

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. Bisläng 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

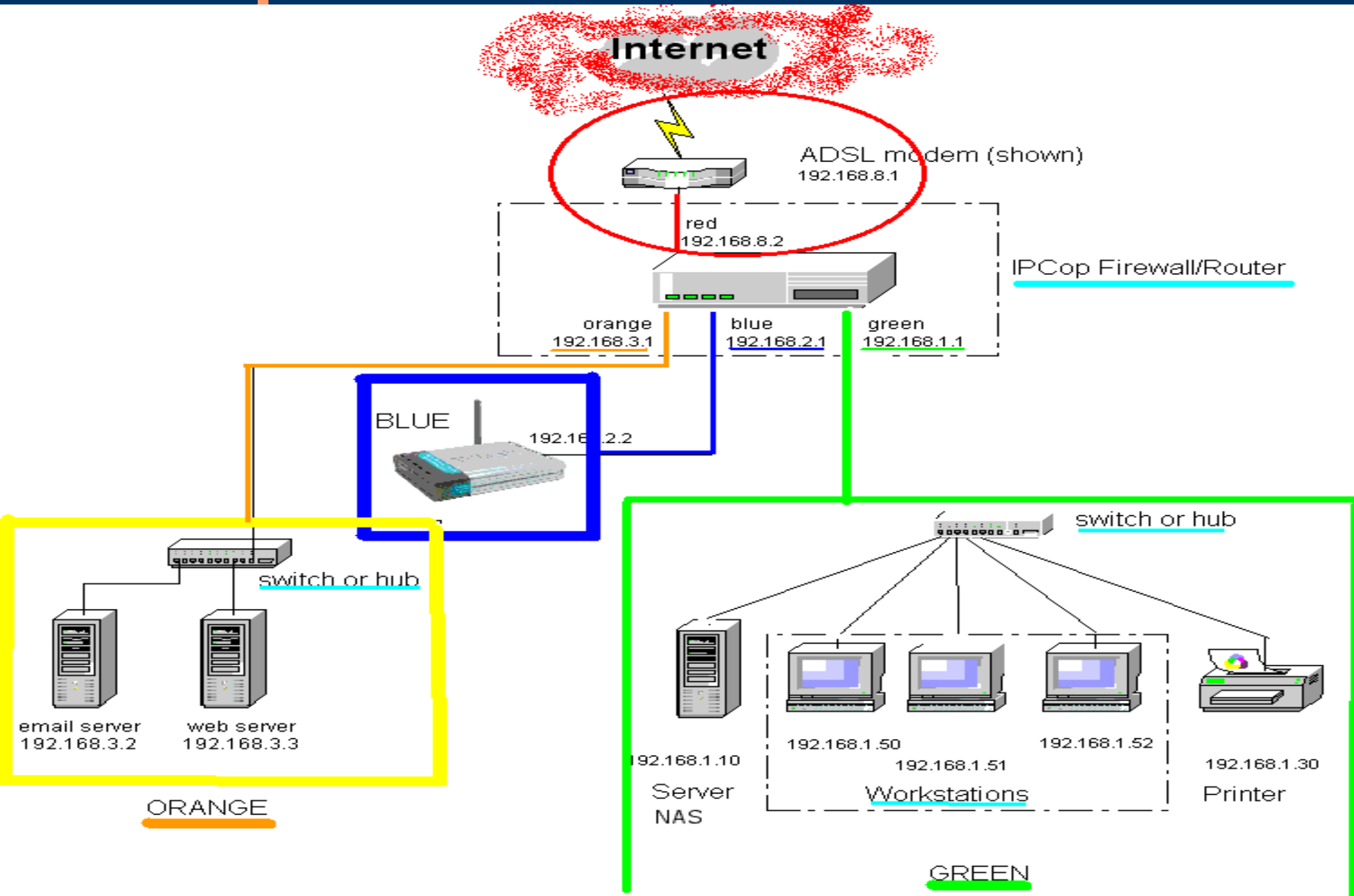
- Download des ca. 42 MB großen iso-images
 - von CD booten oder Startdiskette+ image von Webserver
 - hda wird **kpl** neu formatiert mit *ext3* (egal ob 500 MB oder 10 GB - Partitionierung nicht beeinflussbar)
 - 486/DX2 mit 16 MB mindestens, 586 (Pentium1)+ 64 MB erlaubt normales Arbeiten - abhängig 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

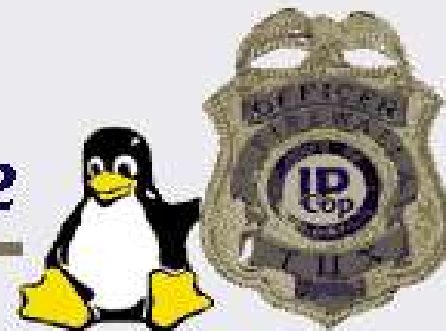
GNU GRUB version 0.95 (638K lower / 804800K upper memory)

```
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.

