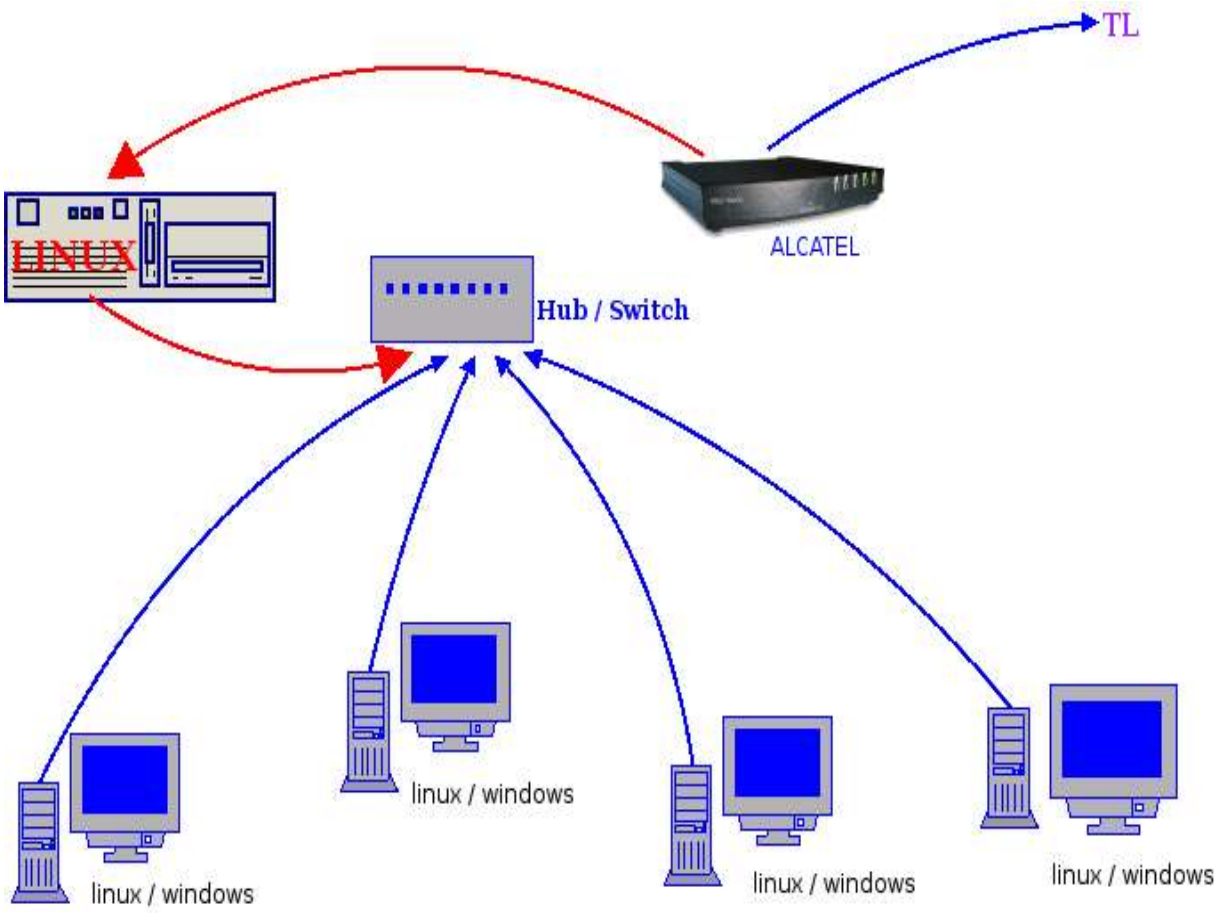
איך להפוך מחשב לינוקס לראוטר/חומת-אש

מבוא:

מה עושה ראוטר ?

משתף חיבור לאינטרנט, ומאפשר לכמה מחשבים לגלוש בו זמנית, ללא צורך בקו טלפון נוסף או חשבון נוסף אצל ספק האינטרנט.



למה לא לקנות ראוטר מוכן (קופסה) ?

ראוטר "חומרה" אינו מאפשר ל "פריק המחשבים" להנות מאין סוף האפשרויות שקיימות בלינוקס, בנוסף אנו משתמשים במחשבים ישנים מאד, ללא הוצאה כספית.

עד כמה אמין יהיה הראוטר שאבנה ?

נסיון אישי – הראוטר בביתי עובד למעלה משנתיים, ללא טיפולים מיוחדים (מצורפת תמונה).

