Arch Linux als Proxy und Firewall Lösung

Tino Reichardt, Steffen Martini

Schulverwaltungs- und Sportamt, Landkreis Elbe-Elster

15. Mai 2007

Gliederung

1. Warum Arch Linux ?
2. Installation
3. Firewall
4. Squid / Squidwall / Auswertung
5. Weitere Dienste
6. Überwachung der Server
7. Zusammenfassung

Warum Arch Linux: KISS

- Packetverwaltung:
  - sehr leicht zu erlernen
  - Packete sind sehr aktuell und original
  - man kann jedes Packet durch eigene ersetzen $\Rightarrow$ Anpassbarkeit
  - Organisation in Repositories $\Rightarrow$ durch Community gepflegt
- Konfiguration:
  - eine zentrale Konfigurationsdatei: /etc/rc.conf
  - für Notebooks: Netzwerk Profile für verschiedene Umgebungen
  - usw...

Installation

- CD booten
- Festplatte mit cfdisk vorbereiten und neu starten
- CD erneut booten
- Installation via `/arch/setup` starten
- CD / FTP Installation durchführen
- Installationszeit <20 Minuten (DSL empfohlen)

LKEE Firewall

- Übersicht:
  - alles ist verboten, er sei denn es wird explizit zugelassen
  - zusätzliche Sicherheit durch DENY=()
  - einfach zu konfigurieren
- Variablen:
  - LO=(lo)
  - INET=(eth0)
  - NETs=(eth1)
  - NETv=(eth2)
  - MASQ=(192.168.101.0/24 192.168.100.10/32)
  - DENY=(net1/mask:net2/mask)

Squid / Squidwall / Auswertung

- Squid ist der quasi Standard unter den Linux Proxy Servern
- Filterung via Squidwall und Clamav
  - sehr schneller und kleiner Content- und URL-Filter
  - inklusive Virenfilter zum Nulltarif (ClamAV)
  - ist über ein Webinterface sehr leicht zu bedienen
- Auswerung von Logdateien via SARG

Weitere Dienste

- DSL Einwahl via pppd mit kleinem Patch zum Auswerten von DSL Traffik
- pdnsd und dhcpd für DNS/DHCP inklusive fester und dynmasicher IP Vergabe anhand der MAC
- apache/php für das squidwall Webinterface
- proftpd für internes anonymous FTP (Bereitstellung von Antivirus Signaturen eTrust)
- sshd und knockd zur Fernwartung über ssh nach anklopfen durch Port Knocking
- openvpn zur Vernetzung von einigen Standorten

Überwachung der Server

- die meisten Komserver sind ohne Tastatur/Monitor (KVM Umschalter bei größeren Einrichtungen)

- Überwachung erfolgt derzeit durch ein SubmitStatus Shell Skript:
  - Festplattenplatz und Partitionsübersicht, Smartstatus
  - Übersicht zu: CPU, Speicher, IP Adressen und Routen
  - Sicherung von ’/etc’ als tar.gz zum download
  - alles via Webinterface jederzeit abrufbar

Zusammenfassung

- Arch Linux wird zur Zeit auf allen Linux Servern unserer Schulen eingesetzt
- die Kombinierbarkeit verschiedener Dienste an einem zentralem Punkt ist zeitsparend und einheitlich
- es kostet nichts und bietet maximale Sicherheit

Danke für die Aufmerksamkeit!

- Fragen ?
- Folien unter http://www.mcmilk.de/docs/
- Informationen zu Arch Linux unter http://www.archlinux.org/