

# RELAZIONE\_VIRTUALBOX

Basso Nicola

## Contents

<b>Virtualbox, M0n0wall e l'architettura client-server</b>	<b>2</b>
INTRODUZIONE ↑	2
Descrizione VirtualBox	2
Descrizione M0n0wall	2
Obbiettivo	2
Utilità varie ↑	3
Download links	3
Funzioni utili Virtualbox	3
Creazione VM Client ↑	3
Informazioni generali	3
Installazione OS client ↑	3
Configurazione OS Client ↑	12
Creazione VM Server ↑	15
Creazione VM Router ↑	17
Grafica sul Client ↑	21
Configurazione M0n0wall ↑	24
Configurare la rete ↑	29
Impostare l'ip del client	29
Impostare DMZ nel router ↑	30
Applicare modifiche della rete ↑	31
Aggiungere regole in M0n0wall ↑	32
Migrazione IP ↑	33
Restrizioni aggiuntive sul firewall ↑	34
Condizioni	34
Schema ↑	39
Realizzazione ↑	39
Servizi per il server ↑	40
Apache	40
Sostituzione FoxyProxy con SmartProxy ↑	43
VPN ↑	43
PPTP ↑	43
IPsec ↑	44
Client e server ↑	46
Sostituire IPsec con OpenVPN ↑	46
Software OpenVPN ↑	46
OpenVPN e la cifratura ↑	46
Connessione punto punto	46
Rete VPN tra LAN	52
SNMP ↑	52
Installare sul server MRTG ↑	52

Cacti ↑	55
Installare le dipendenze di cacti	55
Aggiungere un altro apparecchio nella rete ↑	56
Utilità e curiosità ↑	57
Possibili problemi	57
Curiosità varie ↑	58
Funzionamento librerie ↑	59
File utili ↑	59
Esercizio Cisco ↑	59
SPERIMENTAZIONE VLAN CON ROUTER CISCO	59
Avvio di OS linux e init.d ↑	60
Storia di CentOS ↑	60
TODO ↑	60

# Virtualbox, M0n0wall e l'architettura client-server

---

## INTRODUZIONE ↑

### Descrizione VirtualBox



Figure 1: Virtualbox logo

Virtualbox è un software che ci permette di emulare il funzionamento di altri sistemi operativi al di sopra di un altro che sarà il nostro “pc ospite”.

### Descrizione M0n0wall



Figure 2: M0n0wall logo

M0n0wall è un sistema operativo open source ora abbandonato che ci permette di gestire tutti gli aspetti avanzati di un router.

### Obbiettivo

Riuscire a creare un laboratorio virtuale completo:

- router con firewall, NAT e DMZ
- server fruitore di servizi in locale e all'esterno verso il laboratorio fisico
- svariati client virtuali, tra i quali alcuni vulnerabili per svariati attacchi da provare

### Informazioni aggiuntive

Software utilizzati per questa relazione:

- Atom (editor di testo)
- Notable (editor di note markdown)
- pandoc (comando per generare pdf da markdown)

```
pandoc --pdf-engine=xelatex -f markdown-raw_tex \
--highlight-style breezedark -V colorlinks -V toccolor=Red \
-s --toc --listings \
-V geometry:"top=2cm, bottom=1.5cm, left=2cm, right=2cm" \
--default-image-extension=.png -V papersize=a4 -V mainfont='DejaVu_Sans' -V fontsize=12pt
-H lists.tex -H head.tex \
-f markdown RELAZIONE_VIRTUALBOX.md -o RELAZIONE_VIRTUALBOX.pdf
```

Guida pandoc: [markdown2pdf\\_pandoc](#)

---

## Utilità varie ↑

### Download links

[Distribuzione debian](#)

### Funzioni utili Virtualbox

Screenshot Virtualbox: **R-CTRL + E**

Clonazione Virtualbox: **R-CTRL + T**

---

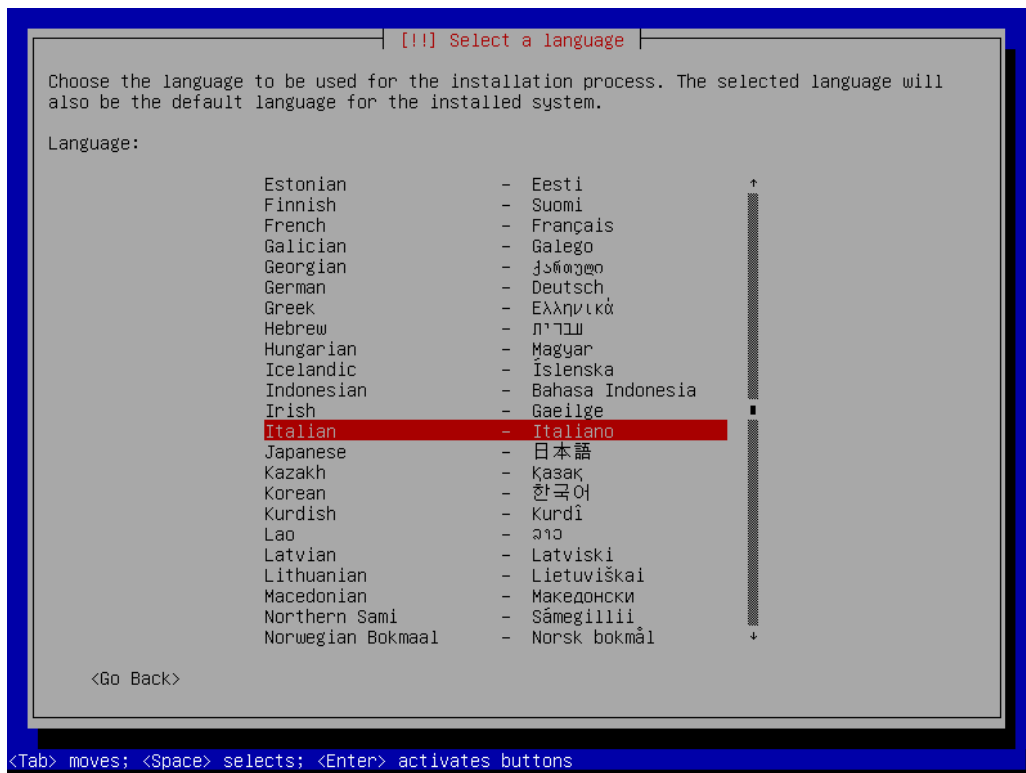
## Creazione VM Client ↑

### Informazioni generali

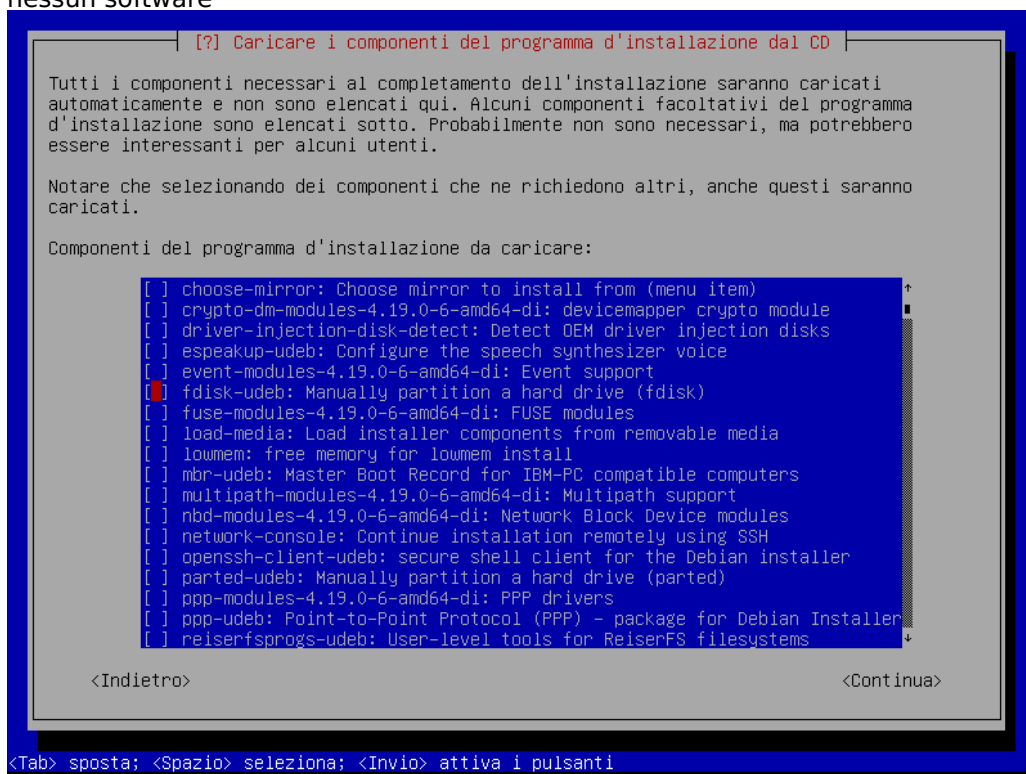
- nome VM = clientcognome
- password per tutto = lasolita
- Debian (64bit)
- RAM 1 GB
- HDD 4 GB (4.0 GB root, 368 MB swap)
- Rete con NAT