המדריך נכתב ע"י מיקי 10/2004

כמו שאתם רואים, אין צורך בכונן סידי, כונן דיסקטים, מקלדת עכבר ומסך, לאחר ההתקנה.

מתחילים בעבודה:

החומרים הדרושים-

מחשב כדוגמת P133Mhz הכולל 24Ram זכרון

2 כרטיסי רשת

כונן סידי ו/או כונן דיסקטים, רק לצורך ההתקנה.

בחירת ההפצה:

מנסיון, RH לסוגיו כולל clarkconnect דורש זיכרון מינימום של 24 מגה, דביאן וסלאקוור מסתפקים בפחות, אז החלטתכם תלוייה בחומרה שבידכם.

**** אני אדגים כאן את קינפוג ההפצה שבחרתי בזמנו, RH7.3 , אמור לעבוד גם על הפצות אחרות אם כי מצריך שינויים . החיבור הוא ADSL + מודם אלקטל.**

התקנה:

חשוב מאד להתקין את החבילות הקשורות לרשת, אין צורך להתקין KDE או ממשק גראפי כלשהו,

כמובן בתלות בגודל הדיסק הקשיח שלכם, תוכלו לבחור.

לאחר ההתקנה:

** רק ב- RH , יש להפעיל ntsysv כ- root, להוריד את הכוכבית מ- ipchains, ולסמן את iptables .

חיבור לאינטרנט:

בעלי מודם סמסונג או ECI , יכולים להשתמש ב- adsl-setup או ב- pppoeconfig , תלוי בהפצה, כמו כן מי שיש ברשותו אלקטל ומעוניין להופכו ל- pppoe לפי המדריך:

http://www.netguru.co.il/modules.php?op=modload&name=News&file=article&sid=53

יכול להשתמש בתוכנת החיבור שמגיעה "מהקופסה" .

אני השתמשתי בסקריפט של יריב, לא לשכוח להגדיר את כרטיס הרשת:

http://www.totaleclipse.co.il/adsl-hebrew.htm

לא הצלחתי לשתף אינטרנט ע"י שימוש בסקריפט, אז השתמשתי בזה:

```
#!/bin/sh
#######################################################################
#                                     #
#          IPTABLES Firewall Script 1.0              #
#           (c) by Peter Rektorschek                #
#                                     #
#######################################################################
# Internal and External Devices
dev_world=ppp0
dev_int=eth0
# Firewall IP
addr_int=192.168.0.1
# Internal Net
net_int=192.168.0.0/24
#######################################################################
# Load Modules
```

```
insmod ip_tables
insmod ip_conntrack
insmod ip_conntrack_ftp
insmod ipt_state
insmod iptable_nat
insmod ipt_MASQUERADE
#####################################################################
# Delete all Rules in Filtertable
iptables -F
#####################################################################
# Define new chains
iptables -N BLOCK
iptables -N EXT-INT
iptables -N INT-EXT
iptables -N ICMP-DENY
iptables -N INT-IF
iptables -N EXT-IF
iptables -A BLOCK -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A BLOCK -m state --state NEW -i ! $dev_world -j ACCEPT
iptables -A BLOCK -j DROP
iptables -A INPUT -j BLOCK
iptables -A FORWARD -j BLOCK
#####################################################################
# Point to chains
iptables -A INPUT -i lo -j ACCEPT
iptables -A INPUT -i $dev_int -s $net_int -j INT-IF
iptables -A INPUT -d ! $addr_int -i $dev_world -s ! $net_int -j EXT-IF
iptables -A INPUT -j DROP
iptables -A FORWARD -d ! $net_int -i $dev_world -s $net_int -j INT-EXT
iptables -A FORWARD -d $net_int -i $dev_int -s ! $net_int -j EXT-INT
iptables -A FORWARD -j DROP
```

```
iptables -A OUTPUT -j ACCEPT
# Chain Rules
iptables -A EXT-INT -j DROP
iptables -A EXT-IF -i ! $dev_world -j DROP
iptables -A EXT-IF -p tcp --dport 22 -j ACCEPT
iptables -A EXT-IF -j DROP
iptables -A INT-IF -j ACCEPT
# NAT Rules
# Standard Routing
iptables -A POSTROUTING -t nat -o $dev_world -j MASQUERADE -s $net_int
# Port Forwarding
# Enable IP-Forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward
adsl-il start
```

הסקריפט מאפשר לכם כניסה מהרשת הפנימית דרך SSH לראוטר.

רצוי לקרוא על אפשרויות iptables ו/או להשתמש בסקריפטים מוכנים של חומת-אש הקיימים באינטרנט.