**IP
Cop**

The Bad Packets Stop Here



- 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



und wie wird ausgeschaltet?

The screenshot displays the IP Cop 1.4.9 web interface. The top navigation bar includes the IP Cop logo and version number (1.4.9) on the left, and the slogan "The bad packets stop here." with a cartoon character on the right. The main navigation menu contains several items: SYSTEM (highlighted with a red circle), STATUS, NETZWERK, DIENSTE, FIREWALL, VPNS, LOGS, and ADDONS. The "SYSTEM" menu is currently selected, showing a sub-menu with the option "HERUNTERFAHREN". Below the navigation bar, the "Herunterfahren:" section contains two buttons: "Neustart" (Restart) and "Herunterfahren" (Shutdown).

erst Mal SSH ...

nightcity.localnet - Fernwartung - Mozilla Firefox

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

nightcity wiki Linux press Sci Google local Gudrun .de

IP Cop 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

Fertig

17:38:17 up 24 min, 1 user, load average: 0.01, 0.01, 0.00

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

nightcity.localnet - Webproxy-Konfiguration - Mozilla Firefox

Datei Bearbeiten Ansicht Gehe Lesezeichen Extras Hilfe

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

nightcity wiki Linux press Sci Google local Gudrun .de

IP Cop 1.4.9

DIENSTE **PROXY** The bad packets stop here.

SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS

Web-Proxy:

Aktiviert auf Green:

Transparent auf Green:

Log aktiviert:

Vorgelagerter Proxy (hostname:port):

Proxy-Benutzername:

Proxy-Passwort:

Proxy-Port:

Cache Verwaltung

Cache-Größe (MB):

Min. Objektgröße (kB):

Max. Objektgröße (kB):

Transferbeschränkungen

Max. eingehende Größe (kB):

Max. abgehende Größe (kB):

Dieses Feld kann leer bleiben.

Zwischenspeicher löschen Speichern

wohin verbindet sich der Router?

The screenshot shows a Linux desktop environment with a taskbar at the top containing several open applications: 'Datei-Browser: ij', 'Datei-Browser: II', 'IPcop14-Bruno.s', 'Präsentation', 'nightcity.localnet', 'KolourPaint', and 'mc - shredder:~'. The main window is Mozilla Firefox, displaying the IPCop web interface for PPP settings. The browser's address bar shows the URL 'https://192.168.1.100:445/cgi-bin/pppsetup.cgi'. The IPCop interface has a navigation menu with 'NETZWERK' selected, and a sub-menu with 'EINWAHL'. The main content area is titled 'Profile:' and shows a dropdown menu for 'Profil:' with '1.' selected. Below this are buttons for 'Auswählen', 'Löschen', and 'Wiederherstellen'. The 'Verbindung:' section includes a dropdown for 'Schnittstelle:' set to 'Modem', a button for 'Aktualisieren', and a text field for 'USB:' set to 'usb-uhci'. Further down, there are fields for 'Schnittstelle:' (set to 'Modem an COM1'), 'Übertragungsrate zwischen Computer und Modem:' (set to '115200'), 'Nummer:', 'Wählmodus:' (set to 'Ton'), 'Modemlautsprecher an:' (checkbox), 'ISP verlangt Zeilenrücklaufzeichen:' (checkbox), 'Leerlauf-Wartezeit in min (0 zum Deaktivieren):' (set to '5'), 'Verbinden bei IPCop-Neustart' (checkbox), and 'Verbindungs-Debugging:' (checkbox). The 'Wiederverbindung:' section has radio buttons for 'Manuell', 'Dauerhaft', and 'Dial-on-Demand-Modus' (selected), a text field for 'Holdoff-Zeit in (Sekunden):' (set to '45'), and a dropdown for 'Falls die Wiederverbindung scheitert, auf Profil umschalten:' (set to '1.'). Other options include 'Dial-on-Demand für DNS:' (checkbox, checked) and 'Maximale Wiederholversuche:' (set to '2'). The bottom status bar shows 'Fertig' on the left, the IP address '192.168.1.100:445' on the right, and system icons for 'Anwendungen', 'Aktionen', and a clock showing '18.08'.

