Webserver – Update 24. 10. 2003

Grundidee: SuSE 9.0 installieren und User etc. von alter Installation übertragen.

1. Problem: Netzwerkkarte Realtek 8139 einbauen

Vorteil: Updates laufen täglich automatisch.

Sidestep: Beschaffung Unterstufe: BBG war auch überrascht ..., im Prinzip bei BBG kaufen.BBG gute Angebote: Beamer, Kyocera-Netzwerkdrucker

Disketteninstallation:

Boot-Diskette
Modules 1 – Disk

Kernelmodule ladne
für NTFS-INstallation: Modules 3 – Netzwerkkartentreiber

rtl8139 wählen

keine Parameter!

Dann zurrück, Installation starten

Netzwerk, NFS

keine DHCP

IP: z.b: 10.0.1.224

Gateway 10.0.1.220
Server 10.0.1.220

Neuinstallation::

Partitionierung: keine Boot-Partition

10 GB root-Partition, ext2, aber:quotas nicht unbedingt notwendig – postfix!, swap-Partition 500 MB

Manuell: Partitionen löschen
Windows-Partition lassen

Softwareauswahl:

Standardsystem + folgendes:

erweiterte Auswahl: Selektion –
suchen:
apache2, docu, modperl, modphp4,
mysql
mysql-client
phpMyAdmin

dann

Suche:

vsftp
squid
squidguard

postfix
antivir
amavis
popper
qpopper

firewall

SuSE etc. schon gewählt

webmin

perl-net
perl-Net_SSLeay !!!
(für https – webmin)

allenfalls dhcp
allenfalls dns-Server: bind

ftpdir - „change root“

[Akzeptieren]

Alles fehlende nachinstallieren.

Apache2-worker

Dann [Neu Prüfen] – er nimmt dann den Apache2 prefork (:-))

Übernehmen
Ja-installieren

Nach der Installation: PW für root angeben: „schule“

IP-Adresse n von: Schulnetz und offizielle IP-Adresse:

z.B.: zwei Netzwerkkarten.
Später konfigurieren!

Internetzugang später

Einzelplatzrechner

einen Benutzer anlegen: Weiterleitung von System-Mails! Daher Benutzer entsprechend anlegen!

Autoatische Anmeldung weghaken.

Weiter

Hardwareerkennung

Weiter

Installation fertig, neu hochfahren.

Installationsmedien entfernen!

Bemerkung: Grafikmodi wechseln: STRG + ALT + <+/->

Neuanmeldung als root!

1. Webserver starten, yast, [System....] System – Runlevel Editor

   Die meisten Dienste können über Runlevel-Editor gestartet werden, apache starten!

   Dann Werte speichern, Webserver läuft

2. ftp-Server: ... Runlevel-Editor, ftp-Server ist ein Teil von inetd, (früherer inetd ist zum xinetd geworden) also: xinetd aktivieren. (damit sind pop3 und ftp gestartet)

3. ftp-Dienst nachkonfigurieren: Standard: Anonymes FTP ist möglich, man kann nur schreiben. Wir: anonymes ftp verhindern, nur angemeldete Benutzer zulassen, Konfigurationsdatei ändern.

Konfiurationsdateien stehen in /etc, bzw. in /etc/Sysconfig

konqueror starten, Wurzelverzeichnis anzeigen, /etc und dort: vsftpd.conf:
(zur Erinnerung: vsftp und ftpdir müssen installiert sein)

dort:

write_enable=YES

ftpd_banner: Begrüßungstext

local_enable=YES

local_umask=022 (ist das Problem!!! - bei manchen stört das)

chroot_local_user=YES

Hinweis: Homepage-Wartung: Homeverzeichnis auf Homepageverzeichnis setzen.

chroot_list_file=/etc/vstpd.chroot_list (Datei mit ftp-Benutzern, die ...)

anonymous_enable=NO
Dann: rcxinetd restart

Problem: Bei manchen läuft der ftpd nicht!

Später eventuell ftp-Server deinstallieren und installieren probieren.

Oder PC neu starten.

Wird gemacht, Billy lacht (:-))

NUN: Netzwerkkarte konfigurieren: Yast: Netzwerk, erkannte Karte [Ändern]
[Bearbeiten]
zwei Karten: äußere und innere, eth0 = äußeres device, IP-Adresse = Schuladresse, z.B: 193.170.211.45, 255.255.255.248
Rechnername: www, domainname: bgtulln.ac.at:

nameserver 193.171.123.14

Domainsuche 1: bgtulln.ac.at

Gateway: 193.170.211.46 (letzte Netzwerkadresse)

routingtabelle: Alle Netze, die hinter dem linux-Rechner liegen:

z.B.: 192.168.100.64 Gateway: 192.168.100.91 (innere Netzwerkkarte des linux-Rechners), mask: 255.255.255.224
IP-Weiterleitung YES

Beenden zum Speichern.

