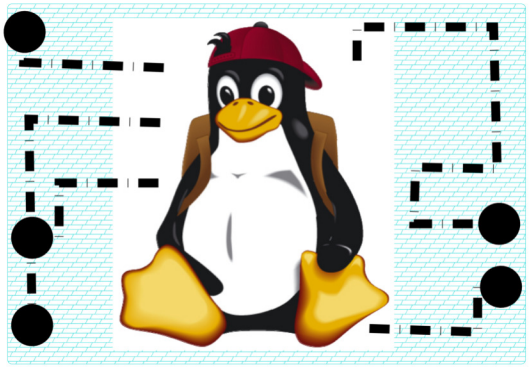
Skolerouter M11

[redacted]

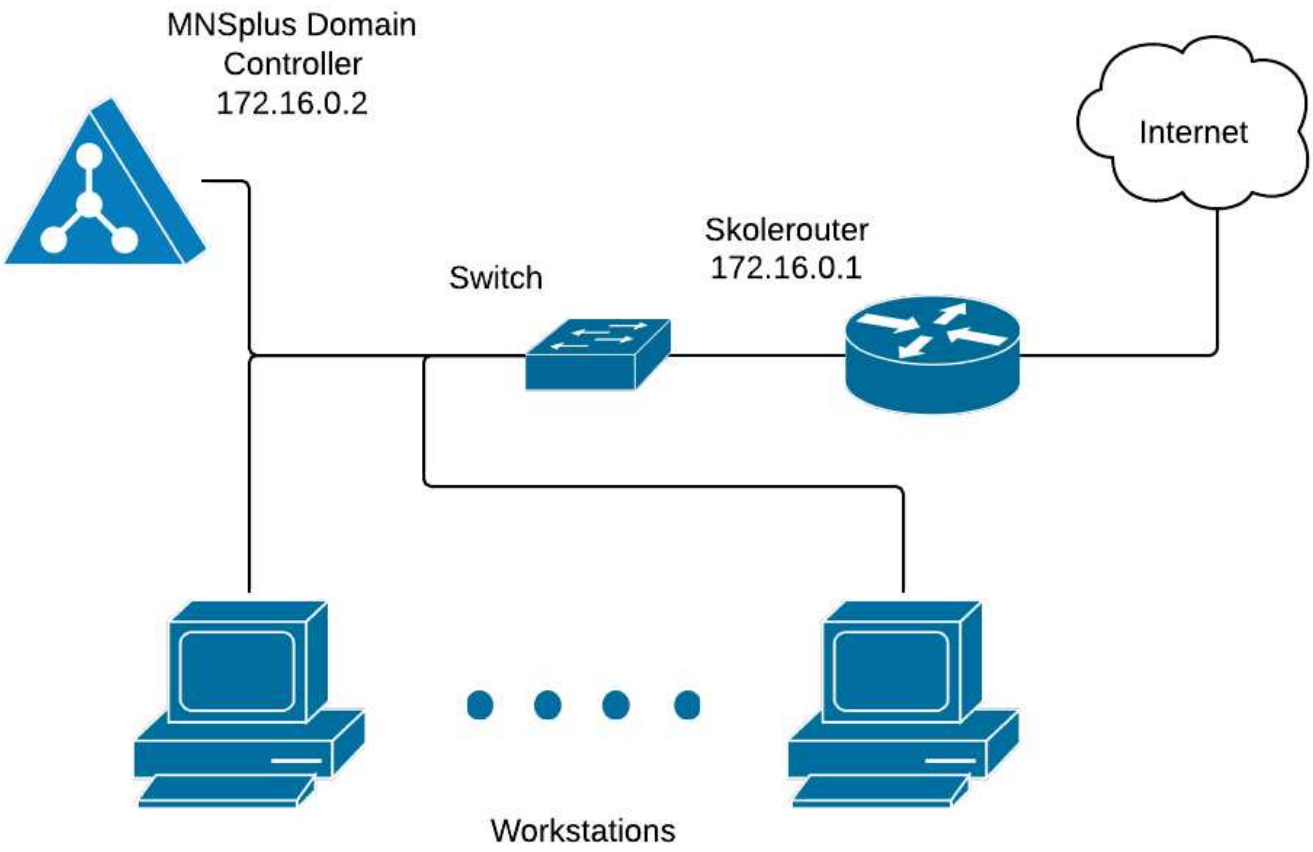
Stand 20.01.2013



Inhaltsverzeichnis

1 Einsatz

Der Skolerouter dient der externen Netzanbindung von MNS+, und enthält einen IP- , Benutzer- und content-basierten Filter sowie eine Konfigurationsschnittstelle.



2 Softwarebasis/Lizenz

Die Softwarebasis besteht ausschließlich aus öffentlich zugänglichen Open Source Komponenten bzw. Komponenten, die eine uneingeschränkte Verbreitung, und Verwendung der Software erlauben.

3 Komponenten

Als Basiskomponenten werden eingesetzt:

- Microknoppix (aktuell Version 7.0.5)
  Debian GNU/Linux (Squeeze/stable)-basierte GNU/Linux Distribution als installierbares Live-System mit automatischer Hardwareerkennung,

- squid
  Webproxy/Cache mit ACLs und Contentfilter-Plugin-Support
- dansguardian
  Content-basierter Webfilter mit Support für Antivirus-Plugins und Sperrlisten
- SSH Schnittstelle zur verzögerungsfreien Aktivierung bei Änderungen, sowie SSH-Login zur Konfiguration per Text-GUI
- Iptables-basierte Firewall (wahlweise Shorewall möglich)
- QoS (Traffic Shaping) durch tc. htb egress und ingress möglich
- OpenVPN
- VLAN-Support zur Zusammenarbeit mit modernen Netzwerk-Architekturen

4 Dateisystem

4.1 Statische Daten (FAT32)

Zwecks einfachem Update und Verringerung der Komplexität befinden sich die Systemdateien (Programme, Bibliotheken) in einem komprimierten Containerformat auf einer FAT32-Partition, von der die meisten Rechner problemlos booten können.

