

Dipl.-Inform. Univ.

Peter Allgeyer

<p.allgeyer@protec-t.de>



Mehr Sicherheit durch OpenSource:

Betrachtung aktueller Firewall Systeme auf OpenSource Basis

Linux Informationsveranstaltung
der LUG Traunstein am 12. März 2005



Grundlegendes

<http://m0n0.ch/wall>

- Embedded Firewall Software (Image < 6mB)
- Basiert auf FreeBSD/ipfilter
- Administrierbar über Webbrowser
- XML-Konfiguration
- PHP Boot Skripten
- BSD Lizenz

Hardware

- Soekris 45xx, 48xx
- PC-engines WRAP board
- Standard x86 PC Hardware
 - raw CF/HD image for generic PCs
 - 2048 byte/sector Mode-1 ISO image



Features

- web interface (supports SSL, Firmware upgradable via WEB)
- serial console interface for recovery
- wireless support (access point with PRISM-II/2.5/3 cards, cisco cards)
- captive portal
- 802.1Q VLAN support
- DHCP client, PPPoE, PPTP, static support on the WAN interface
- IPsec VPN tunnels (support for hardware crypto cards and mobile clients)
- PPTP VPN (with RADIUS server support)
- OpenVPN (experimental)
- DHCP server, caching DNS forwarder
- DynDNS client
- SNMP agent
- traffic shaper (QoS)
- Wake on LAN client
- configuration backup/restore



Stärken und Schwächen

- ✓ Minimal-Lösung lauffähig von CD, schnell installiert und eingerichtet
- ✓ Fehlende mechanische Teile bei Embedded Plattform
- ✓ Wireless- und Captiv Portal-Lösung
- ✓ OpenVPN, IPSEC für mobile User (PreShared Keys)
- ✓ Zentrale Codebegutachtung und -freigabe
- ✓ Zentrale Konfigurationsdatei (gutes Backup/Restore-Konzept)
- ✓ Automatischer Timeout und manuelle Verbindungseinstellung für WAN
- × Kein modularer Aufbau -> keine zusätzlichen Proxies (SMTP, HTTP, SOCKS)
- × Fehlende Zertifikatslösung
- × IPSEC Verkehr kann nicht gefiltert werden

Ausblick: pfSense



Grundlegendes

<http://www.ipcop.org>

- Linux firewall distribution (iptables)
- IPCop interface webbasierend
- OLD PC + IPCOP = Secure Internet Appliance
- Modularer Aufbau
- GNU GPL

Hardware

- Standard x86 PC Hardware
- Festplatten-Installation (CF wird ebenso unterstützt)
- ISO Image for Alpha processors
- Unterstützung vieler WAN-Schnittstellen (PPPoE, PPTP, ISDN, ...)



Features

- Easy administration through the built in web server
- DHCP client that allows IPCop to, optionally, obtain its IP address from your ISP
- A DHCP server that can help configure machines on your internal network
- A caching DNS proxy, to help speed up Domain Name queries
- A web caching proxy, to speed up web access (Squid)
- An intrusion detection system to detect external attacks on your network
- GREEN, BLUE, ORANGE, RED Network Interfaces
- IPSEC VPN
- Traffic shaping capabilities (QoS)
- MRTG build in
- Improved VPN support with x509 certificates.
- A choice of four kernel configurations, allowing you to choose an optimum configuration for your circumstances.
- Running IPCop from a flash disk



Stärken und Schwächen

- ✓ Schnelle Installation
- ✓ Farbliche Trennung der Schnittstellen -> Übersichtlichkeit
- ✓ Modulkonzept ermöglicht Proxies
- ✓ Viren-, SPAM- und IDS-Lösung
- ✓ Integrierte Statistikauswertung

- × Sicherheit des Modulkonzeptes fragwürdig
- × Festplatteninstallation, bewegliche Teile
- × Umsetzung des CF-Konzeptes mangelhaft



Grundlegendes

<http://www.astaro.de>

- Kommerzielle Firewalllösung
- Basierend auf Linux/iptables
- Webbasierende Administration (erweiterbar durch Astaro Configuration Manager)
- Appliance Lösung
- Frei für nichtkommerzielle Nutzung

Hardware

- Standard x86 PC Hardware (mindestens 400 Mhz, 256MB)
- Festplatten-Installation (8 GB IDE oder SCSI)



Features

- Firewall mit Stateful Packet Inspection
- Virtual Private Network (IPSec, Site-2-Site, mobile User /w certificates)
- Virus Protection (kommerziell)
- Intrusion Protection
- Spam Protection
- Surf Protection (URL-, Content-Filtering)
- Automatische Updates
- Proxydienste (HTTP, DNS, SOCKS, POP3, IDENT, SMTP)



Stärken und Schwächen

- ✓ Bewährte Lösung, die auch kommerziell vermarktet wird
- ✓ IPSEC Zertifikatslösung mit integrierter CA
- ✓ Schnelle Installation
- ✓ Integrierte Viren-, SPAM- und IDS-Lösung (leider kommerziell)
- ✓ HA möglich (leider kommerziell)
- ✓ Zentrale Konfigurationsdatei (gutes Backup/Restore-Konzept)

- × Module lizenzpflichtig
- × Keine weiteren Erweiterungsmöglichkeiten



Fazit

- OpenSource Firewall Lösungen bieten viele Features
- Unterstützung günstiger (alter) Hardware
- Keine Benutzer-, Regel- oder Bandbreiteneinschränkungen
- Kostenlose Updates und Upgrades
- Webbasierende Oberflächen schaffen Ordnung und erleichtern die Konfiguration
- Filtercode basiert auf Standardsoftware (iptables, ipfilter)
- Mehr Sicherheit durch „echte“ Firewalllösungen mit richtigen ACLs und physikalisch getrennten Schnittstellen
- Breite Support-Unterstützung in Mailinglisten, Foren und Fachzeitschriften
- High-End Features wie Stateful-Failover fehlen (noch)

Dipl.-Inform. Univ.

Peter Allgeyer

<p.allgeyer@protec-t.de>



Danke für Ihre Aufmerksamkeit!