### Installazione OS client ↑

1. Creare nuova macchina virtuale
2. abilitare Network con NAT
3. expert install
4. Choose language
  1. Italiano

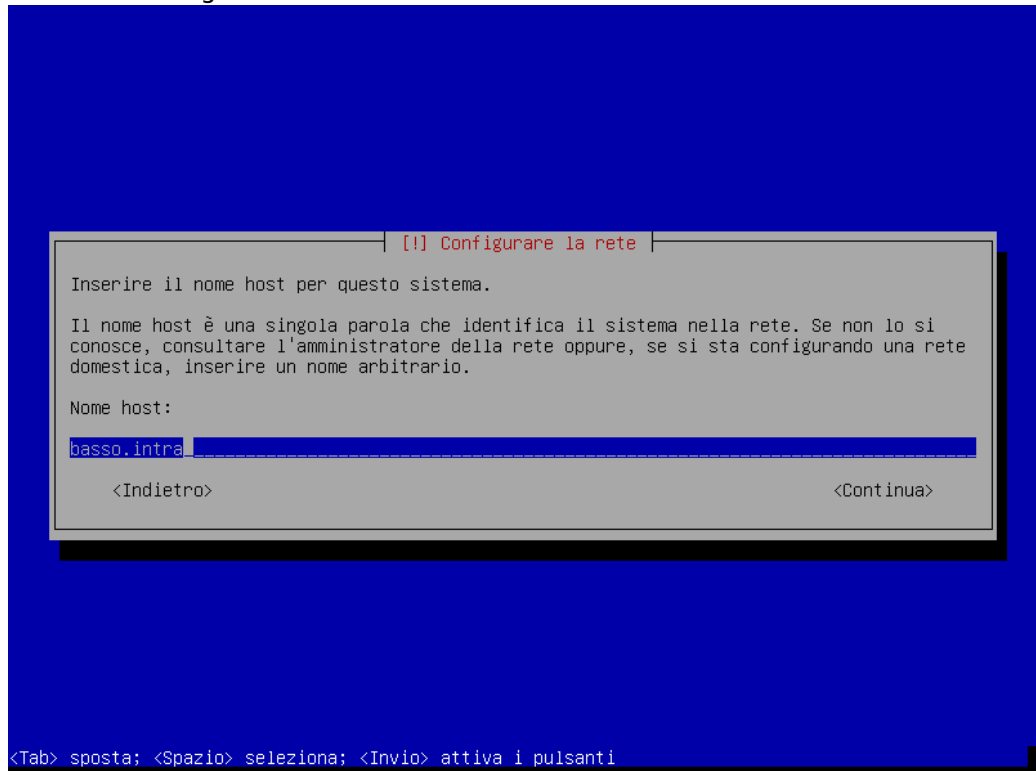


2. Italia - it\_IT.UTF-8
3. it\_IT e it\_IT@euro
4. UTF8
5. Configurazione tastiera
  1. Italiana
6. Caricare i componenti del programma
  1. nessun software



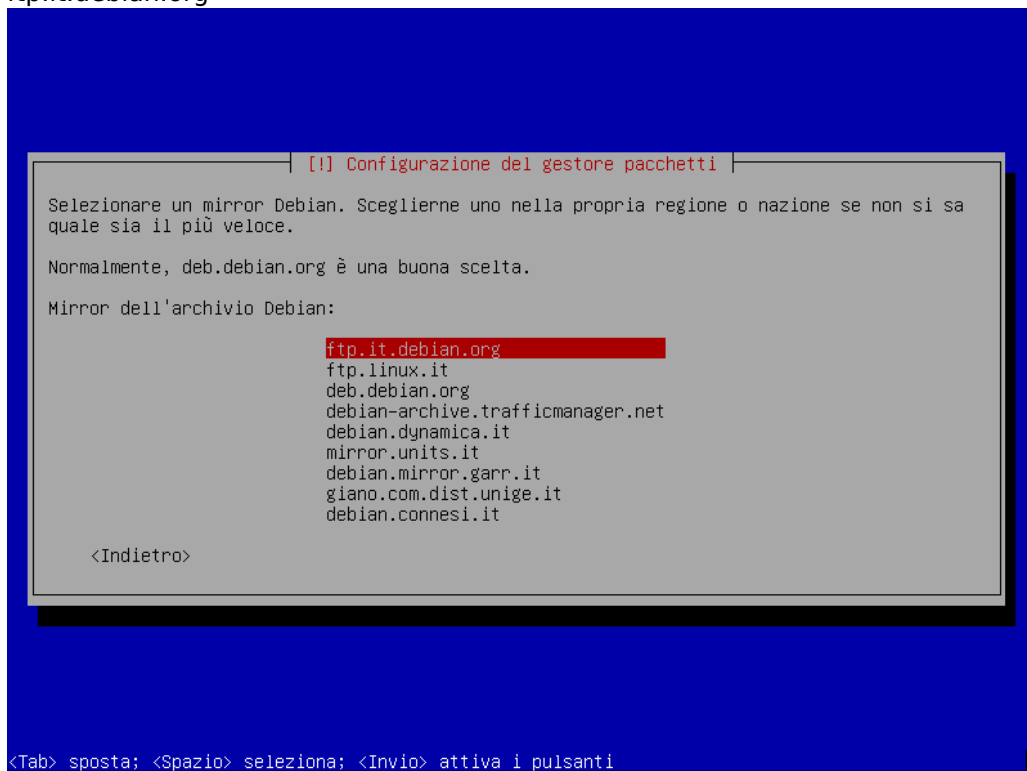
7. Rilevare l'hardware di rete
8. Configurare la rete
  1. DHCP
    1. dare "Sì"

