Firewallsystem

Montage, Installation und Konfiguration (Proxy / Packetfilter) zwischen dem LAN des NLWK-Brake und dem Landesinternen WAN

Ablauf der Präsentation

- Aufgaben des NLWK-Brake
- Warum eine Firewall ?
- Zielsetzungen des Projektes
- Phasen im Projektverlauf
  - Ist – Analyse
  - Soll – Konzept
  - Planung
  - Realisierung
  - Test
- Fazit

Aufgaben des NLWK-Brake

- Betrieb und Unterhaltung von landeseigenen Gewässern
- Planung und Bau von Küstenschutzeinrichtungen, Gewässern und Wasserwirtschaftlichen Anlagen
- Gewässerkundlicher Landesdienst

Warum eine Firewallsystem ?

Bei einem Fileserverausfall, aufgrund eines Angriffes, können folgende kosten entstehen:

41 Arbeitnehmer x 8 Std x 70€ = 22.960 €

Ein Firewallsystem *kann* solche Angriffe und deren Folgekosten abwehren und ist deshalb als wirtschaftlich zu bezeichnen

Zielsetzungen des Projektes

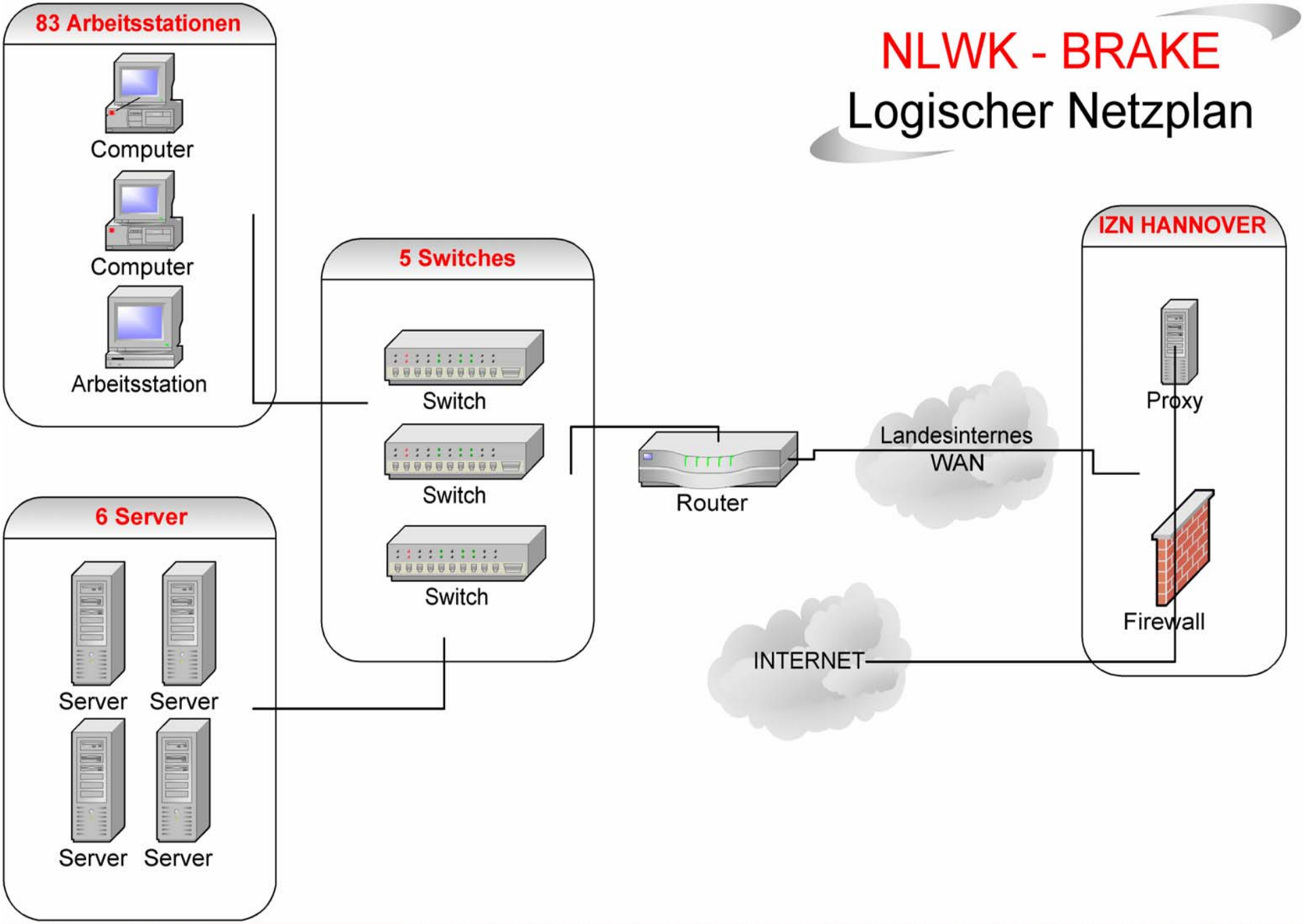
Das Netzsegment des NLWK-Brake vor Angriffen mit Hilfe eines Packetfilters schützen