Es bietet sich der Einsatz von einem USB-Datenträger aus an. Um den Schulen eine preiswerte Ausfallsicherheit zu bieten wurde darauf geachtet, dass das System auf einen handelsüblichen, preiswerten Flash-Speicher (<= 1 GB) passt. Hiermit kann nach der Konfiguration des Systems auf einfache Weise ein gleichwertig konfiguriertes System durch Kopieren des Wechsel-Datenträgers erzeugt werden. Fällt die Router-Hardware aus, so lässt diese sich leicht durch ein im Hinblick auf die Netzwerk-Schnittstellen gleichwertiges Produkt ersetzen. Es ist keine Spezialhardware notwendig.

4.2 Veränderliche Daten (optional AES256-verschlüsselt)

Für die Konfigurationsdateien, Log-Dateien, Webcache, kleinere Updates etc. wird eine optional AES256-Bit verschlüsselte Partition verwendet, um den Ansprüchen des Schutzes personenbezogener Verbindungsdaten Rechnung zu tragen. Der optionale Schlüssel zum Einbinden der Partition wird wahlweise per interaktiver Eingabe, oder automatisch für das unbeaufsichtigte Hochfahren, über einen geeigneten Mechanismus zur Verfügung gestellt.

5 Konfiguration

5.1 Lokale Konfigurationsschnittstelle (Systemkonsole)

Auf der lokalen Systemkonsole läuft ein Login, das nach erfolgreicher Anmeldung per Shell-GUI eine weitgehende Konfiguration des Systems mit einfacher Menüsteuerung bietet, wahlweise auch mit Framebuffer-basiertem Webbrowser (links2), mit Maus- und Tastatursteuerung. Weiterhin stehen auf den Textkonsolen

2 bis 4 (Alt-F2…F4) Logins (während der Installationsphase root-Shells ohne Passwortabfrage) zur Verfügung.

5.2 Remote-Administrationszugang, skriptbar

Per SSH ist eine Fernwartung direkt auf Unix-Ebene möglich, wobei die gängigen Konfigurationsaufgaben (LDAP, externes Netz) mit einfach gehaltenen Menüs gesteuert werden. Alternativ ist ein IPSec-oder OpenVPN-Zugang zur Remote-Administration möglich. Zur Erhöhung der Sicherheit der Remote-Zugänge ist die Benutzung eines Hardware-Tokens (Smartcard, Krypto-Dongle) als Erweiterung des Systems möglich.

5.3 Steuerung Webzugriffe

Zur feingranulierten Steuerung der Zugriffe von Clients (Adressen- oder Benutzerbasiert) werden Squid-ACLs verwendet, die mit Vorgaben wahlweise aus LDAP-Listen, oder statischen Dateien mit Daten versorgt werden.

Optional kann ein übergeordneter Proxy („parent proxy“), mit oder ohne Passwort-Authentifizierung, zum Einsatz kommen wenn der Skolerouter nicht direkt auf Webseiten zugreifen soll.

Die Abbildung „Squid-Zugriffsregeln“ enthält einen schematischen Überblick des Squid-Regelsatzes.

Die in der

`/etc/squid3/squid.conf`

konfigurierten Regeln sind wie folgt der Abbildung zuzuordnen (Index in der Abbildung → Squid Zugriffsregel):

(1) → `http_access allow ProxyAllowSite`

(2) → `http_access allow ProxyAllowURL`

(3) → `http_access allow ProxyAllowClient`

(4) → `http_access allow ProxyAllowClientIP`

Regel (4) erlaubt Clients ohne DNS-Eintrag Web-Zugriff.

(5) → `http_access allow ProxyWhitelistClient ProxyWhitelistSite`

(6) → `cache_peer_access localhost_bl allow ProxyBlacklistLocalClient !ProxyBlacklistSite`

`http_access allow ProxyBlacklistLocalClient !ProxyBlacklistSite`

Regel (6) lenkt Zugriffe auf nicht in den Sperrlisten benannte Seiten durch den Webfilter zur weitergehenden Prüfung.

(7) → `http_access deny  ProxyBlacklistLocalClient ProxyBlacklistSite`

Regel (7) sorgt dafür, dass Rechnern der Gruppe `ProxyBlacklistLocalClient` gegenüber der Rechnergruppe `ProxyBlacklistClient` kein Authentifizierungs-Dialog angeboten wird.

(8) → `http_access deny !authenticated`

Regel (8) trennt die rein Client-basierten Regeln von den Regeln welche die Benutzergruppen zusätzlich auswerten.

(9) → `cache_peer_access localhost allow ProxyBlacklistClient ! ProxyBlacklistSite`

`http_access allow ProxyBlacklistClient !ProxyBlacklistSite`

Regel (9) lenkt die Zugriffe der Mitglieder von `ProxyBlacklistClient` nach Authentifizierung auf den Dansguardian Webfilter. Die Dansguardian-Konfiguration ab Version 2012-12 unterscheidet zwischen Benutzern der Gruppe `ProxyAllowUser` und Benutzern der übrigen Gruppen. Mitgliedern der Gruppe `ProxyAllowUser` wird ungefilterter Web-Zugriff gewährt.