2. opzione 3
3. hostname = cognome.intra

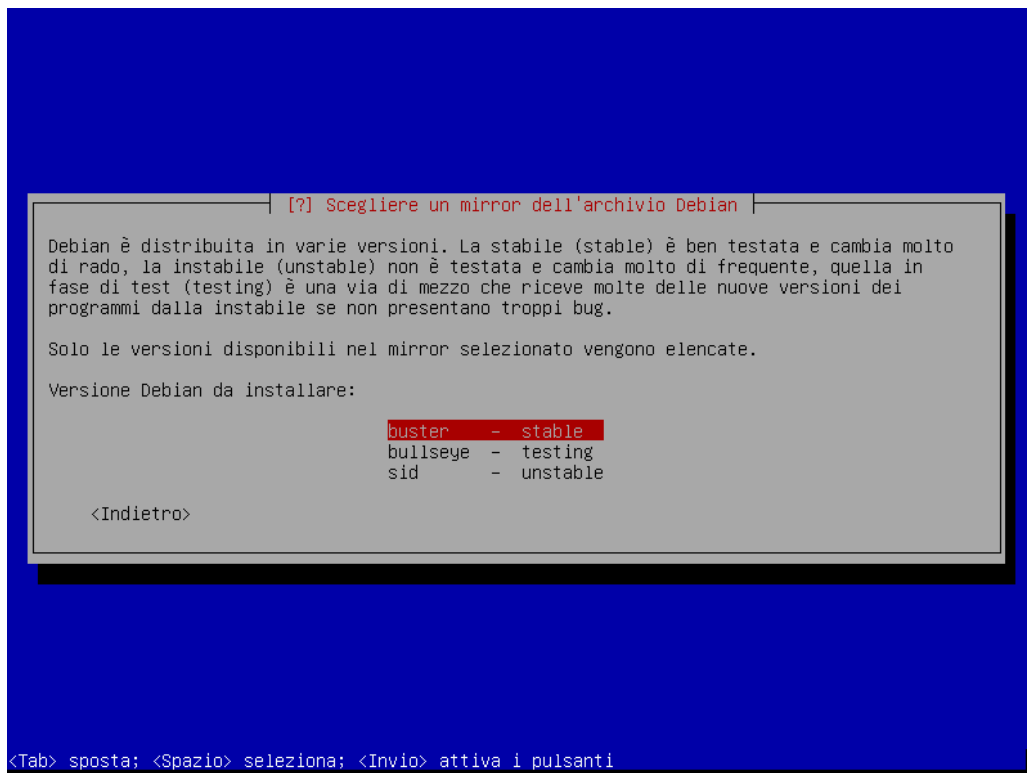


#### 9. Scelta distribuzione

1. http
2. Italy
3. ftp.it.debian.org



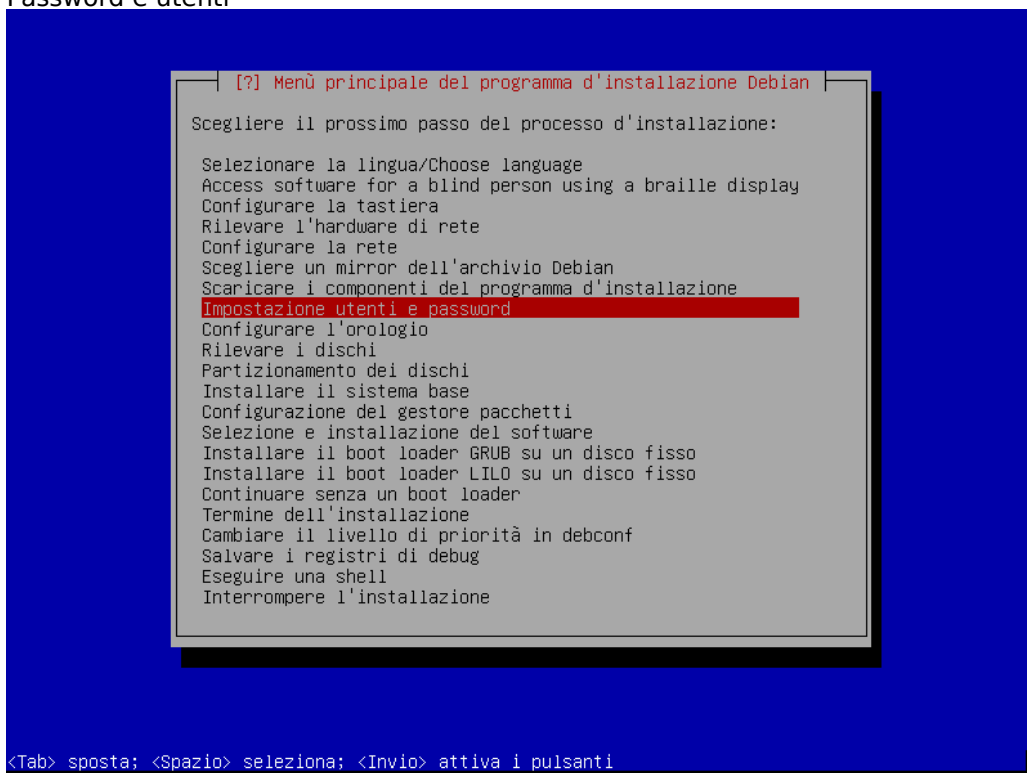
4. Archivio Debian: buster - stable (testing, unstable, experimental sono le rolling release)



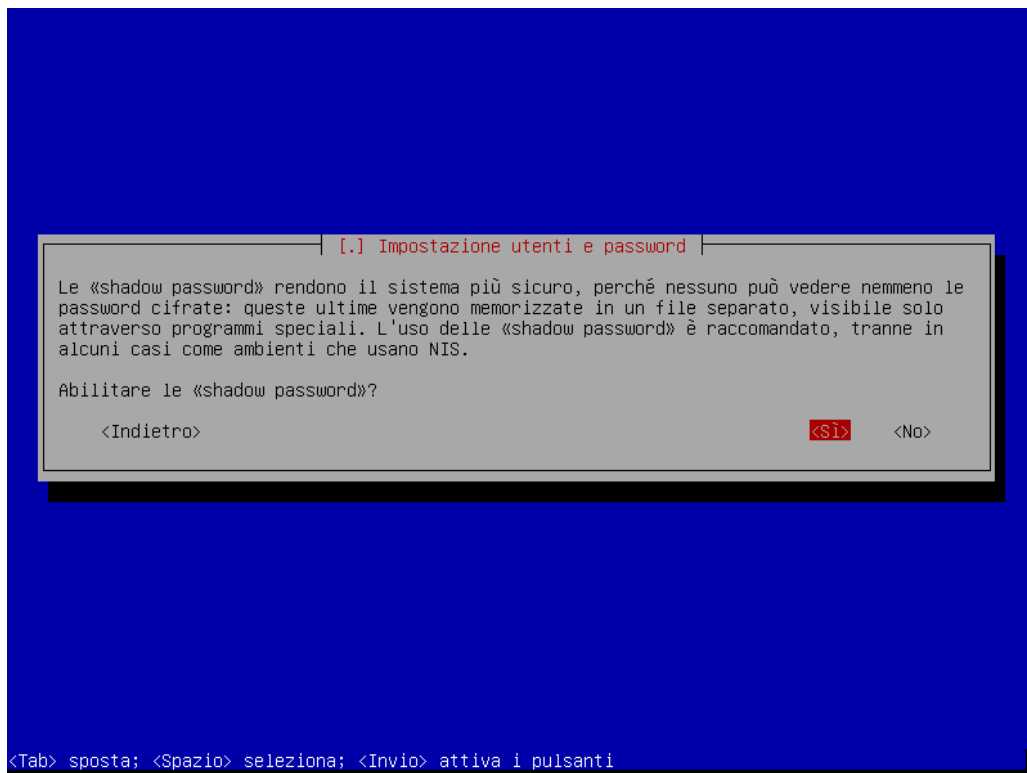
## 10. Scaricare componenti del programma installazione

1. Modalità esperta permette di installare i programmi dall'immagine ISO

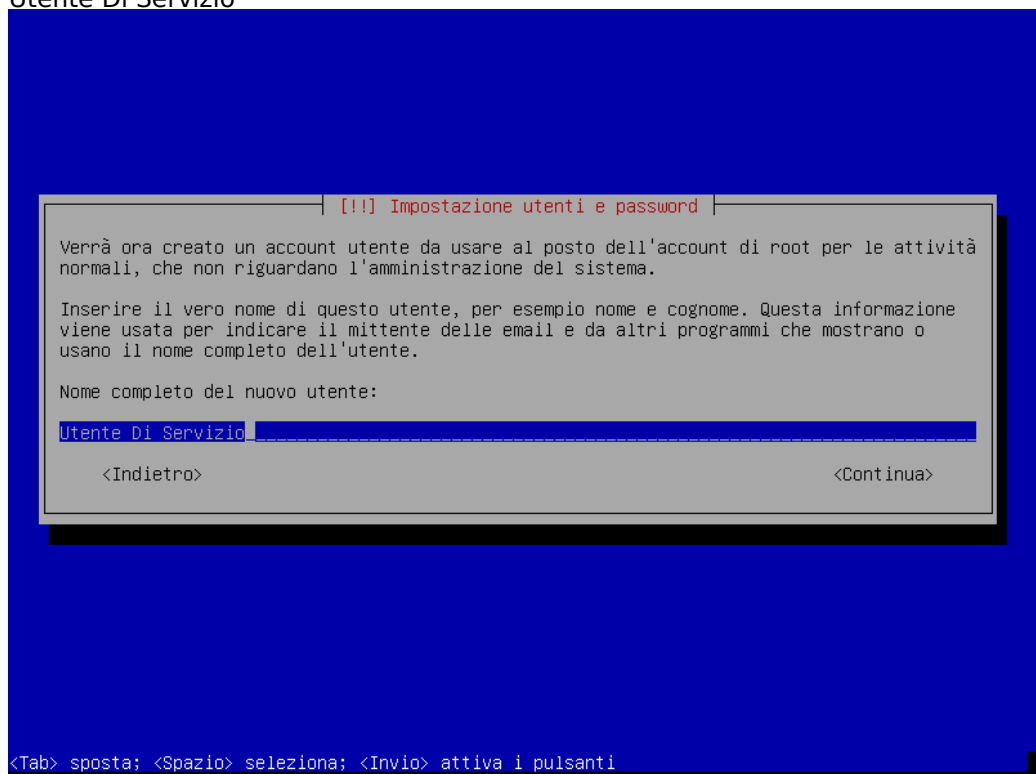
## 11. Password e utenti



1. nomi e password erano nello stesso file, ora sono separati
2. "shadow passowrd" abilitato (Si)

