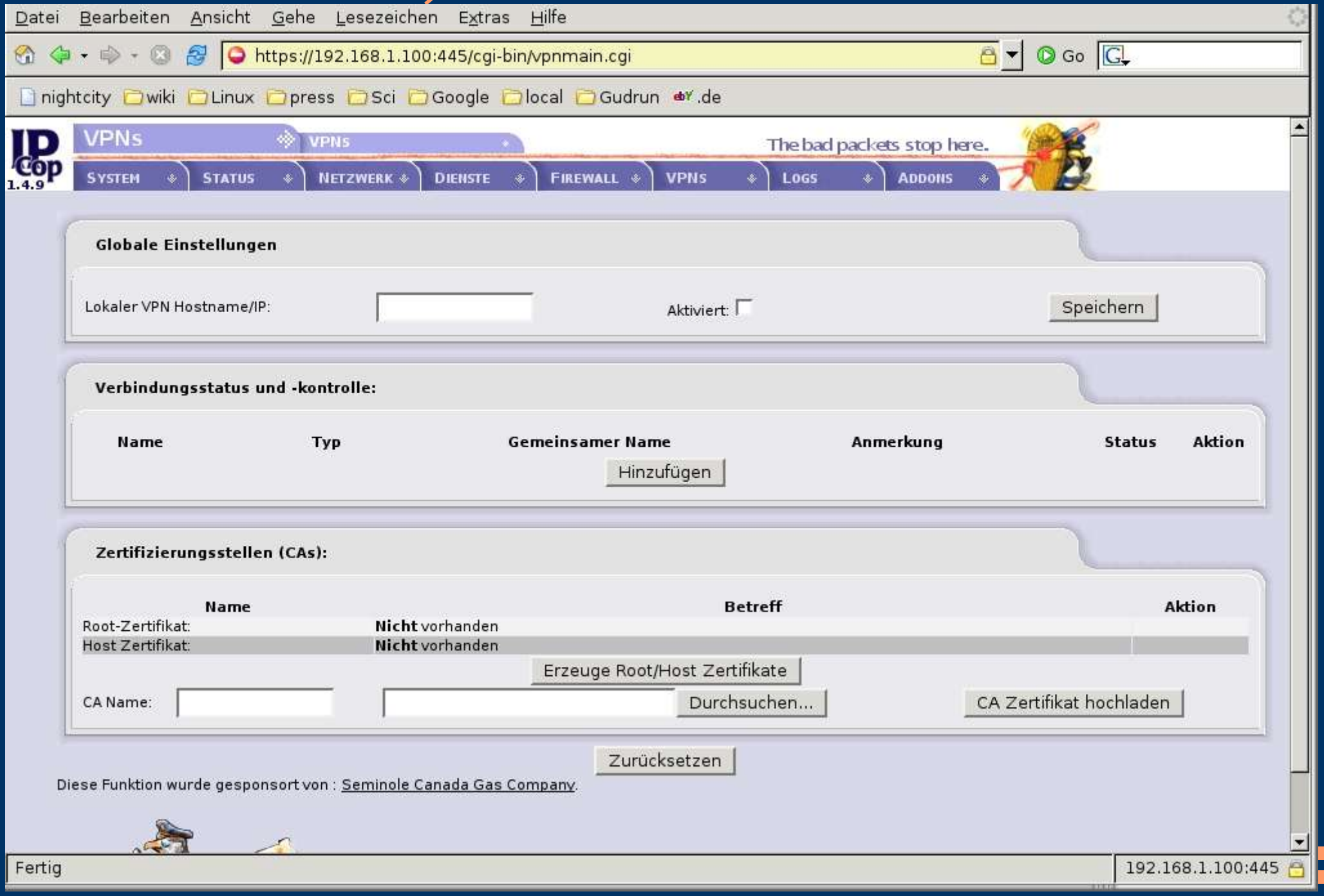
This site Protected by:

SquidGuard

URL-redirect: Treffer, auch versenkt



VPNs, IPsec mit 3DES...