was sieht der Paketfilter?

https://192.168.1.100:445/cgi-bin/logs.cgi/firewalllog.dat

nightcity wiki Linux press Sci Google local

IP Cop 1.4.9

LOGS FIREWALL-LOGDATEIEN The bad packets stop here.

SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS

Konfiguration:

Monat: Januar Tag: 5 << >> Aktualisieren Export

Protokoll:

Gesamtanzahl der Firewall-Treffer für Januar 05, 2006: 438

Uhrzeit	Verknüpfung	Älter Iface	Proto	Quelle	Quell-Port	MAC-Adresse	Neuer 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

File Edit View Go Search Extras Help

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

nightcity wiki Linux press Sci Google local Gudrun .de

IP Cop 1.4.9

DIENTE **EINBRUCHDETEKTIERUNG** The bad packets stop here. 

SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS

Intrusion Detection System:

GREEN Snort
 RED Snort

Snort Regeln Update

Nein
 Sourcefire VRT Regeln für registrierte Benutzer
 Sourcefire VRT Regeln mit Abonnement

Um Sourcefire VRT Zertifizierte Regeln zu nutzen, müssen Sie sich registrieren auf <http://www.snort.org>.

Bestätigen Sie die Lizenz, empfangen Sie Ihr Passwort per email und gehen Sie auf die Website. Gehen Sie zu [USER PREFERENCES](#), klicken Sie den 'Get Code' Knopf am Fuß und kopieren den 40-Zeichen Oink Code in das untere Feld.

Oink Code:

Updates wurden installiert:

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?
microsoft.com, msn.... yahoo, xy.doubleclick.net....
werbeerfolgskontrolle.de...
- sollen ausgewählte URL-Bestandteile geblockt werden?
xyz.de/**banners**/...*.gif .uni-koeln.de/**grafik**/.....

SquidGuard (1)

Browser address bar: <https://192.168.1.100:445/cgi-bin/sproxy.cgi>

Navigation: nightcity | wiki | Linux | press | Sci | Google | local | Gudrun | .de

IP Cop 1.4.9 | DIENSTE | **SQUIDGUARD** | The bad packets stop here. | 

SYSTEM | STATUS | NETZWERK | DIENSTE | FIREWALL | VPNS | LOGS | ADDONS

SquidGuard Options:

Ad Filter:	<input checked="" type="checkbox"/>	Privileged IP Range:	<input type="text"/>
Aggressive filter:	<input checked="" type="checkbox"/>	Banned IP range:	<input type="text"/>
Audio/Video filter:	<input type="checkbox"/>	Network IP Range:	192.168.1.0/24
Drugs filter:	<input checked="" type="checkbox"/>	Gambling filter:	<input type="checkbox"/>
Hacking filter:	<input type="checkbox"/>	Mail filter:	<input type="checkbox"/>
Porn filter:	<input checked="" type="checkbox"/>	Proxy filter:	<input type="checkbox"/>
Violence filter:	<input checked="" type="checkbox"/>	Warez filter:	<input type="checkbox"/>
Whitelist:	<input checked="" type="checkbox"/> Bearbeiten	Blacklist:	<input checked="" type="checkbox"/> Bearbeiten
Enable Logging:	<input checked="" type="checkbox"/>	Mail Server:	<input type="text"/>
Enable Ad Logging:	<input checked="" type="checkbox"/>	Administrator Email:	root@localhost
Mail Logs:	<input type="checkbox"/>	Mail Username:	<input type="text"/>
Automatic Update:	<input type="checkbox"/>	Mail Password:	<input type="text"/>

To disable SquidGuard go to the Web Proxy and hit 'SAVE'

Dieses Feld kann leer bleiben.

Start/Restart SquidGuard | Update Blacklists

SquidGuard (2): *blacklist*

The screenshot shows a web browser window with the address bar containing `https://192.168.1.100:445/cgi-bin/blacklist.cgi`. The browser's address bar also shows a search bar with the text "Go" and a magnifying glass icon. Below the address bar, there is a navigation menu with several tabs: "nightcity", "wiki", "Linux", "press", "Sci", "Google", "local", "Gudrun", and ".de".