Nochmal auf Netzwerkdevices, NetworkCard, zweite Netzwerkkarte konfigurieren („innere“) - eth1
z.B.: 192.168.100.91, 255.255.255.224

Rechnername und Nameserver sind bereits konfiguriert

Speichern!

Rooting-Tabelle:

Hinweis: Wenn hier alle Routingeinträge stimmen, dann ist firewall-Konfiguration sehr einfach!

Karte ändern, bearbeiten, rooting-Tabelle

Wenn hinter dem linux-Rechner ein weiterer Server liegt, dann muss dieser im Netzwerksegment 192.168.100.64 liegen. Alle anderen Netze müssen nunmehr angeführt werden:

z.B.: 192.168.100.96 Gateway: 192.168.100.65, mask 255.255.255.224 eth1

also: auf eth1 raus auf 192.168.100.65, von dort in das Netz 192.168.100.96

IP-Weiterleitung yes

Auf der äußeren Karten sind mehrere IP-Adressen gebunden! Händisch machen: in / /etc/sysconfig/network

dort findet man: ifcfg-eth0

dort stehen die Daten für die erste Karte.

Cp ifcfg-eth0 ifcfg-eth0:1
Cp ifcfg-eth0 ifcfg-eth0:2

diese beiden Dateien müssen editiert werden:

dort die beiden IP-Adressen ändern! IPADDR='193.170.211.44' usw. für mail-Server und ftp-Server

Als nächstes: Webserver testen:

http://localhost/phpMyAdmin

läuft ...

https://127.0.0.1:10000 webmin läuft!

NUN: YAST Netzwerkdienste, Netzwerkdienste inetd, Aktivieren: POP3, ftp (vsftpd!) Status ändern!

Dann rcxinetd restart OK!

NUN: Konfiguration Firewall:

YAST
Sicherheit und Benutzer
Firewall
externe Karte eth0 wählen
inneres Netz ist die eth1

für weitere IP oder weitere Karten nachbearbeiten – Zeilen dazuschreiben!

Dienste angeben, die durchgehen sollen: http, https, smtp, pop3, ssh. Zusätzliche Dienste:
(Experten) Portadressen anschreiben: 80 20 21 100000 3306

(Nummern aus services auslesen)

weiter

Masquerade einfach anhaken, internes Netz schützen weghaken.

Weiter

4. Seite einfach lassen

dann speichern und aktivieren.

Als nächstes:

Alle Konfigurationsdateien aus /etc/sysconfig lassen sich unter yast, system, Editor für sysconfig-Dateien verändern!

Network, Firewall, SuSE Firewall2, alle Einträge da:

FW_MASQ_NETS 0/0 dh. Maskiert alles.
(0 für alle Netze, 0 für alle Adressen)

Bei mehreren Karten: FW_DEV_EXT: eth0 eth0:1 eth0:2
beim internen Device genauso!

Achtung: eine Reihe von Variablen sind ausdokumentiert, daher müssen wir und die Datei ansehen:

/etc/sysconfig/SuSEfirewall2

dort folgende Variablen zulassen: FW_SERVICE_SQUID="YES" setzen

(auf lange Sicht der transparente Proxy)

dann: FW_REDIRECT="192.168.100.64/27, 0/0, tcp,80,3128 192.168.100.96/26,0/0, tcp,80,3128 10.0.0.0/0,0/0,tcp,80,3128"

maW: Alles was aus dem Netz 192.168.100.64 kommt und über tcp einen Port 80 abfragt, dann

wird diese Abfrage auf den Port 3128 umgebogen i.e. Auf den Proxy!

oder: 192.168.0.0/16 0/0,tcp,80,3128

/16 bedeutet mask: 255.255.0.0
/24 bedeutet mask: 255.255.255.0
/26 bedeutet mask: 255.255.255.196
usw.

3128 nach außen nicht offen!

22 telnet
25 smtp
110 pop3
80 http

oder so ähnlich.

Schließlich:

rcSuSEfirewall2 restart

Mit der Firewall sind wir noch nicht fertig: Problem: Von der inneren Adresse ist der mailserver noch nicht erreichbar. Zugriff auf Mailserver erfolgt über offizielle IP-Adresse, damit erfolgt ein Sprung von eth1 auf eth0 und das verhindert die neue Firewall!

Lösung: Wenn man vom inneren Netz kommt, dann muss die Anfrage auf die innere Adresse gehen:

a) hosts-Datei ändern – gibt es auf jedem Windows – Rechner – SUCHEN!