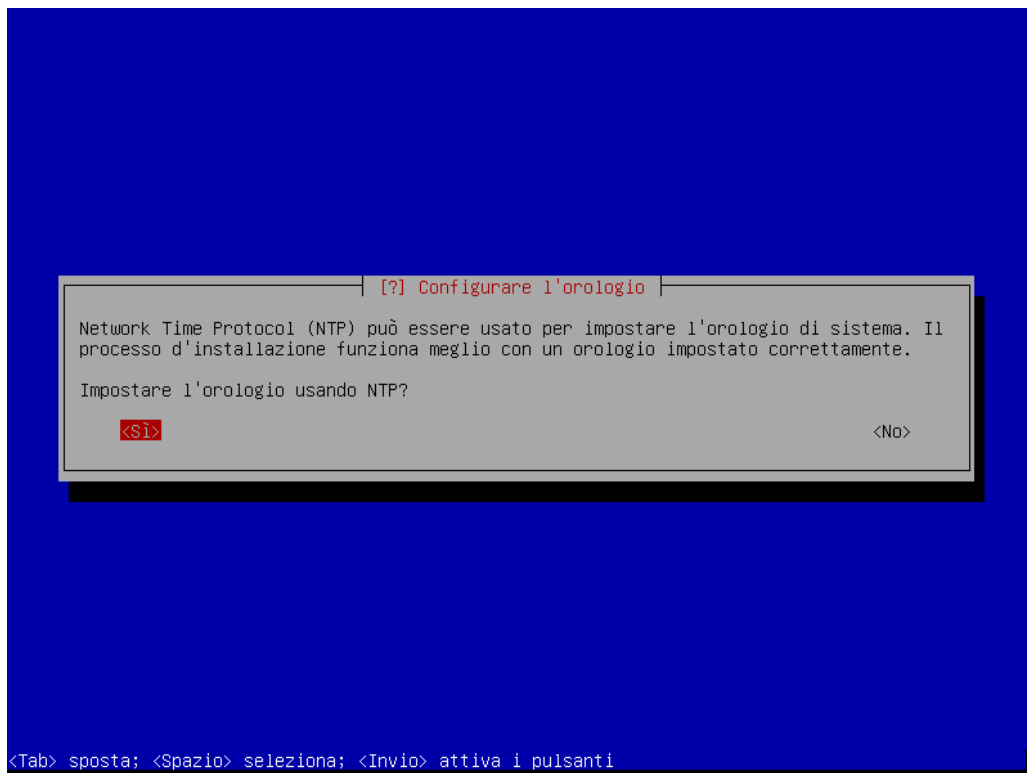


3. accesso a root abilitato (Sì) utente root deve essere in possesso di una sola persona (GDPR)
4. password: lasolita
5. Creazione utente normale
  1. Utente Di Servizio

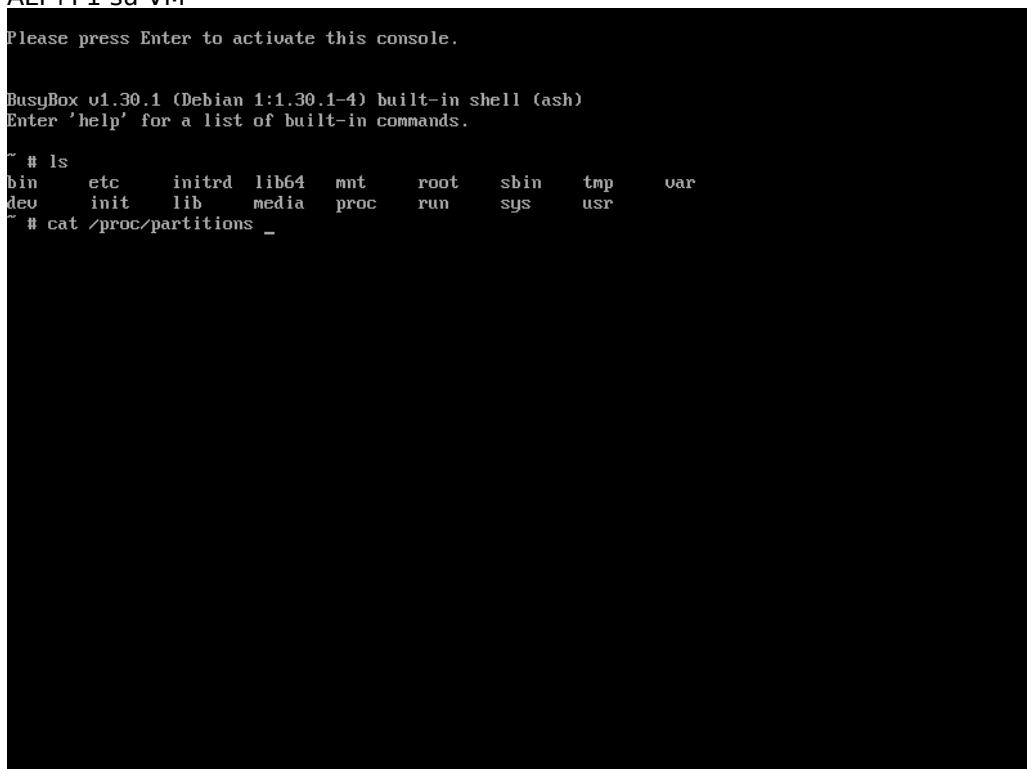


2. uds
3. lasolita
6. Configurare orologio (RTC = real time clock a batteria, GPS via satellite manda l'ora e localizzazione, Orologio telecomandato di Francoforte)





7. NTP = Si
  1. Consigliato (italiano)
  2. Europe/Rome (UTC Greenwich +1 inverno, +2 estate, CEST (central europe standard time))
8. Rilevare dischi (auto)
9. Partizionamento dei dischi
  - permette di usare il terminale grazie al multiplexing - 6 terminali + altre grafiche (CTRL+ALT+F1 F2 F3... F9(su pc lab))
  - ALT+F1 su VM



1. Manuale
  1. HDD nuovo da partizionare (opzioni disponibili: gpt e mbr)

## 2. Partizioni primarie

### 1. esteso

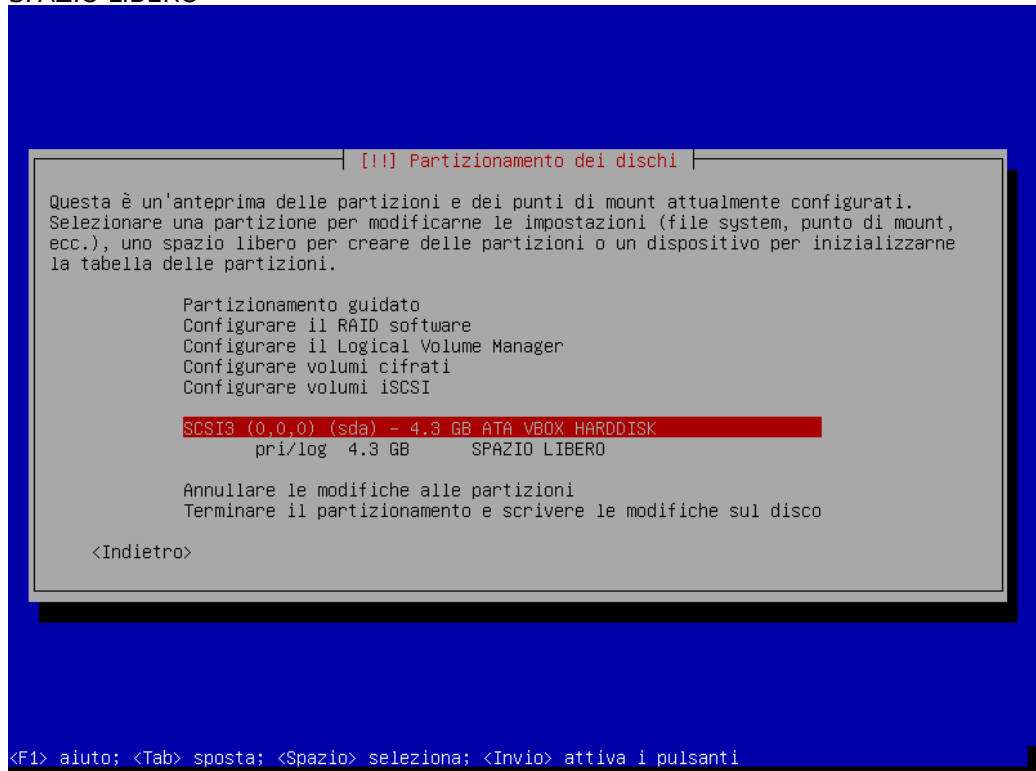
### 2. partizioni logiche

- 2TB e avvio OS EFI con partizionamento gpt (senza limiti sul partizionamento)
- tabella del partizionamento presente all'inizio del disco (gpt copiata anche a senso inverso alla fine del disco)