The main content area of the browser displays the SquidGuard web interface. At the top left, there is a logo for "Cop 1.4.9". To the right of the logo is a navigation menu with tabs: "SYSTEM", "STATUS", "NETZWERK", "DIENSTE", "FIREWALL", "VPNS", "LOGS", and "ADDONS".

The main content area is divided into two sections:

- Add Site to Block:** This section contains a text input field labeled "Domain or URL" and a button labeled "Hinzufügen".
- Sites in Blacklist file:** This section contains a table with the following columns: "Domain or URL", "Update Database", "Löschen", "Bearbeiten", and "Markieren". The table lists several domains, each with a corresponding checkbox in the "Markieren" column.

The table data is as follows:

Domain or URL	Update Database	Löschen	Bearbeiten	Markieren
doubleclick.org				<input type="checkbox"/>
doubleclick.com				<input type="checkbox"/>
doubleclick.net				<input type="checkbox"/>
doubleclick.de				<input type="checkbox"/>
esomniture.com				<input type="checkbox"/>
falkag.de				<input type="checkbox"/>
falkag.net				<input type="checkbox"/>
falkag.org				<input type="checkbox"/>
freenet.de				<input type="checkbox"/>
microsoft.com				<input type="checkbox"/>
microsoft.de				<input type="checkbox"/>
msn.de				<input type="checkbox"/>
msn.com				<input type="checkbox"/>
ivwbox.de				<input type="checkbox"/>

At the bottom of the browser window, the status bar shows "Fertig" on the left and "192.168.1.100:445" on the right.

und noch'n Addon: URLfilter

IPCop - Copfilter - Mozilla Firefox

File Edit View Go Bookmarks Tools Help

https://192.168.112.254:445/cgi-bin/copfilter_status.cgi

IPCop 1.4.8

COPFILTER STATUS

The bad packets stop here.

SYSTEM STATUS NETWORK SERVICES FIREWALL VPNS LOGS COPFILTER

Copfilter

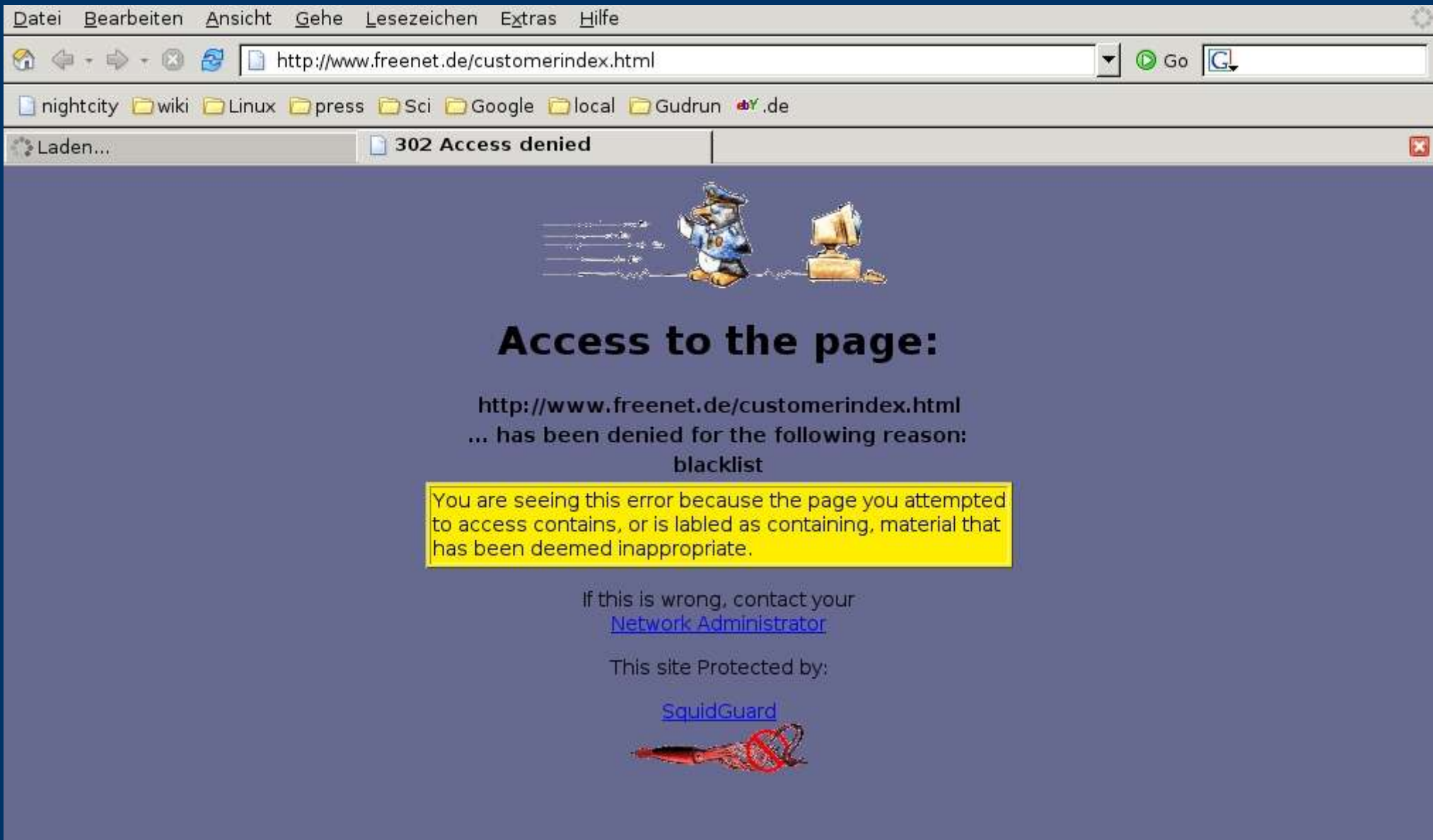
Version: 0.81.4 Documentation: [README](#) [CHANGELOG](#) [CREDITS](#) [BUGS](#)

WARNING: This package is NOT an official ipcop addon. It has not been approved or reviewed by the ipcop team. It comes with NO warranty or guarantee, so use it at your own risk. This package adds firewall rules, proxies, scanners to your ipcop machine. Do NOT use Copfilter if firewall security is an issue. With HAVP you could s...

STATUS
EMAIL
MONITORING
POP3 FILTER