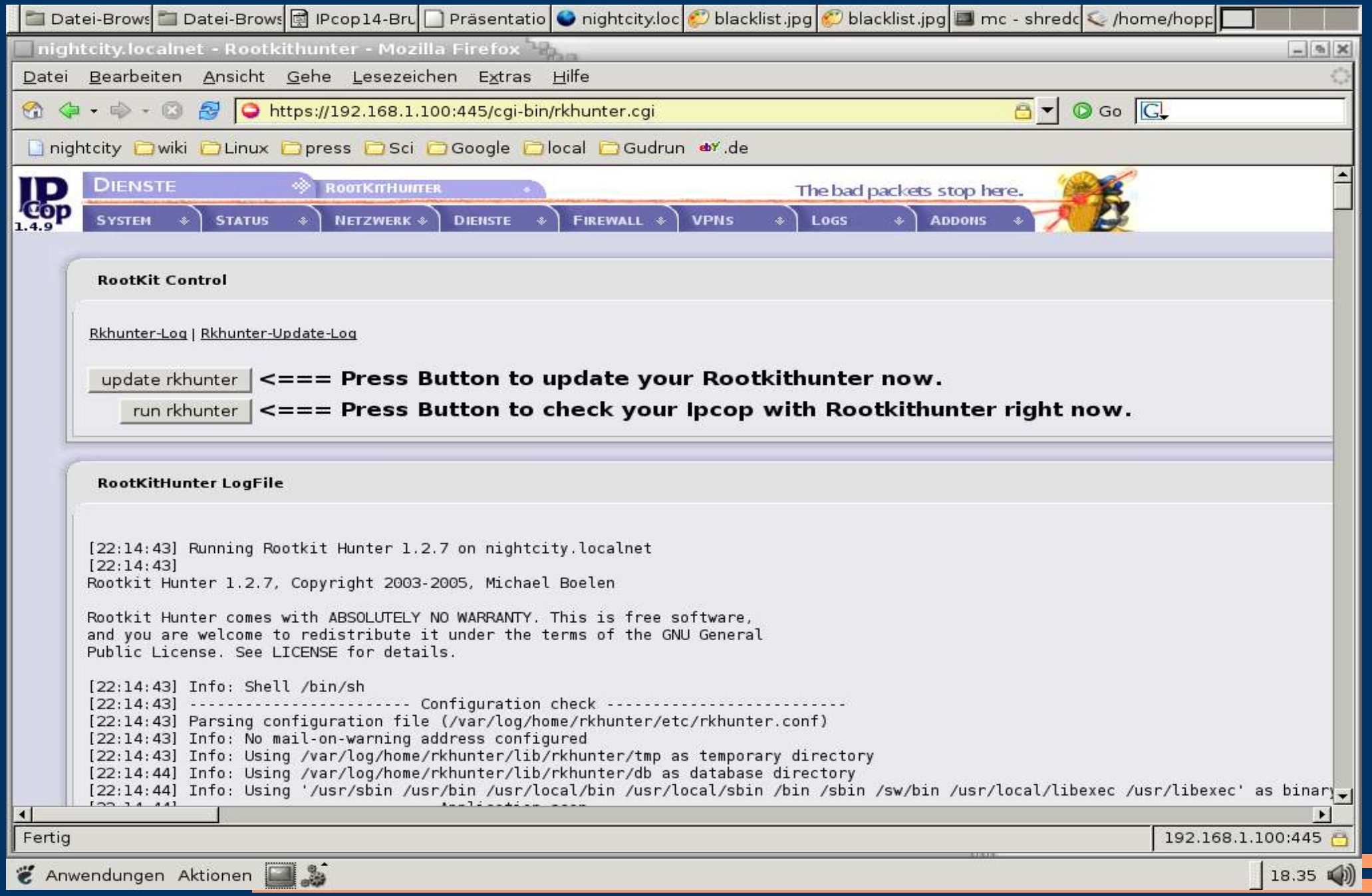
Warnung: Content filtern ist ....

nicht ganz einfach!

Im privaten Bereich ist der Einsatz von Squid, SquidGuard, ULRfilter etc. unproblematisch solange betroffene Anwender wissen, was da warum passiert.

Im kommerziellen/professionellen Umfeld fehlt die Voraussetzung: erschwerend kommen die Auflagen der Telekommunikations-gesetze, der TKÜV etc. zum Einsatz.
D.h. Anwender haben ein per Gesetz ein "Anrecht" auf SPAM, auf unbemerktes usertracking und Ausspioniertwerden wenn sie kranke Webseiten zwanghaft aufsuchen.
Wer dem nicht zustimmt, muss als Admin seine user und seinen Arbeitgeber "erziehen" - unternehmensweit etwa den IE verbieten (mit URLfilter möglich), Amazon und ebay von 8-17.00 Uhr verbieten etc.