### 1. SCSI (0,0,0) (sda) - 10,7 GB

### 2. msdos

## 3. SPAZIO LIBERO



### 1. Creare nuova partizione

### 2. 4.0 GB

### 3. Primaria (mbr)

### 4. Inizio (btrfs per i dischi flash per sistemi ibridi, FAT va a leggere i dati nella prima parte chiavetta usurandola)

### 5. Usare come ext4 (estesa con journaling)

### 6. Punti di mount: / (cartella di root) (mount: attacca il disco nel tree delle directory. Opzioni disponibili: root, home, swap)

### 7. attivare nelle opzioni di mount:

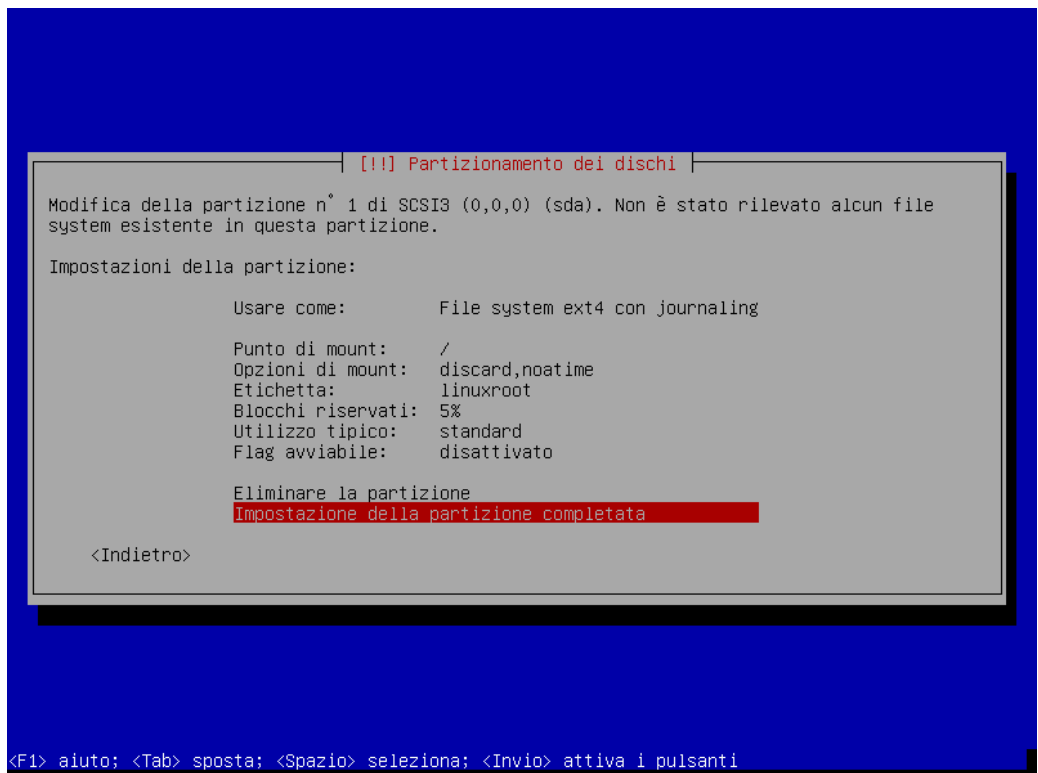
### 8. discard: rimuovere un file: dereferenziazione per poi essere sovrascritto da altri file, informa il disco della cancellazione, durante i periodi di inattività cancella i settori marchiati "discard" (dispositivi flash: scrivere e riscrivere: cancellazione costa risorse su zone già scritte)

### 9. noatime: lettura dei file: scrive le date (accesso, creazione, modifica, ...) sul file letto, quindi scrive e rallenta = alcuni servizi necessitano la gestione di atime (orario di accesso).

### 10. etichetta: linuxroot

### 11. Flag avviabile: utilizzato da DOS

### 12. Impostazione della partizione completata

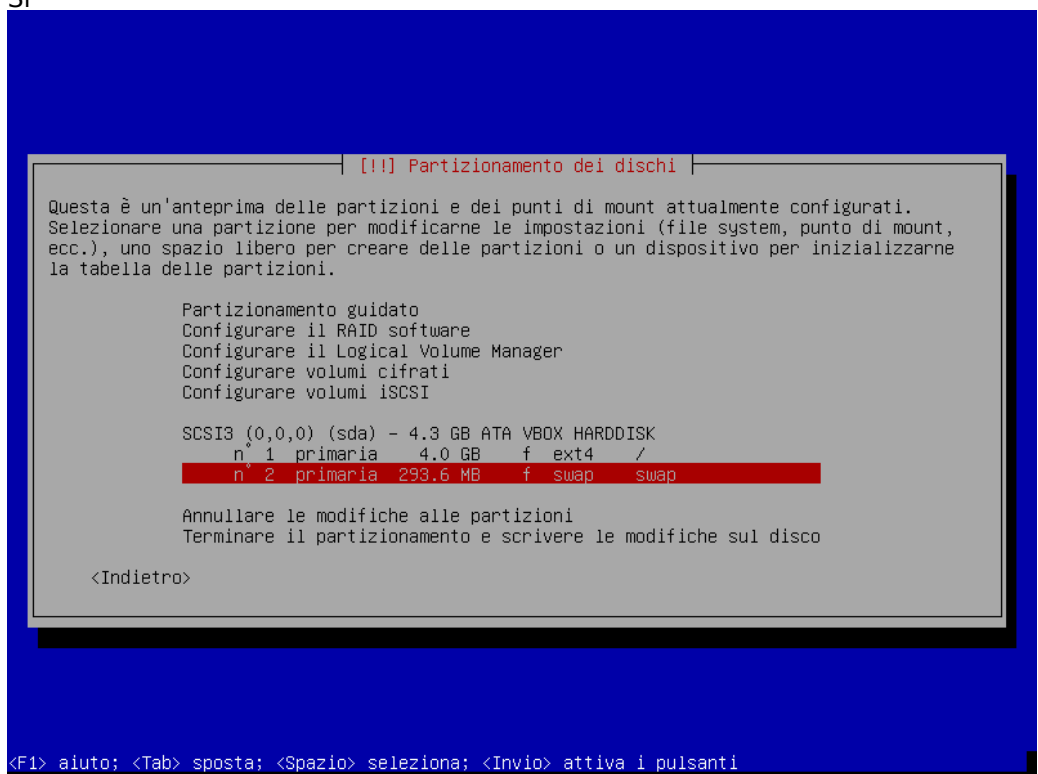


#### 4. SPAZIO LIBERO

1. Primaria
2. Fine
3. Area di swap: (memoria virtuale in winzoz), se la RAM è occupata va ad utilizzare il disco nella partizione dedicata

