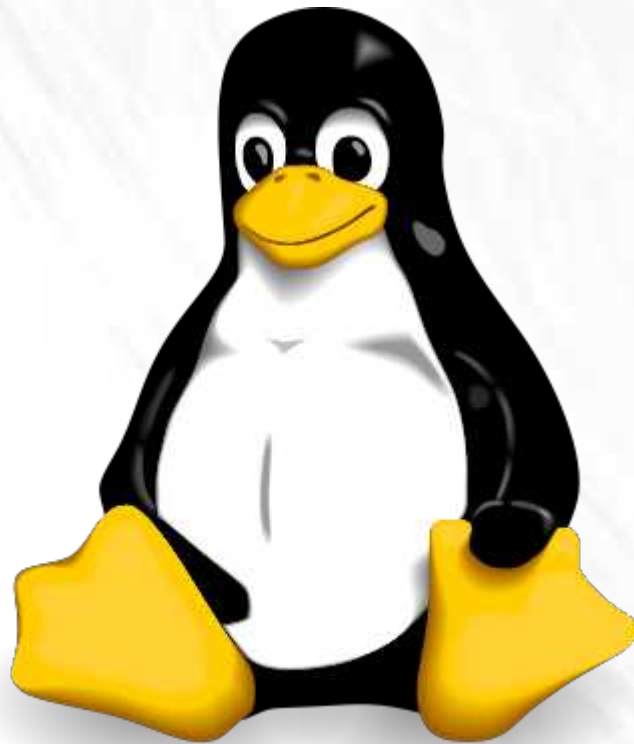


SLT - Schwabacher Linuxtage 2009

IP-COP "The bad packets stop here"

Firewall auf Linuxbasis



**IP
Cop**

IP-COP "The bad packets stop here"

Zusammenfassung Teil 1

- Was ist IP-COP?
- Warum IP-COP?
- Hardwarevoraussetzungen
- Konzept von IP-COP
- Installation Schritt für Schritt
- Erster Start



IP-COP "The bad packets stop here"

Zusammenfassung Teil 2

- Einstellungen
- Addons / Erweiterungen
- Fazit (Vorteile / Nachteile)
- Alternativen
- Zukunftsaussichten
- Webadressen

The logo for IP Cop, featuring the letters 'IP' in a large, bold, dark blue serif font above the letters 'Cop' in a smaller, bold, dark blue serif font. The 'C' and 'o' in 'Cop' are connected, and the 'p' has a long descender.

IP-COP "The bad packets stop here"

Was ist IP-COP?

"Eine Firewall. Nicht mehr und auch nicht weniger."

- Komplette Linux Distribution wie z.B. Debian oder Ubuntu
- Abspaltung des „Smoothwall“ Projektes
- Grafische Oberfläche über den Webbrowser
- Einfache Konfiguration
- Vielseitig erweiterbar
- Sehr viele Infos im Internet verfügbar

IP-COP "The bad packets stop here"

Warum IP-COP?

- Der Mann auf der Autobahn
- Wann erfolgen die ersten Angriffe? Wieviel ca. Pro Stunde?
- Schutz vor Angriffen von Aussen
- Schutz vor Angriffen von Innen (z.B. Firmennetzwerke)
- Trennung von LAN / WAN / W-Lan / DMZ
- Durch aktive Community schnelle Reaktionen auf Sicherheitsluecken

IP-COP "The bad packets stop here"

Hardwarevoraussetzungen

- PC ab Pentium 1 (besser PII oder PIII)
- Mindestens 64 MB RAM (besser mehr)
- Festplatte zwischen 3 – 80 GB
- CD ROM/DVD ROM, Monitor, Tastatur, Grafikkarte
(nur zur Installation)
- Floppy Laufwerk zur Datensicherung

IP-COP "The bad packets stop here"

Konzept von IP-COP

Farbliche Unterschiede der einzelnen Netzwerksegmente

Rot	Das unsichere Internet (WAN)
Grün	Das interne Netz (LAN)
Blau	Das W-Lan Netz
Orange	DMZ z.b. Webserver, Mailserver, usw.
Grau	Zusätzliches selbst definierbares Segment

IP-COP "The bad packets stop here"

Erster Start / Grub-Bootmenue

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



IP-COP "The bad packets stop here"

Startseite IP-COP



The screenshot displays the IP-COP web interface. At the top left is the IP-COP logo with version 1.4.15. The main navigation bar includes tabs for SYSTEM, STARTSEITE (selected), STATUS, NETZWERK, DIENSTE, FIREWALL, VPNS, and LOGS. A slogan "The bad packets stop here." is visible on the right. The main content area shows the domain "ipcop.localdomain" and three buttons: "Verbinden", "Trennen", and "Aktualisieren". Below these buttons, the current profile is identified as "Aktuelles Profil: DSL einwahl" with the connection name "Leerlauf - DSL einwahl". A system update notification states: "1. Ihre Update-Datei ist 64d 16h 15m 19s Tage alt. Wir empfehlen Ihnen, Ihr System über die 'Updates'-Seite zu aktualisieren." At the bottom, system statistics are shown: "17:51:45 up 11 min, 1 user, load average: 0.14, 0.15, 0.09".