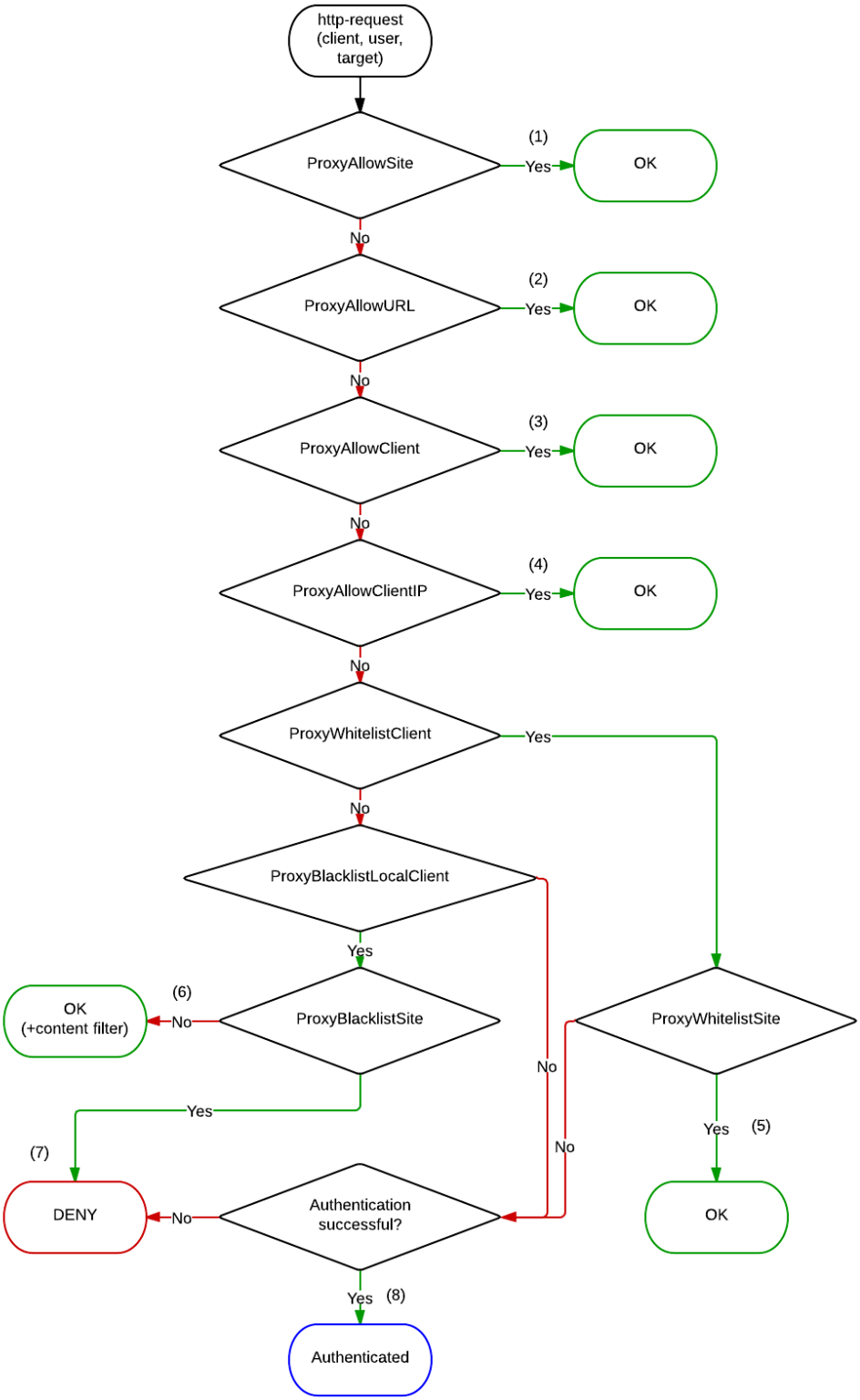
Die folgenden Regeln ordnen, falls noch kein Zugriff gewährt wurde, die Benutzergruppen den für sie erlaubten Web-Zugriffsregeln zu:

(10) → `http_access allow ProxyAllowUser`

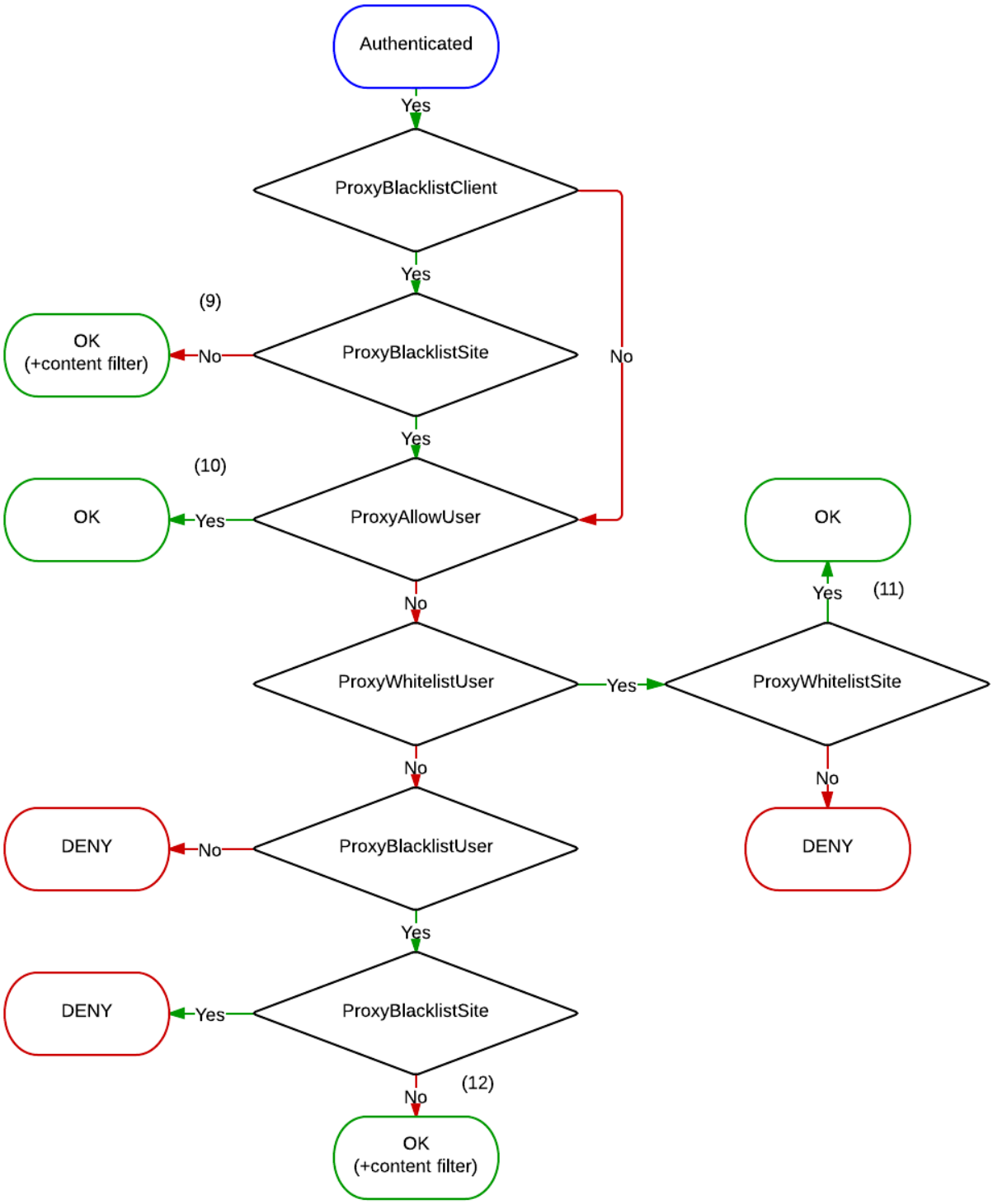
(11) → `http_access allow ProxyWhitelistUser ProxyWhitelistSite`