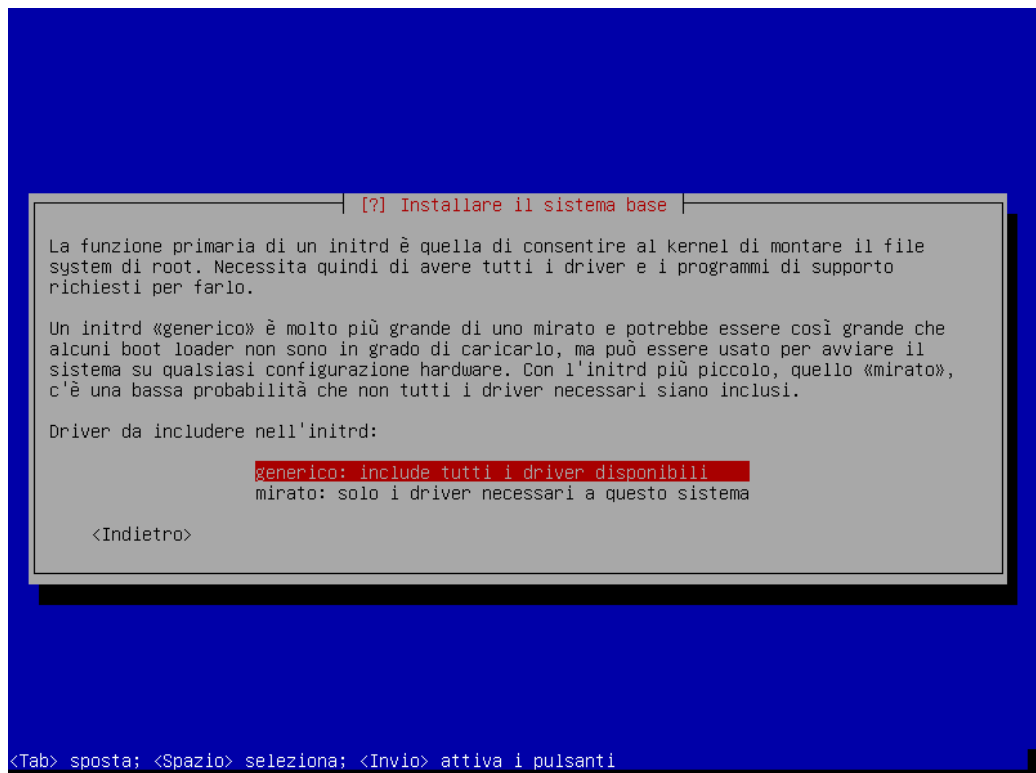
#### 5. Terminare le modifiche

1. Si



#### 2. Sistema di base

1. scelta del kernel: 1. Creazione macchina virtuale linux-image-amd64 (ultimo kernel stabile)
2. generico (mappatura del disco all'avvio, driver autoconfigurati)

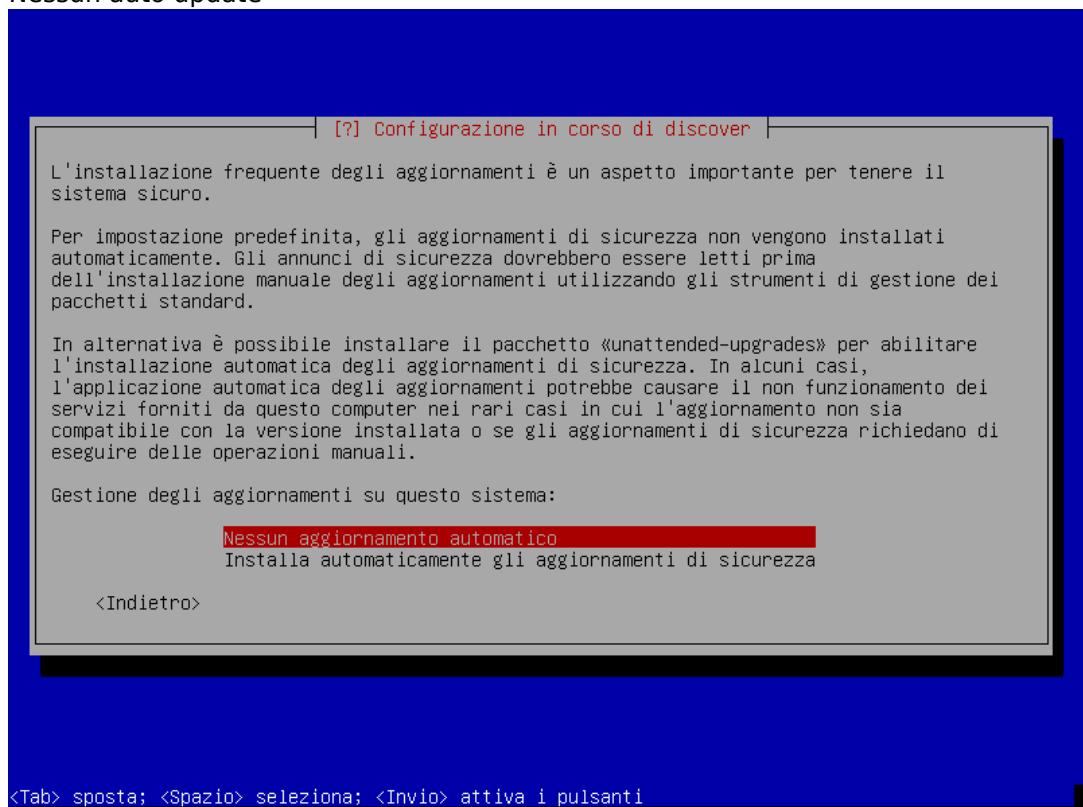


### 3. Gestore dei pacchetti

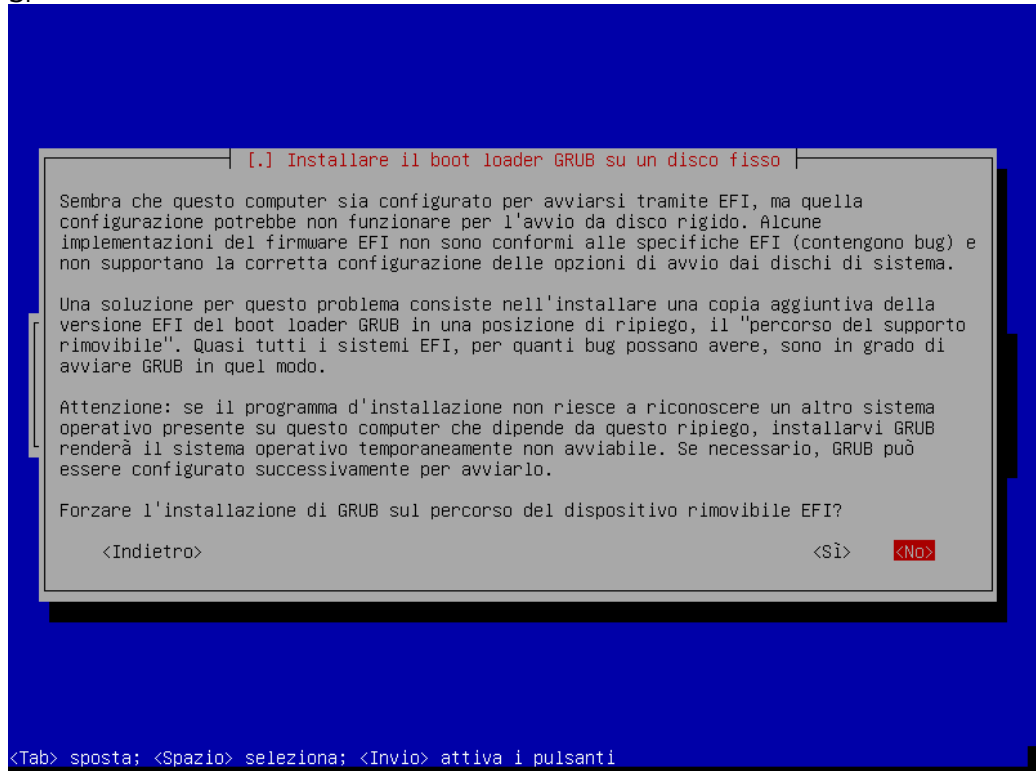
1. No (solo software libero)
2. Sì Software contrib (software libero con parti non libere) (installazione di Adobe Flash Player (libreria), (Font proprietari Microsoft
3. No repository sorgenti APT
4. Continua