Internetzugang über lokalen Proxy für bestimmte Nutzer

Auflage
Packetfilter und Proxy sind getrennt jeweils auf einen Rechner einzurichten

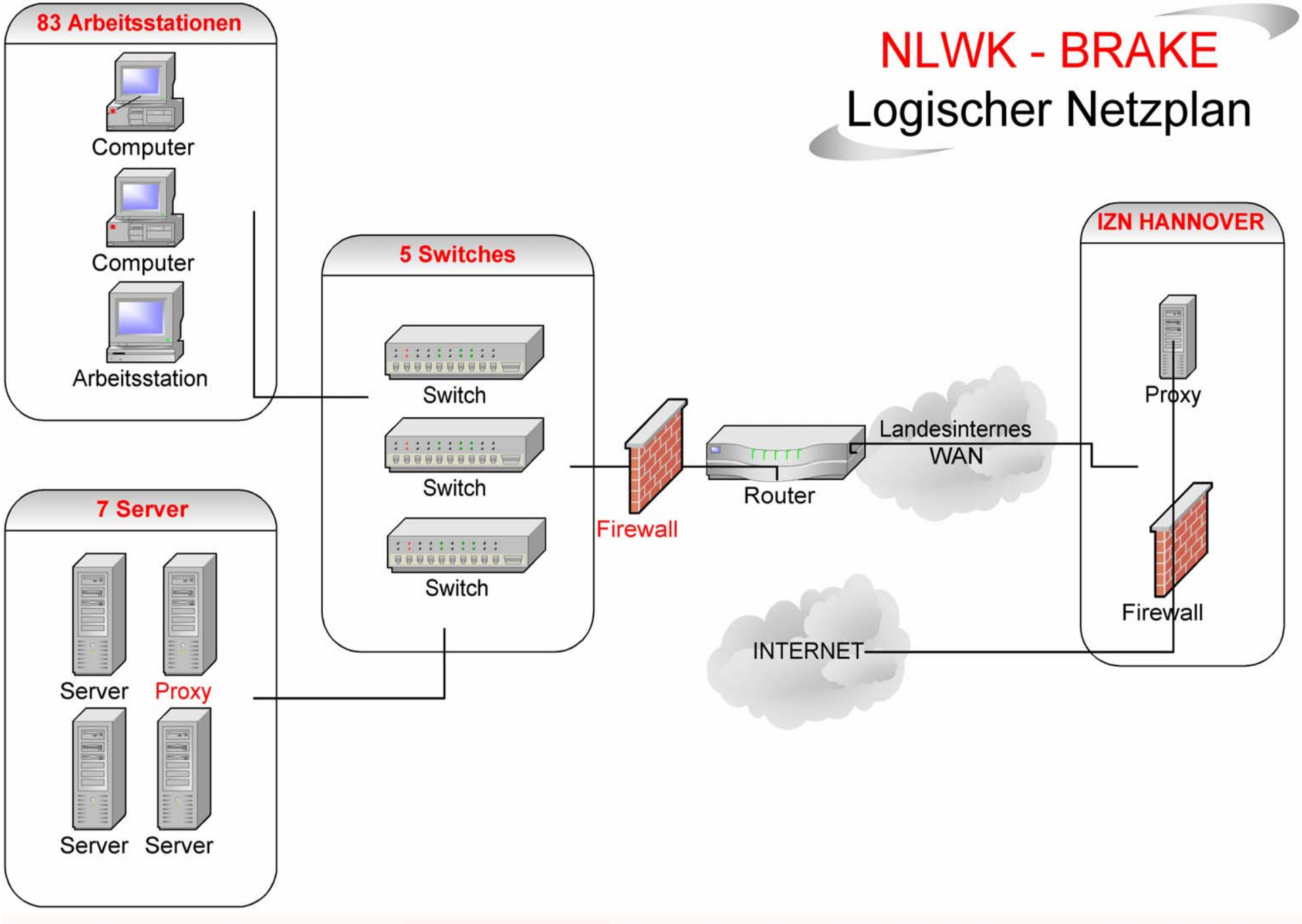
NLWK - BRAKE

Logischer Netzplan



NLWK - BRAKE

Logischer Netzplan



Anforderungen

Segment	Anforderung
Proxy	Gewährt und verhindert Zugriffe auf IP - Basis
	Speichert Internetseiten in seinem Cache für weitere Verwendung und protokolliert Aufrufe
	Greift auf den weiteren Proxy im IZN als „parent cache“ zu
Packetfilter	Lässt nur erlaubten Datenverkehr passieren
	Protokolliert abgewiesene Datenpakete

Kostenvergleich der Firewall Plattformen

Windows Komponente	Linux Komponente	Preis WIN	Preis Linux