(12) → `cache_peer_access localhost allow ProxyBlacklistUser !ProxyBlacklistSite`

`http_access allow ProxyBlacklistUser !ProxyBlacklistSite`



Squid Proxy – Zugriffsregeln



Squid Proxy – Zugriffsregeln (Fortsetzung)

5.4 Anbindung an MNS+

5.4.1 LDAP-Anbindung MNSplus – Skolerouter

Der Active Directory Service des MNSplus Systems bildet die Konfigurationsdatenbank des Skolerouters. Zum Betrieb des Skolerouters ist nach der initialen Installation daher kein direkter Eingriff auf dem Router notwendig, die Steuerung kann komplett aus der Ferne erfolgen.

Als atomare Elemente dieser Konfiguration werden LDAP-Einträge für Computer und für Benutzer genutzt. Durch Zuordnung dieser Elemente zu dem LDAP-Gruppen wird die Zugriffssteuerung realisiert .

Die Zugriffssteuerung der VPN-Zugänge erfolgt über die Gruppen

- PPTPLehrer
- PPTPSchueler
- PPTPSupporter

Für jedes Mitglied dieser Gruppe wirkt ein eigener Satz von Firewalling-Regeln beim Login via PPTP. Nach einem erfolgreichen Login auf dem Skolerouter wird ein Benutzer seiner Zugriffsklasse zugeordnet und kann auf die freigegebenen Rechner innerhalb des Schulnetzwerkes zugreifen. In diesen Zugriffsgruppen werden lediglich Benutzer eingetragen, Computer-Accounts werden in diesen Gruppen ignoriert.

Das Firewalling für diese Zugriffsklassen kann je Installation separat erfolgen.

Die Zugriffssteuerung der Surfaktivitäten über den Proxy erfolgt über die Gruppen

- ProxyAllowUser: Benutzer, die frei surfen dürfen.
- ProxyAllowClient: Computer (DNS), die frei surfen dürfen.
- ProxyAllowClientIP (**Sonderfall**): Computer (ohne DNS), die frei surfen dürfen. Diese Gruppe wird nur über die Konfigurationsdatei

  ```
  /etc/skolerouter.d/ProxyAllowClientIP.extra
  ```

  gepflegt, es wird keine LDAP-Gruppe ausgewertet.
- ProxyWhitelistClient: Computer (DNS), die nur in einer Whitelist definierte Webseiten ansurfen dürfen.
- ProxyWhitelistUser: Benutzer, die nur in einer Whitelist definierte Webseiten ansurfen dürfen.
- ProxyBlacklistClient: Computer, die alle außer den in einer Blacklist definierte Webseiten ansurfen dürfen, wenn diese nicht zusätzlich per Contentfilter gesperrt sind. Nach erfolgter Authentifizierung ist es durch Mitgliedschaft in ProxyAllowUser möglich, von diesen Rechnern aus frei zu

surfen.

- ProxyBlackListLocalClient (**Sonderfall**): für diese Clients gelten die gleichen Regeln wie für ProxyBlacklistClient, jedoch wird kein Authentifizierungs-Dialog angeboten. Daher ist kein freies Surfen nach Authentifizierung und passender Mitgliedschaft möglich. Diese Gruppe wird nur über die Konfigurationsdatei

  ```
  /etc/skolerouter.d/ProxyBlacklistLocalClient.extra
  ```

  gepflegt, es wird keine LDAP-Gruppe ausgewertet.
- ProxyBlacklistUser: Benutzer die alle außer den in einer Blacklist definierte Webseiten ansurfen dürfen, wenn diese nicht zusätzlich per Contentfilter gesperrt sind.

Passend zur dargestellten Konfiguration würde diese Struktur durch folgende LDAP-Gruppen realisiert:

```
dn:CN=ProxyAllowClient,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,DC=loca
l
dn:CN=ProxyAllowUser,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,DC=local
dn:CN=ProxyWhitelistClient,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,
  DC=local
dn:CN=ProxyWhitelistUser,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,
  DC=local
dn: CN=ProxyBlacklistClient,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,
  DC=local
dn: CN=ProxyBlacklistUser,OU=Benutzer_Gruppen,OU=Schule,DC=TEST5,
  DC=local
```

Zusätzlich ist die Definition einer Liste von Adressen oder Benutzern möglich, welche unabhängig von einem LDAP-Eintrag in den einzelnen Filterklassen berücksichtigt werden. Diese werden in einer einfachen Textdatei mit Endung „.extra“, zu den automatisch generierten Gruppen in /etc/skolerouter.d/ auf dem Router-System eingepflegt.