### 4. Selezione installazione software:

1. Deselezionare tutto
2. Abilitare pacchetti VirtualBox
3. Nessun auto update



4. No partecipare alle statistiche
5. Deseleziona tutto
5. Installare Boot loader GRUB (GRUB è un OS per avviare gli altri OS)
  1. Installare boot loader GRUB nel master boot record (prima parte del disco che serve ad avviare l'OS)
    - BIOS legacy: letto primo settore del disco e viene mandato in esecuzione
    - BIOS EFI: legge il disco per trovare partizioni EFI, carica un file EFI in memoria
  1. Si



2. /dev/sda
3. Forzare l'installazione di GRUB su dispositivo rimovibile EFI? No
  - EFI: partizionamento da 100 MB nella prima parte del disco formattato in gpt
6. Terminare l'installazione
  1. Orologio di sistema da impostare su UTC? Si
    - Winzoz: locale
    - Linux: UTC
  1. Continua
    - (RIMUOVERE IL CD DAL LETTORE VIRTUALE SE USATA UNA ISO)

## Configurazione OS Client ↑

1. TAB COMPLETITION: doppio tab per completare le parole sul terminale
2. Segnalazione dell'integrazione del puntatore del mouse
3. clientcognome login: uds
4. password: lasolita
5. UTENTE NORMALE
  1. pwd : print working directory
  2. df -h : visualizza lo stato dell'hard disk
  3. sudo : super user do often
  4. su - : super user
  5. password di root: lasolita

```
Debian GNU/Linux 10 clientbasso tty1
clientbasso login:
```

Figure 3: Screenshot

```
Linux clientbasso 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
uds@clientbasso:~$ pwd
/home/uds
uds@clientbasso:~$ df -h
File system      Dim. Usati Dispon. Uso% Montato su
udev             480M      0      480M   0% /dev
tmpfs            99M      1,6M      98M   2% /run
/dev/sda1        3,7G    750M    2,7G  22% /
tmpfs            494M      0      494M   0% /dev/shm
tmpfs            5,0M      0      5,0M   0% /run/lock
tmpfs            494M      0      494M   0% /sys/fs/cgroup
uds@clientbasso:~$ su -
Password:
root@clientbasso:~# apt install less joe tcpdump mtr-tiny cowsay
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
less è già alla versione più recente (487-0.1+b1).
I seguenti pacchetti aggiuntivi saranno inoltre installati:
  libgdbm-compat4 libgdbm6 libpcap0.8 libperl5.28 perl perl-modules-5.28
Pacchetti suggeriti:
  filters cowsay-off perl-doc libterm-readline-gnu-perl | libterm-readline-perl-perl make
  libb-debug-perl liblocale-codes-perl
I seguenti pacchetti NUOVI saranno installati:
  cowsay joe libgdbm-compat4 libgdbm6 libpcap0.8 libperl5.28 mtr-tiny perl perl-modules-5.28
  tcpdump
0 aggiornati, 10 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 8.241 kB di archivi.
Dopo quest'operazione, verranno occupati 50,9 MB di spazio su disco.
Continuare? [S/n]
```

## 6. UTENTE ROOT

1. apt update
2. apt upgrade
3. (in caso di problemi: nano /etc/apt/sources.list)

deb <http://deb.debian.org/debian> buster main

deb-src <http://deb.debian.org/debian> buster main

```
deb http://deb.debian.org/debian-security/ buster/updates main
deb-src http://deb.debian.org/debian-security/ buster/updates main
```

```
deb http://deb.debian.org/debian buster-updates main
deb-src http://deb.debian.org/debian buster-updates main
```

7. apt install less joe tcpdump mtr-tiny cowsay (opzionali: bash-completion, dnsutils, netcat)

```
root@clientbasso:/home/uds# apt clean
root@clientbasso:/home/uds# history
 1 apt install less joe tcpdump mtr-tiny cowsay
 2 apt install sudo
 3 id
 4 id uds
 5 adduser uds sudo
 6 id uds
 7 exit
 8 apt clean
 9 clear
10 apt clean
11 history
root@clientbasso:/home/uds# cls
bash: cls: comando non trovato
root@clientbasso:/home/uds# apt update
Scaricamento di:1 http://security.debian.org/debian-security buster/updates InRelease [39,1 kB]
Trovato:2 http://ftp.it.debian.org/debian buster InRelease
Scaricamento di:3 http://ftp.it.debian.org/debian buster-updates InRelease [49,3 kB]
Lettura elenco dei pacchetti... Fatto
E: Il file Release per http://security.debian.org/debian-security/dists/buster/updates/InRelease non
è ancora valido (non valido per 5g 14h 4min 27s). Gli aggiornamenti per questo repository non verranno
applicati.
E: Il file Release per http://ftp.it.debian.org/debian/dists/buster-updates/InRelease non è ancora v
alido (non valido per 5g 15h 37min 8s). Gli aggiornamenti per questo repository non verranno applica
ti.
root@clientbasso:/home/uds# apt upgrade
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
Calcolo dell'aggiornamento... Fatto
0 aggiornati, 0 installati, 0 da rimuovere e 0 non aggiornati.
root@clientbasso:/home/uds# _
```

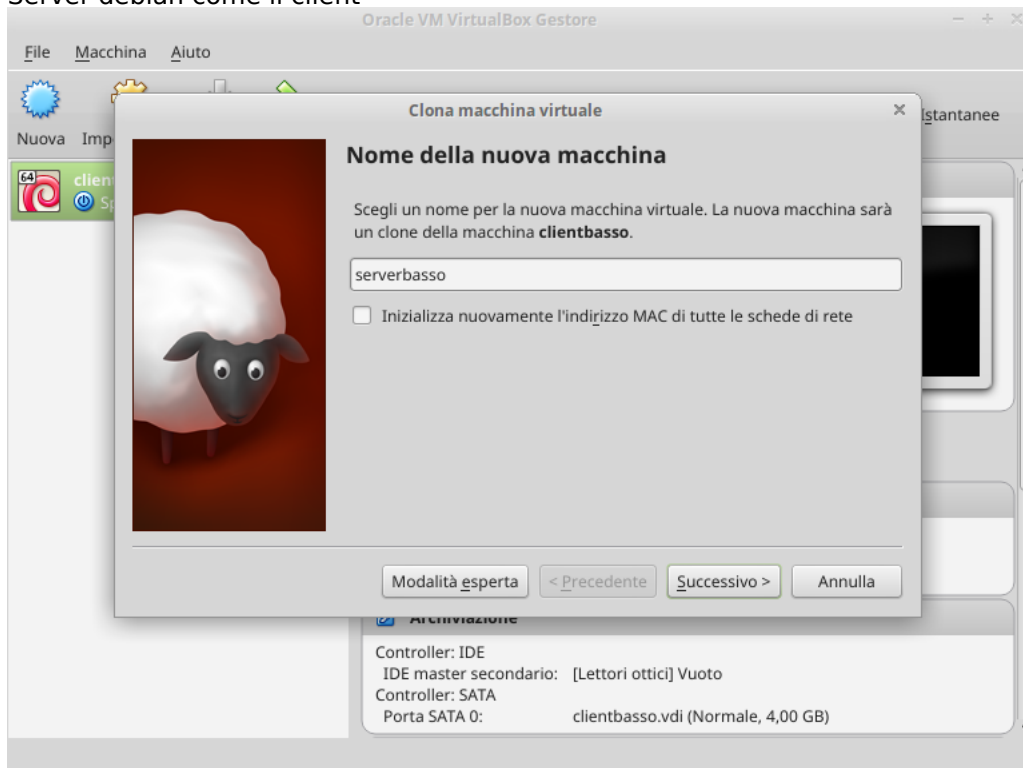
- pacchetti aggiuntivi: librerie mancanti per i programmi selezionati -> DIPENDENZE INCLUSIVE
- contesa dei software: propone la scelta, configurandone la scelta scartata -> DIPENDENZE ESCLUSIVE

1. S
2. cowsay : non funziona perchè i giochi non esistono per root
3. apt install sudo
  - SUDO permette di usufruire di azioni da amministratore da parte dell'utente normale senza sapere la password di root ma usando la propria (Wireshark richiede accesso hardware alla scheda di rete)
  - crea gruppo sudo
1. id : mostra i gruppi a cui appartiene l'utente corrente
2. id uds : mostra i gruppi a cui appartiene all'utente
3. adduser uds sudo : iscrive un utente al gruppo
4. id uds : controllo se è su sudo
5. exit
6. id
7. exit
8. relogin con uds lasolita
9. id : ora uds è sudo
10. sudo -s
  1. password
11. apt clean : configurazione di sistema non viene rimossa, nel caso di una reinstallazione la configurazione rimuove i file superflui