Wem gehört mein Router?



Ruhe im Karton: Fazit rkh

[22:16:51] Scanning Bind%%DNS...
[22:16:51] Application not found
[22:16:51] ----------
[22:16:51] Scanning OpenSSL...
[22:16:51] /usr/bin/openssl found
[22:16:52] No information available. Unknown version number
[22:16:52] ----------
[22:16:52] Scanning PHP...
[22:16:52] Application not found
[22:16:52] ----------
[22:16:52] Scanning Procmail%%MTA...
[22:16:52] Application not found
[22:16:52] ----------
[22:16:52] Scanning ProFTPd...
[22:16:52] Application not found
[22:16:53] ----------
[22:16:53] Scanning OpenSSH...
[22:16:53] /usr/sbin/sshd found
[22:16:53] Version 3.9p1 is available in non-vulnerable group and seems to be OK!
[22:16:54] ---------- Security advisories ----------
[22:16:56] Info: Found no explicit values, but a default value of 'yes'
[22:16:56] Warning: root login possible. Change for your safety the 'PermitRootLogin'
[22:16:56] (into 'no') and use 'su -' to become root.
[22:16:59] Scanned for: 55808 Trojan - Variant A, AjaKit, aPa Kit, Apache Worm, Ambient (ark) Rootkit, Balaur Rootkit, BeastKit, beX2, BOBKit, CiNIK Worm (Slapper.B variant), Danny-Boy's Abuse Kit, Devil RootKit, Dica, Dreams Rootkit, Duarawkz, Flea Linux Rootkit, FreeBSD Rootkit, Fuck`it Rootkit, GasKit, Heroin LKM, HjC Kit, ignoKit, ImperalsS-FBRK, Irix Rootkit, Kitko, Knark, Li0n Worm, Lockit / LJK2, MRK, Ni0 Rootkit, RootKit for SunOS / NSDAP, Optic Kit (Tux), Oz Rootkit, Portacelo, R3dstorm Toolkit, RH-Sharpe's rootkit, RSHA's rootkit, Scalper Worm, Shutdown, SHV4, SHV5, Sin Rootkit, Slapper, Sneakin Rootkit, Suckit Rootkit, SunOS Rootkit, Superkit, TBD (Telnet BackDoor), TeLeKiT, T0rn Rootkit, Trojanit Kit, Tuxtendo, URK, VcKit, Volc Rootkit, X-Org SunOS Rootkit, zaRwT.KiT Rootkit

[22:17:00] 0 vulnerable applications found

geht's auch professioneller?

- Floppylaufwerk an Kinder/WinDAUs verschenken
- Verschenke Grafikkarte (nur für Installation benötigt) und (vorher!) Editieren der grub.conf
- Deaktiviere Swapfile (/etc/rc.d/rc.sysinit) und Anlegen von Swappartition möglichst auf zweiter HD
- kontrolliere HD-performance mit **hdparm -v /dev/hda**
- CD-LW im Karneval statt Kamelle werfen (filetransfers per scp)
- WRAP-Gehäuse - lüfterlos, klein+leise aber teuer
- bootfähiges FLASH-ROM (keine konventionelle HD) noch teurer
- hole neue Ideen aus der "Galerie" von www.ipcop-forum.de
- Einbau in Pappkarton, Videorekorder oder Bierfass
- Mitarbeit bei ipcop.org ?

References

http://www.ipcop.org/ # englisch

http://www.ipcop-forum.de/ # deutsch

http://prdownloads.sourceforge.net/ipcop/ # download

http://www.ipcop-forum.de/forum/index.php # Foren

http://www.tom-e.de/binary.html # binary add-on collection

http://www.routerdesign.com # noch mehr Designideen

bitte Dokumentation auf den Webseiten beachten:
VPN-over-Blue-HOWTO.

mehrere verwendete Grafiken wurden der IPcop Dokumentation entnommen!

Dieses Dokument wurde erstellt unter Mitwirkung freilaufender Pinguine aus art-gerechter IT-Haltung:

Debian GNU/Linux 3.1 mit OpenOffice, Firefox Browser und **IPcop Linux**