SMTP FILTER
HTTP FILTER
FTP FILTER
ANTISPAM
ANTIVIRUS
TESTS & LOGS

Done 192.168.112.254:445

Treffer, versenkt




The screenshot shows a web browser window with the address bar containing `http://www.freenet.de/customerindex.html`. The browser's status bar indicates a `302 Access denied` error. The main content area features a cartoon illustration of a squid-like character standing next to a computer monitor. Below the illustration, the text reads: **Access to the page:**
`http://www.freenet.de/customerindex.html`
... has been denied for the following reason:
blacklist

A yellow highlighted box contains the following text: "You are seeing this error because the page you attempted to access contains, or is labled as containing, material that has been deemed inappropriate."

Below the highlighted box, the text says: "If this is wrong, contact your [Network Administrator](#)".

Further down, it states: "This site Protected by: [SquidGuard](#)".



URL-redirect: Treffer, auch versenkt

The screenshot shows a web browser window with the address bar containing `http://www.ebay.de/`. The browser's address bar also shows a search icon, a 'Go' button, and a search input field. The browser's tab bar shows two tabs: 'nightcity.localnet - Startseite' and 'eBay Deutschland - Der we...'. The main content area of the browser displays the eBay Germany homepage. The page has a yellow header with the text 'Der weltweite Online-Marktplatz'. Below the header is a search bar with a dropdown menu set to 'Alle Kategorien', a 'Finden' button, and a link to 'Erweiterte Suche'. The page is divided into several sections: 'Fahrzeuge' with links for 'Auto finden' and 'Auto anbieten'; 'eBay Business' with a link for 'Alles für Industrie, Handwerk und Gewerbe'; and 'Kategorien' with a list of various product categories. On the right side, there is a 'Hilfreiche Links' section with several links. A large error message is overlaid on the right side of the page, featuring a cartoon dog and a computer monitor. The error message reads: 'Access to the page: http://ebay.doubleclick.net/adi/eba... has been denied for black'. Below the error message, a yellow box contains the text: 'You are seeing this error because the page you attempted to access contains or is labeled as'.