Windows 2000 Server	Mandrake Linux - Powerpack Edition 8.1	835 €	80 €
Clientlizenzen	/	Schon vorhanden	/
Microsoft ISA Server Standard Edition, Proxy und Packetfilter integriert	Iptables (Packetfilter), Squid (Proxy)	1935 €	integriert
Konfigurationsaufwand x1 15 Std (55€/std)	Konfigurationsaufwand x2	825 €	1650 €
Gesamtpreis		**3595 €**	**1730 €**

Bewertungsmatrix zum Vergleich der beiden Firewall Plattformen

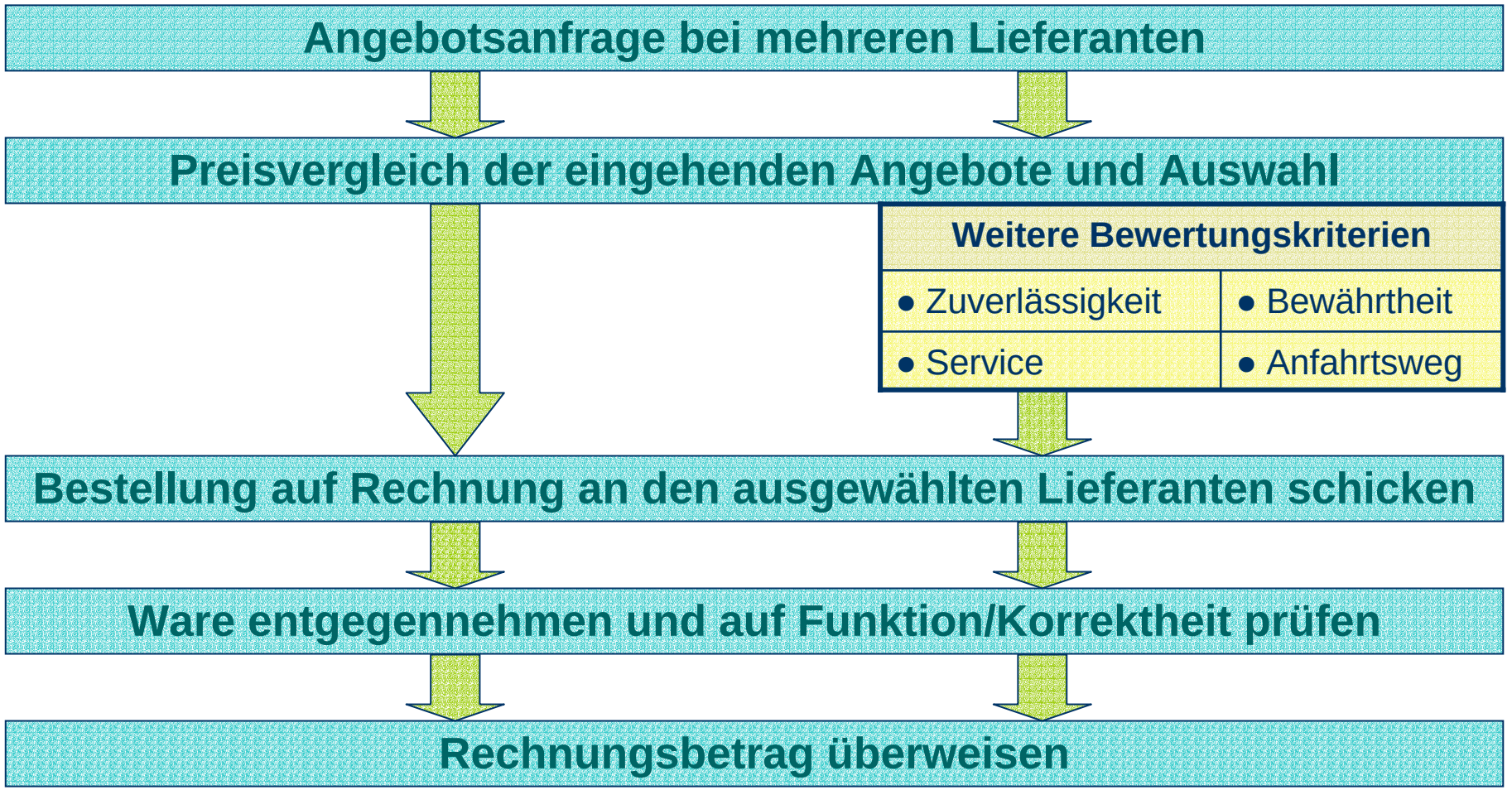
Kriterium *[Gewichtung]*	Linux	Windows 2k
Anschaffungskosten [2]	8	3
Updatekosten [1]	10	3
Stabilität [4]	8	8
Erweiterbarkeit durch neue Technologien [2]	9	6
Sicherheit [4]	8	6
Benutzerfreundlichkeit [3]	5	8
Administrationsaufwand [3]	5	7
	138	**122**