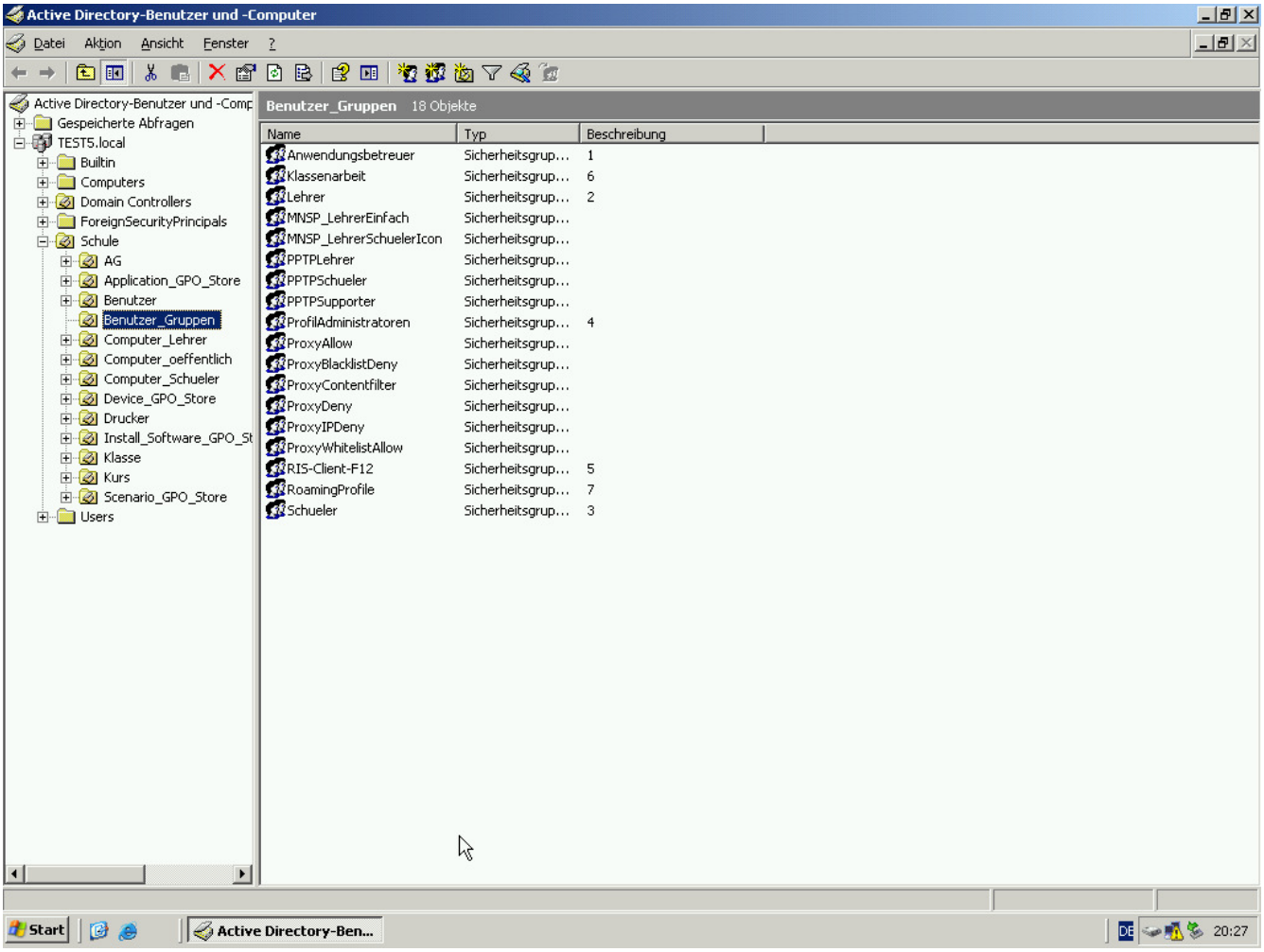
Syntax der ProxyBlacklist/WhitelistSites Listen:

1. Ein Eintrag pro Zeile
2. Entweder Hostname (FQDN) des Zielrechners, ODER Domainname mit führendem Punkt:

   ```
   www.google.de
   .google.de
   ```

3. Das check_LDAP.sh-Skript auf dem Skolerouter ergänzt bei Hostnamen in der ProxyClientBlack/Whitelist automatisch die Domain.

Folgendermaßen würden diese Gruppen auf einem MNS+ System konfiguriert werden:

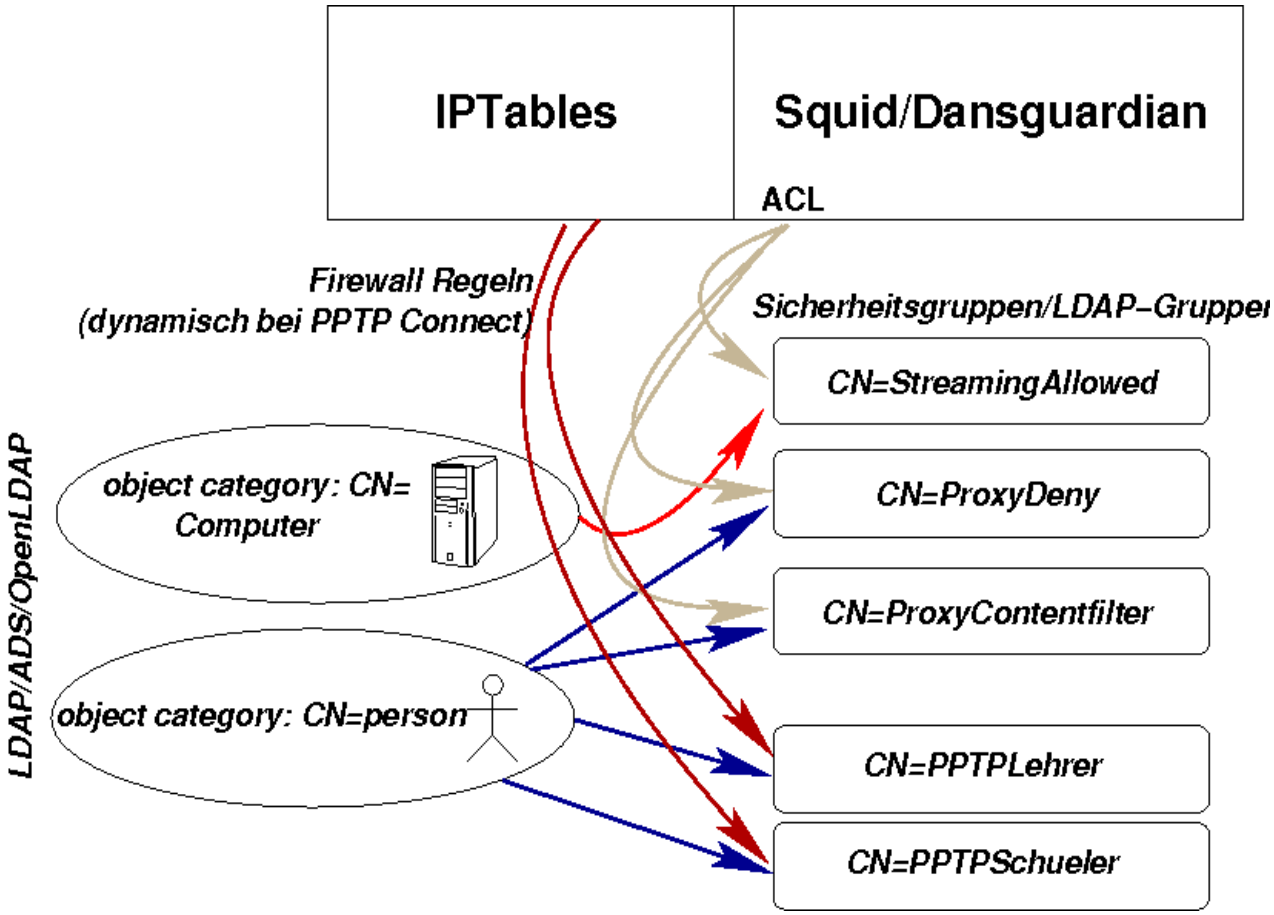


Der Skolerouter aktualisiert über SSH-Trigger die Zugriffsgruppen von seiner zugeordneten LDAP-Datenbank. Sollte die Kommunikation zum LDAP-System abbrechen, so wird die letzte vorgenommene Konfiguration vorgehalten.

Das Skript, das hierzu vom Administrations-Client aus per SSH auf dem Skolerouter aufgerufen wird, befindet sich unter `/usr/local/bin/skolerouter` und wird mit der folgenden Syntax gestartet:

Kommando	Bedeutung
`skolerouter shutdown`	Fährt den Skolerouter herunter
`skolerouter reboot`	Löst einen Neustart des Skolerouters aus
`skolerouter updateproxygroups`	Liest die Proxy-Gruppen erneut aus dem LDAP
`skoelrouter reloadsquid`	Lädt die Squid-Konfiguration neu
`skolerouter shell [cmdline]`	Führt ein Shell-Kommando aus

Folgendes Schaubild visualisiert den Informationsfluss von der ADS zum Skolerouter-System anhand einiger Beispielgruppen:



5.4.2 RPC-Schnittstelle

Webmin stellt über die URL https://benutzer:passwort@skolerouter/xmlrpc.cgi eine RPC-Schnittstelle zur Verfügung, über die sämtliche Webmin-Module angesteuert werden können. Ein Beispiel für die Benutzung des Firewall-Moduls per RPC liegt in Perl vor.

Hinweis: Die API ist effektiv nur im webmin-Code dokumentiert, Beispiele für das Setzen von iptables sind vorhanden. Diese Möglichkeit wird derzeit jedoch weder von MNS+ noch von Skolelinux genutzt und ist daher optional.

5.4.3 Konfiguration von Default-Werten bei der Installation

Beim Start des unmodifizierten Skolerouters (ISO/CD oder Flash) startet der Installer, und fragt die Ziel-Festplatte und das Verschlüsselungs-Passwort ab.

Nach Übertragung der Daten von CD/Flash auf die Festplatte und Einbinden der

verschlüsselten Partition werden bei der Erstinstallation die essentiellen Netzwerkdaten nacheinander abgefragt, teilweise auch automatisch ermittelt.

1. Verschlüsselungs-Passwort Datenpartition (optional)
2. Root-Passwort.
3. Konfiguration Intranet. Hier wird durch Abfrage des Carriers beim Herausziehen und Einstecken des Netzwerkkabels die Schnittstelle **eth0** ermittelt, welche stets an das **interne** Netzwerk angekoppelt wird.
4. SSH-Key für die „Sofortaktivierung“ von Konfigurationsoptionen von Windows und Linux aus.
5. Durch ping auf die bekannten Server-Adressen wird das Profil ermittelt – SKOLE oder MNS+. Wird keiner der beiden Server erkannt, so werden die IP-Daten des Routers nacheinander abgefragt.
6. Konfiguration LDAP/ADS (Änderungen gegenüber den Standardprofilen für MNS+ bzw. Skole).
7. Konfiguration Internet-Anbindung (ISDN, LAN/WLAN, UMTS).

Nach Eingabe der Daten werden diese in die entsprechenden Konfigurationsdateien gepatcht, wobei ggf. Vorlagen von Konfigurationsdateien mit der Endung `.in` (z.B. `/etc/squid3/squid.conf.in`) verwendet werden.

Das Setup kann nach der Erstinstallation jederzeit wiederholt werden. Aus praktischen Gründen ist das Skript zur Festplatteninstallation (`INSTALL.sh`) und Setup (`SETUP.sh`) außerhalb des komprimierten Systems im Wurzelverzeichnis des Installationsmediums bzw. auf der FAT32-Partition der installierten Version untergebracht. Bei der nachträglichen (Re-)konfiguration wird ein Menü präsentiert, in dem die Konfigurationsabschnitte einzeln ausgewählt werden können.

5.4.4 Default-Passwörter, die geändert werden sollten

admin admin (webmin)
log view (webmin)

Das AES-Passwort der verschlüsselten Reiserfs-Partition ist ohne Neuformatierung nicht änderbar.