Der weltweite Online-Marktplatz

Alle Kategorien Finden [Erweiterte Suche](#)

Fahrzeuge

- [Auto finden](#)
Rund eine Million Fahrzeuge
- [Auto anbieten](#)
Millionen Käufer, geringe Gebühren

eBay Business

- [Alles für Industrie, Handwerk und Gewerbe](#)

Kategorien

- [Antiquitäten & Kunst](#)
- [Audio & Hi-Fi](#)
- [Auto & Motorrad](#)
- [Baby](#)
- [Beauty & Gesundheit](#)
- [Briefmarken](#)
- [Bücher](#)
- [Büro & Schreibwaren](#)
- [Business & Industrie](#)
- [Computer](#)
- [Feinschmecker](#)
- [Filme & DVDs](#)
- [Foto & Camcorder](#)
- [Handy & Organizer](#)
- [Haushaltsgeräte](#)
- [Heimwerker & Garten](#)
- [Immobilien](#)

Hilfreiche Links

- [Mit eBay Kontakt aufnehmen](#)
- [Sicher handeln bei eBay](#)
- [eBay Services](#)
- [NEU: eBay zum Hören!](#)
- [eBay-News](#)
- [Foren und Cafés](#)
- [eBay Trainingsportal](#)
- [eBay Versandcenter](#)

Access to the page:

`http://ebay.doubleclick.net/adi/eba`
... has been denied for black

You are seeing this error because the page you attempted to access contains or is labeled as

VPNs, IPsec mit 3DES...

File Edit View Go Bookmarks Extras Help

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

nightcity wiki Linux press Sci Google local Gudrun .de

IP Cop 1.4.9

VPNs

The bad packets stop here.

- SYSTEM
- STATUS
- NETZWERK
- DIENSTE
- FIREWALL
- VPNS
- LOGS
- ADDONS

Globale Einstellungen

Lokaler VPN Hostname/IP: Aktiviert:

Verbindungsstatus und -kontrolle:

Name	Typ	Gemeinsamer Name	Anmerkung	Status	Aktion
<input type="button" value="Hinzufügen"/>					

Zertifizierungsstellen (CAs):

Name	Betreff	Aktion
Root-Zertifikat:	Nicht vorhanden	
Host Zertifikat:	Nicht vorhanden	

CA Name:

Diese Funktion wurde gesponsort von : [Seminole Canada Gas Company](#).

Fertig 192.168.1.100:445

Warnung: Content filtern ist ... nicht ganz einfach!

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

Im kommerziellen/professionellen Umfeld fehlt die Voraussetzung: erschwerend kommen die Auflagen der Telekommunikationsgesetze, 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?

nightcity.localnet - Rootkithunter - Mozilla Firefox

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

nightcity wiki Linux press Sci Google local Gudrun .de

IP Cop 1.4.9 DIENSTE **ROOTKITHUNTER** The bad packets stop here.

SYSTEM STATUS NETZWERK DIENSTE FIREWALL VPNS LOGS ADDONS

RootKit Control

[Rkhunter-Log](#) | [Rkhunter-Update-Log](#)

<=== Press Button to update your Rootkithunter now.

<=== Press Button to check your Ipcop with Rootkithunter right now.

RootKitHunter LogFile

```
[22:14:43] Running Rootkit Hunter 1.2.7 on nightcity.localnet
[22:14:43]
Rootkit Hunter 1.2.7, Copyright 2003-2005, Michael Boelen

Rootkit Hunter comes with ABSOLUTELY NO WARRANTY. This is free software,
and you are welcome to redistribute it under the terms of the GNU General
Public License. See LICENSE for details.

[22:14:43] Info: Shell /bin/sh
[22:14:43] ----- Configuration check -----
[22:14:43] Parsing configuration file (/var/log/home/rkhunter/etc/rkhunter.conf)
[22:14:43] Info: No mail-on-warning address configured
[22:14:43] Info: Using /var/log/home/rkhunter/lib/rkhunter/tmp as temporary directory
[22:14:44] Info: Using /var/log/home/rkhunter/lib/rkhunter/db as database directory
[22:14:44] Info: Using '/usr/sbin /usr/bin /usr/local/bin /usr/local/sbin /bin /sbin /sw/bin /usr/local/libexec /usr/libexec' as binary
[22:14:44] Application scan
```

Fertig 192.168.1.100:445

Anwendungen Aktionen 18.35

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 artgerechter IT-Haltung:

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