Dimensionierung der Hardware für den Einsatz von Linux als Plattform

Proxy	Packetfilter
AMD Duron 900 Mhz	AMD Duron 900 Mhz
Sockel A Mainboard	Sockel A Mainboard
128 MB RAM	128 MB RAM
20 GB Festplatte	20 GB Festplatte
CD – ROM	CD – ROM
1x 10/100 Mbit Realtek Netzwerkkarte	2x 10/100 Mbit Realtek Netzwerkkarte

Dimensionierung beider Systeme ist identisch, ausser bei der Netzwerkarte, da der Packetfilter für das Routing 2 Karten benötigt

Beschaffung der Hard- und Software Komponenten



Vorgehensweise bei der Installation und Konfiguration der beiden Systeme

Installation des Proxies

Installation des Minimalsystems (KDE, Konsolentools)

Installation des Packetes „squid“

Squid durch Anpassen der squid.conf konfigurieren

Cache für Squid erstellen

Squid – Dienst starten

Werktags

Installation des Packetfilters

Minimalsystem installieren (KDE, Konsolentools)

Installation des Packetes „iptables“

Installation der für Firewall Builder benötigten Packete

Routing aktivieren und Test

Regeln des Packetfilters mit Hilfe von Firewall Builder erstellen

Starten des Dienstes

Wochenende

Qualitätssicherung und Inbetriebnahme

- **Packetfilter (Test)**
  - Können benötigte Anwendungen Kommunizieren (BAAN, E-Mail)
  - Werden nicht erlaubte Packete abgelehnt und geloggt ?
- **Proxy (Test)**
  - Können Webseiten aufgerufen werden ?
  - Werden Zugriffe geloggt (access.log) ?
  - Können nur bestimmte Nutzer den Proxy nutzen ?
- **Konfigurationsdateien sichern**
  - Squid.conf
  - Firewall Builder Konfigurationsdatei

FAZIT

- Schon ein abgewehrter Angriff kann die Kosten für ein Firewallsystem ausgleichen, deshalb ist ein Firewallsystem durchaus als wirtschaftlich zu betrachten
- Das landesinterne WAN wird durch den Proxy-Cache entlastet, was Kosten spart
- Durch die Inbetriebnahme mit nachfolgendem Test und der Fehlerbeseitigung an einem Wochenende, konnte die betriebliche Beeinträchtigung (Kosten) auf ein Minimum reduziert werden
- Die Hard- und Softwarekosten können als gering bezeichnet werden

Vielen Dank für ihre Aufmerksamkeit!

Für weitergehende Fragen stehe ich ihnen gerne im anschließenden Fachgespräch zur Verfügung