5.4.5 Laufende Dienste und Protokolle

pptpd, ssh (per iptables freizuschalten), squid, dansguardian, bind9/resolvconf, isdnutils, cron, syslogd (lokal), winbind, kein cups.

Alle Dienste werden (wie unter BSD) im Skolerouter in der `/etc/rc.local` (SERVICES=) gestartet, und führen die entsprechenden Skripte unter `/etc/init.d/*` aus. Die sonst unter SystemV-ähnlichen System verwendeten Runlevel-Skripte `/etc/rc*.d/*` werden ignoriert. IPV6 wird vom Kernel unterstützt, ist aber per Default nicht aktiv

6 Updates

6.1 System-Upgrade (neue Releases)

6.1.1 Manueller Austausch der „Firmware“

Die Aktualisierung des Skolerouter erfolgt, ähnlich wie bei „embedded“-Geräten, im Wesentlichen durch den vollständigen Austausch des read-only Systems unter Beibehaltung der Konfigurationsdateien im schreibbaren Overlay.

Zum Basissystem gehören die hier angegebenen Dateien auf der FAT32-Partition, die im Produktivbetrieb als `/mnt-system` gemountet ist:

Dateiname	Beschreibung
boot/syslinux/linux	Kernel (statischer Teil)
boot/syslinux/minirt.gz	Boot-Ramdisk
KNOPPIX/KNOPPIX	Komprimiertes System
SETUP.sh	Setup-GUI

Ein Update der entsprechenden Dateien ist im laufenden Betrieb nach dem im folgenden beschriebenen Verfahren möglich. Das neue System wird nach Neustart aktiv. Nach Download der neuen Dateien von einem (angenommenen) Update-Server ins Verzeichnis „`update`“ werden die alten Dateien in den Ordner „`downgrade`“ gesichert und die neuen Dateien an ihre Stelle umbenannt. Da hierbei keine Daten überschrieben oder gelöscht werden, läuft das alte System bis zum Neustart unverändert weiter.

```
cd /mnt-system
mkdir update downgrade
scp -r user@update-server:skolerouter-version2/\* update/ || exit 1
for i in `find update -type f`; do
 mv -f "${i#update/}" downgrade/ && mv -f "$i" "${i#update/}"
done
```

Skript 1: Bash-Skript Beispiel zum Upgrade des Systems

6.1.2 Skriptbasiertes Upgrade – `UPGRADE.sh /url/to/cd.iso`

Ein automatisiertes Upgrade ist mit den neuen Skripten der Versionen ab 2012-11 möglich.

Dateiname	Beschreibung
UPGRADE.sh	Automatisiertes Upgrade
POSTUPGRADE.sh	Skript zum „Aufräumen“ bzw. zum Löschen manueller Änderungen der vom alten System übernommenen Daten im Overlay

Aufruf:

`/mnt-system/UPGRADE.sh` http://servername/skolerouter-upgrade.iso

`/mnt-system/UPGRADE.sh` ftp://servername/skolerouter-upgrade.iso

`/mnt-system/UPGRADE.sh /tmp/skolerouter-upgrade.iso`

Funktionsweise:

Bei Angabe einer http- oder ftp-URL wird die entsprechende ISO-Datei über das Netzwerk auf die schreibbare Partition heruntergeladen, bei Angabe einer lokalen Datei hingegen direkt verwendet. Die ISO-Datei wird per Loopback-Mount eingebunden, und die für das System relevanten Dateien in die neuen Verzeichnisse kopiert. Das neue System wird in neuen Ordnern angelegt, die die als Ordnernamen die Versionsnummer erhalten. In boot/syslinux/syslinux.cfg werden die neuen Ordner als DEFAULT eingetragen.

Durch Eingabe einer älteren Versionsnummer kann eine frühere Version gestartet werden, durch eingabe von „knoppix“ das zuerst installierte System.

Auch die Daten der Overlay-Partition werden kopiert, hierzu wird ein Unterordner in /KNOPPIX-DATA angelegt und in diesen die Daten des laufenden Systems kopiert, jedoch unter Auslassung/Löschung der Debian-Paketdatenbank sowie `/usr/local/(s)bin`.

6.2 Einzelpakete und manuelle Änderungen

Grundsätzlich ist es durch die Overlay-Struktur möglich, vorhandene Softwarepakete (wie z.B. SAMBA) im read-only Bereich durch Debian-Pakete aus den Standard-Repositories zu aktualisieren, wodurch die Änderungen im Overlay gespeichert werden und die ursprünglichen Versionen „verdecken“.

```
apt-get update
apt-get install -t testing samba
```

Skript 2: Update der Debian-Paketdatenbank und Installation einer neuen SAMBA-Version aus Debian/testing

Hierbei kann jedoch ein Konflikt mit zukünftigen Komplett-Updates nach Abschnitt 6.1 entstehen, da das System nicht feststellen kann, ob die „verdeckte“ oder die nachträglich installierte Version einer Datei tatsächlich „neuer“ ist.

Sämtliche Overlay-Daten bzw. Änderungen zwischen der ursprünglichen CD/read-only Installation und den lokalen Anpassungen, nachinstallierten Paketen, Logdateien und heruntergeladenen Dateien sind im Verzeichnis /KNOPPIX-DATA untergebracht.

7 Hardwareanforderungen

- i*386-kompatible CPU (single oder multicore), >= 600 Mhz
- 512 MB Ram
- Festplatte/Flash >= 4GB
- Webcache- und Log-Speicher nach geschätztem Bedarf
- mind. 1 Netzwerkkarte zum Anschluss in Richtung LAN (eth0)
- ext. Netzwerkkomponente: Modem, ISDN-Karte, WLAN, LAN (nur Linux-unterstützte Hardware)

8 HOWTOs

8.1 Installation / Inbetriebnahme

Wird der Skolerouter vom Installationsmedium das erste Mal gestartet, und existiert noch keine Konfigurationsdatei /etc/skolerouter.conf, so meldet sich das System mit einem „Installations-Splashscreen, und nach erfolgter Hardwareerkennung werden nacheinander die folgenden Konfigurationsschritte abgefragt. Nach Abschluss der Konfiguration und Neustart des Systems koppelt sich der Skolerouter an den jeweils konfigurierten Server (MNS+ Server bzw. Skolelinux Tjener) und erhält von diesem die Proxy-Einstellungen und die Benutzerauthentifikationen per LDAP.