Datei in C:\WINDOWS\Sysgtem32\drivers\etc

Copyright (c) 1993-1999 Microsoft Corp.
#
Dies ist eine HOSTS-Beispieldatei, die von Microsoft TCP/IP
für Windows 2000 verwendet wird.
#
Diese Datei enthält die Zuordnungen der IP-Adressen zu Hostnamen.
Jeder Eintrag muss in einer eigenen Zeile stehen. Die IP-
Adresse sollte in der ersten Spalte gefolgt vom zugehörigen
Hostnamen stehen.
Die IP-Adresse und der Hostname müssen durch mindestens ein
Leerzeichen getrennt sein.
#
Zusätzliche Kommentare (so wie in dieser Datei) können in
einzelnen Zeilen oder hinter dem Computernamen eingefügt werden,

```
# aber müssen mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#      102.54.94.97     rhino.acme.com          # Quellserver
#       38.25.63.10     x.acme.com              # x-Clienthost

127.0.0.1       localhost
192.168.100.91          mail.bgtulln.ac.at
```

b) Firewall – Skript von vorhin:

Ganz unten: (Zeile 704 ...)

FW_CUSTOMRULES=““ auskommentieren, die darüber stehende Zeile dekommentieren:
SuSEFirewall-custom in /etc/sysconfig/scripts

dort stehen die iptables ...

fw-custom-before-masq() ändern:

```
internel-net=“192.168.100.64/26 192.168.0.0/16 10.0.0.0/8“
external_ip=“193.170.211.45 193.170.211.44 193.170.211.43“
internal_ip=“192.168.100.91“
for net in $internal_net
do
  for   ip in $external_ip
  do
     iptables -t nat -I PREROUTING 1 -s $net -d $ip -j DNAT - -to $internal_ip
  done
done
true
```

-t Tabelle
-I Einfügen
1 an der 1. Stelle
-s Source
-d Destination
-j Job
DNAT Zieladresse wird umgesetzt
-- weil Job ein Unterbefehl ist ... zwei – Zeichen!
auf interne IP-Adresse!

True bleibt

NUN Squid:

/etc/squid/squid.conf

acl: Accesslist suchen:

acl schule (beliebiges Wort) src (Source-Netze)

vor

#httpd_access deny all

Zeile 1702: Empfohlene Minimalkonfiguration:

Ergänzen

acl schule src 192.168.0.0/16
acl schule src 10.0.0.0/8

dann darunter

oder zwei Zeilen dekommentieren

1765:

http_access allow localhost
http_access allow schule
http_access deny all

NUN zum transparenten Proxy:

Zeile 2068:

httpd_accel_port 80
httpd_accel_port virtual

Zeile: 2095:

httpd_accel_with_proxy on

und darunter – einige Zeilen: httpd_accel_uses_header on
(ca. Zeile 2120)

Zeile 992:

redirect_program /usr/squid/squidGuard

Nun zum SquidGuard:

wird verschoben, da es schon zu spät ist.

NUN: Postfix:

Postfix installieren.

Ist der Mailserver, verwendet viele Module von sendmail:

Netzwerkdienste, Mail Transfer Agent

Verbindungsart permanent, Virusüberprüfung aktivieren

keinen Mailserver angeben!

Eingehende Mail: entfernte SMTP Verbindungen akzeptieren,
Mail von root weiterleiten an: nuss ....

Weiter Beenden.

Nun: SysconfigEditor aufrufen: System SysconfigEditor

Network
Mail
Postfix:
POSTFIX_LOCALDOMAINS mail.bgtulln.ac.at, bgtulln.ac.at,

Dann Authentifizierung verlangen:

POSTFIX_SMTP_AUTH_SERVER usw.....

später auf YES setzen

dann beenden

Konfigurationsdatei: in /etc/postfix

main.cf:

Fehler ausbessern:

myhostname
mydomain

funktionieren nicht so, wie es soll!

Hinten in der Datei sind die Variablen aufgeführt:

myhostname steht dort
mydomain muss händisch eingefügt werden:

mydomain = bgtulln.ac.at

!!!

dann speichern

noch einmal main.cf:

ziemlich weit oben: Zeile ca. 248

mynetworks nötig, weil postfix Mails nur aus dem eigenen Netzwerksegment verschickt.

Dazu mynetworks verwenden:

mynetworks=10.0.0.0/8, 192.168.0.0/16

eventuell auch fremde IP-Adresse eintragen, fremde eMail-Namen vergeben etc. für Versand von außen.

NUN: Rechner einmal neu starten?

Nachsehen im Runlevel-Editor!

(YAST SYSTEM Runlevel Editor)

Squid und MySQL starten.

Es fehlt noch das Update:

Frage: scannt der avguard auch alle Dateien, die über den Squid laufen?

NUN Update über CRON-Job:

/etc/cron.daily

kopieren irgendeine Datei

cp clean_catman virenupdate

mcedit virenupdate

Da steht eine Menge drinnen, was kein Mensch braucht – alles löschen

antivir - -update

antivir ist vorgefertigtes script, alles was in cron.daily drinnen steht wird einmal täglich ausgefüjhrt.

Das nächste: Online-Update von SuSE: Yast Software Online-Update – Problem:
Internetverbindung nötig, geht erst in der Schule.
Vollautomatisches Update, Zeit einstellen, OK, und das war es.