IP-COP "The bad packets stop here"

Einstellungen: System/Status

- System
- Updates einspielen
- Passwoerter aendern
- SSH Zugriff auf IP-COP
- Datensicherung
- Herunterfahren (auch zeitgesteuert moeglich)
- Status
- Diagramme für System, Netzwerk und Proxy

IP-COP "The bad packets stop here"

Einstellungen: Netzwerk/Dienste

- Netzwerk
- Einwahl ins Internet
- Hochladen von Daten
- Dienste
- Proxy / Dyn DNS
- Zeitserver (NTP Network Time Protocol)
- Traffic Shaping
- IDS Intrusion Detection System (Einbruchserkennung)

IP-COP "The bad packets stop here"

Einstellungen: Firewall / VPNs

- Firewall
- Port Weiterleitungen
- Externer Zugang (auf den IP-COP)
- Zugriff auf „Blau“
- Firewall Optionen
- VPNs
- Einstellungen für VPN Verbindungen

IP-COP "The bad packets stop here"

Einstellungen: Logs (Logdateien)

- Logs (**sehr wichtig**)
- Logdatei Einstellungen
- Log Zusammenfassung
- Proxy Logdateien
- Firewall Logdateien
- IDS Logdateien
- System Logdateien
- usw.

IP-COP “The bad packets stop here”

Addons / Erweiterungen

- Etwa 200 verschiedene Addons verfügbar
- Sinnvolle Addons sind z.B. Advanced Proxy, URL-Filter, BOT (Block Out Traffic) und Zerina (Open VPN)
- Je mehr Erweiterungen, desto unsicherer wird das System
- Es sollten nur die unbedingt benötigten Addons installiert werden
- Die Installation erfolgt über ssh / scp Zugriff auf den IP-COP

IP-COP "The bad packets stop here"

Zugriff per ssh

Zugriff auf den IP-COP per ssh (Secure Shell)

```
#ssh -p 222 root@192.168.x.x
```

Wichtig! IP-COP verwendet fuer ssh Port **222** statt **22**

Kopieren per scp

```
#scp -P 222 /home/Ben./Verz./...tar.gz root@192.168.x.x:/tmp
```

IP-COP "The bad packets stop here"

Installation der Addons

```
#ssh -p 222 root@192.168.x.x
```

```
#cd /tmp
```

```
#ls (nach Bezeichnung des Addons suchen)
```

```
#tar -xvfz .....tar.gz
```

```
#ls (neues entpacktes Verzeichnis suchen)
```

```
#cd (in neues entpacktes Verzeichnis wechseln)
```

```
#./install (teilweise auch ./install -i wird aber angegeben)
```


IP-COP "The bad packets stop here"

Sinnvolle Addons

- Advanced Proxy (Erweiterter Proxyserver, top konfigurierbar)
- URL Filter (z.B. fuer Kinder diverse Webseiten sperren)
- BOT – Block out traffic (Ausgehenden Verkehr regeln)
- ZERINA (Open VPN fuer IP-COP)
- Sysinfo (grafische Systeminformationen)
- Snortalog (grafische Auswertung der snort/IDS Logdateien)

IP-COP "The bad packets stop here"

Fazit: Vorteile

- Sehr gute und selbsterklärende GUI über den Webbrowser
- Auch mit geringen Linux Kenntnissen konfigurierbar
- Sehr hilfsbereite Internet Community
- Viel Hilfe, Dokus, Addons usw. verfügbar
- Geringer Kosten- und Installationsaufwand
- Deutlich mehr Einstellungen als bei einem normalen Router
(z.B. Fritz Box) möglich

IP-COP "The bad packets stop here"

Fazit: Nachteile

- IP-Cop immer noch mit Kernel 2.4.x.x
- Relativ selten Updates verfügbar
- Auf neuerer Hardware (z.B. Atom CPU) nicht lauffaehig
- Gibt Anfaengern das Gefuehl von Sicherheit.