In den folgenden Abschnitten wird die Installation und Konfiguration Schritt für Schritt erklärt.

8.1.1 Festplatte partitionieren und Datenpartition (optional) verschlüsseln

[...work in progress...]

8.2 Außerbetriebnahme / Löschung sensitiver Daten

8.2.1 Verschlüsselte Datenpartition

Um die Datenpartition ohne Kenntnis des Verschlüsselungs-Passwortes unbrauchbar zu machen, genügt es, die Datei KNOPPIX/knoppix-data.aes auf dem unverschlüsselten Teil der Festplatte zu überschreiben.

```
wipe /mnt-system/KNOPPIX/knoppix-data.aes
```

Falls die Variante der Verschlüsselung ohne Speicherung des Passwortes gewählt wurde, ist dieser Schritt nicht notwendig.

8.2.2 Unverschlüsselte Datenpartition

Hier ist zur sicheren Löschung der je nach Größe der Partition sehr lange dauernde Prozess des Überschreibens mit Zufallsdaten für die komplette Partition anzuwenden.

Beispiel (Datenpartition sei /dev/sda2):

```
wipe /dev/sda2
```

9 Die IPTables-Firewall

9.1 Überblick

Die IPTables-basierte Firewall besteht aus einem statischen und einem dynamischen Konfigurationsteil. Der statische Konfigurationsteil beinhaltet die Grundkonfiguration für den Skolerouter sowie die Konfiguration der Regeln, welche für Rechner- und Benutzergruppen angewandt werden. Der dynamische Teil wird durch die PPTP-Scripte durchgeführt, welche die Verbindung eines Benutzers abhängig vom Benutzernamen beim Aufbau einer PPTP-Verbindung in die passende Regelkette einsortiert.

9.2 Konfiguration

Die Firewall wird über das Startscript (neu) gestartet oder gestoppt:

```
/etc/init.d/firewall {start,stop,restart}
```

Die Konfigurationsdateien sind auf dem System unterhalb von

```
/etc/firewall
```

zu finden. Nach einer Änderung an den Konfigurationsdateien ist die Firewall neu zu starten. Sollten hierbei Fehler auftreten, so sind diese zu korrigieren, es wird jedoch nur die fehlerhafte Regel nicht ausgeführt. Die Konfigurationsdatei *custom.conf* enthält die Grundkonfiguration des Systems.

Von *extern* zur Firewall ist erlaubt:

- ssh (22 TCP)
- PPTP (Protokoll 47 sowie Port 1723 TCP)
- OpenVPN (1149 UDP)
- ICMP echo-request

Von *intern* zur Firewall ist erlaubt:

- uneingeschränkter Traffic

Von *intern nach extern* ist folgender Traffic erlaubt:

- für die in der Variable *FORWARD_EXT_HOSTS* konfigurierten Adressen ist die Verbindung von jedem Rechner aus dem internen Netzwerk erlaubt, die Rechner sind von *intern* aus über alle Ports erreichbar.
- die in *FORWARD_INT_HOSTS* gelisteten Rechner dürfen auf das Internet zugreifen.

Beide Variablen sind in

```
/etc/firewall/hosts.conf
```

definiert.

Aus dem VPN zur Firewall ist für alle Benutzer erlaubt:

- die innerhalb der Variablen *PPTP_INPUT_TCP* (Grundkonfiguration: ssh, http-alt) gelisteten Ports via TCP
- die innerhalb der Variablen *PPTP_INPUT_UDP* (Grundkonfiguration: domain) gelisteten Ports via UDP
- ICMP echo-request

Die Variablen sind innerhalb der Konfigurationsdatei

```
/etc/firewall/ports.conf
```

zu finden. Für die Benutzergruppen PPTP-Schueler, PPTP-Supporter und PPTP-Lehrer finden sich in

```
/etc/firewall/conf.d
```

separierte Konfigurationsdateien, welche die Regeln für die jeweilige Benutzergruppe bestimmen.

Basiskonfiguration PPTP-Zugriff:

- Benutzer aus der Gruppe PPTP-Supporter erhalten uneingeschränkten Zugriff in das interne Netzwerk sowie über das externe Interface des Skolerouters in das Internet
- Benutzer aus der Gruppe PPTP-Lehrer erhalten Zugriff auf die in der Variable *FORWARD_INT_PPTPLehrer* gelisteten Hosts. Die Konfigurationsdatei, welche die Variable enthält, findet sich unter

  ```
  /etc/firewall/hosts.conf
  ```

- Benutzer aus der Gruppe PPTP-Schueler erhalten Zugriff auf die in der Variable *FORWARD_INT_PPTPSchueler* gelisteten Hosts. Die Konfigurationsdatei, welche die Variable enthält findet sich unter

  ```
  /etc/firewall/hosts.conf
  ```

9.3 Howtos

9.3.1 DNAT

Eine Portumleitung besteht immer aus zwei Regeln, einer DNAT- und einer FORWARD-Regel.

Beispiel einer Portumleitung von Port 80 (extern) zu Host 172.16.0.123:80 (intern).

```
/etc/firewall/hosts.conf:
WEBSERVER="172.16.0.123"

/etc/firewall/custom.conf:
$IPTABLES -t nat -A PREROUTING -i "$EXTDEV" -p tcp  --dport 80 -j DNAT \
   --to-destination "$WEBSERVER:80"
$IPTABLES -A FORWARD -p tcp –dport 22 -d "$WEBSERVER" -i "$EXTDEV" \
  -o "$INTDEV" -m state --state NEW -j ACCEPT
```