Allerdings koennen durch „Unwissen“ gravierende Sicherheitsluecken entstehen

IP-COP "The bad packets stop here"

"Alternativen"

- Gibraltar Firewall
 - Für Privatgebrauch max. 5 Rechner begrenzt
- Collax Security Gateway
 - Für Privatgebrauch max. 5 Rechner begrenzt
- Iptables/Netfilter (z.B. unter Debian) Sehr umfangreich und ausführlich konfigurierbar
 - Für Anfänger schwieriger, da keine GUI
 - Derzeit wird am Nachfolger NF-Tables gearbeitet
- Monowall

IP-COP “The bad packets stop here”

Zukunftsaussichten

- Version 2.0 in Arbeit
- Umstellung auf Kernel 2.6.....
- Zerina, BOT, und Advanced Proxy werden voraussichtlich integriert sein
- GUI wird aktualisiert, aber weiterhin Benutzer / Einsteigerfreundlich bleiben

IP-COP "The bad packets stop here"

Webadressen

www.ipcop-forum.de

www.ipcopwiki.de

www.ban-solms.de/t/IPCop.html

www.ipcopaddons.org

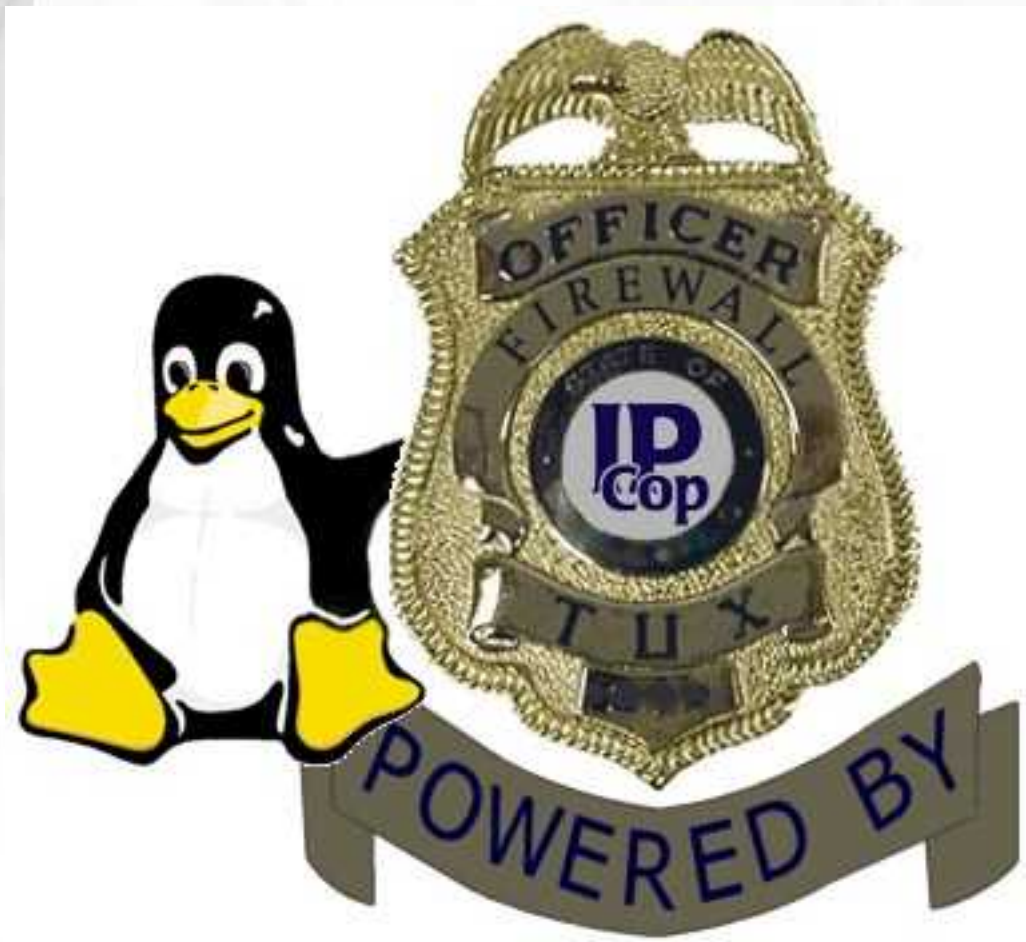
www.selflinux.org

Buch: „IP-COP kompakt“ von Marco Sondermann ISBN

978-3-939316-41-1 (Preis 24,90€) **sehr empfehlenswert**

IP-COP "The bad packets stop here"

**Das wars - Vielen Dank
Noch Fragen??**



**IP
Cop**