12. apt purge nomeprogramma : rimuove programma, config di sistema MA non configurazione utente

## Creazione VM Server ↑

1. Server debian come il client



1. spegnere la macchina da amministratore
  1. la GUI da la possibilità di spegnere la macchina da sudo, mentre da CLI serve per forza sudo
  2. shutdown -h now (oppure sudo shutdown -h now da utente uds)
2. clonare la macchina virtuale *clientcognome*
  1. CTRL + O o Pecora Dolly nel menu a tendina
  2. servercognome
  3. ABILITARE "Inizializza nuovamente l'indirizzo MAC di tutte le schede di rete", (serve per sperimentare lo stesso sistema su sistemi differenti ma con MAC uguale)
  4. Scegliere "Clone completo", copia tutti i file come disco separato.
3. nome sbagliato: modificare /etc/hostname: (i processi prendono l'hostname all'avvio, quindi lo mantengono durante l'esecuzione anche se nel durante viene modificato)
4. login uds
5. joe /etc/hostname



```
I /etc/hosts Row 1 Col 1
127.0.0.1 localhost
127.0.1.1 clientbasso.basso.intra clientbasso

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Joe's Own Editor 4.6 (utf-8) ** Type Ctrl-K Q to exit or Ctrl-K H for help **
```

6. mettere servercognome invece di clientcognome

```
I /etc/hosts (Modified) Row 2 Col 47
127.0.0.1 localhost
127.0.1.1 serverbasso.basso.intra serverbasso

# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

1. CTRL+K e poi X
7. modificare file /etc/hosts
  1. 127.0.0.1 = localhost (127.0.1.1 = sempre indirizzi di loopback (max 16 milioni))
8. ping 127.0.x.x
9. shutdown -h now

## Creazione VM Router ↑

### 1. Creare nuova macchina per monowall



1. configurazione macchina virtuale:
  1. routercognome
  2. BSD
  3. FreeBSD (32-bit)
  4. RAM = 128 MB
  5. HDD = 64 MB
2. Seleziona disco di avvio:
  1. /home/itis/InternetFiles/m0n0wall-generic-pc-1.8.1.iso
3. avvia e poi subito F12
4. Menu di monowall (può funzionare solo con floppy (config ) e CD (OS))

```
built on Wed Jan 15 13:32:38 CET 2014 for generic-pc-cdrom
Copyright (C) 2002-2014 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.
```

```
LAN IP address: 192.168.1.1
WAN IP address: (unknown)
```

```
Port configuration:
```

```
LAN    -> em0
WAN    -> sis1
```

```
m0n0wall console setup
```

```
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive
```

```
Enter a number: █
```

1. 7 - Install on HDD
2. ad0
3. y

```

2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host
7) Install on Hard Drive

Enter a number: 7

Valid disks are:

ad0      UBOX HARDDISK 1.0      64.00 MB

Enter the device name you wish to install onto: ad0

*****
* WARNING!
* m0n0wall is about to be installed onto the ad0 device.
* - everything on this device will be erased!
* - this cannot be undone!
*****

The firewall will reboot after installation.

Do you want to proceed? (y/n) █

```

#### 4. al riavvio spegnere subito

```

BTX loader 1.00  BTX version is 1.02
Consoles: internal video/keyboard
BIOS drive C: is disk0
BIOS 639kB/129984kB available memory

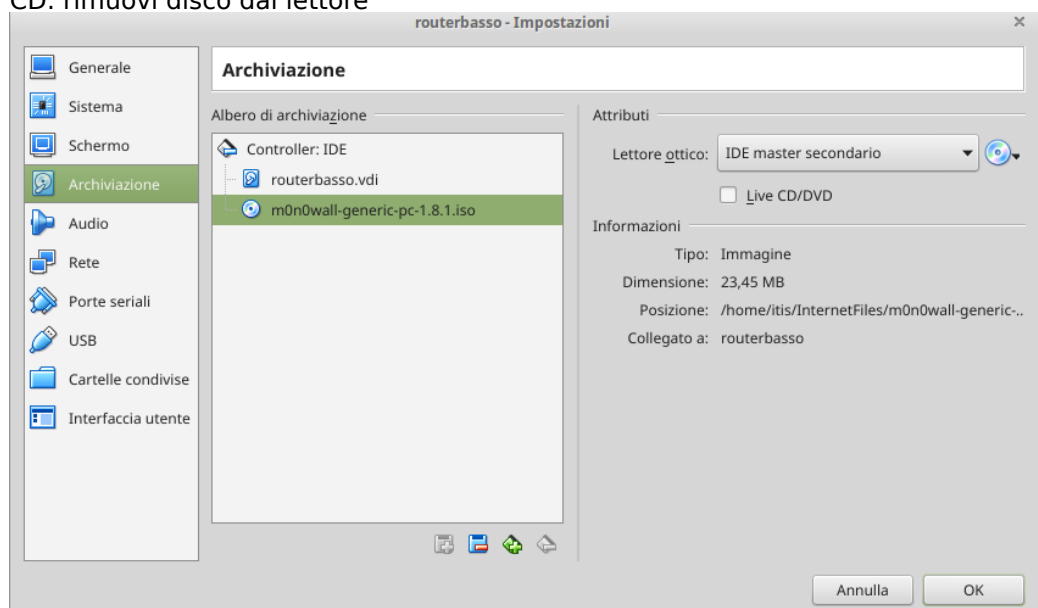
FreeBSD/x86 bootstrap loader, Revision 1.1
(root@bake.isc.freebsd.org, Sun Jun  2 23:37:39 UTC 2013)
/kernel text=0x894e08 data=0xdb7d4+0xa69e0 -
/boot/kernel/acpi.ko text=0x5a990 data=0x2580+0x1b4c syms=[0x4+0x9620+0x4+0xcc6e
]
^

```

#### 5. togliere CD da virtualbox

##### 1. Archiviazione

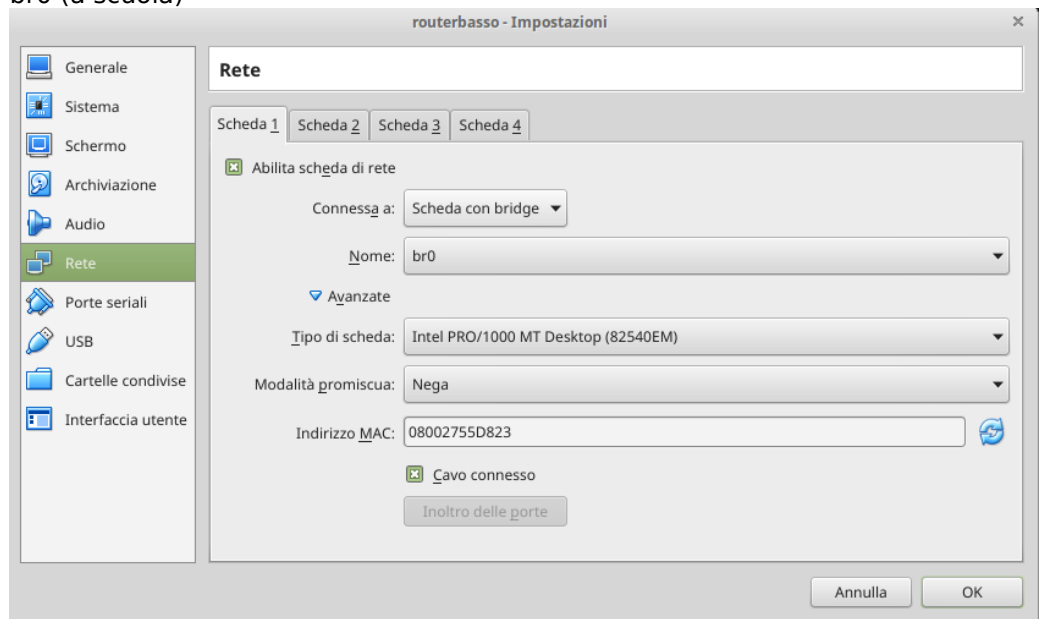
##### 1. CD: rimuovi disco dal lettore



#### 6. Scheda di rete 1

## 1. Scheda con Bridge

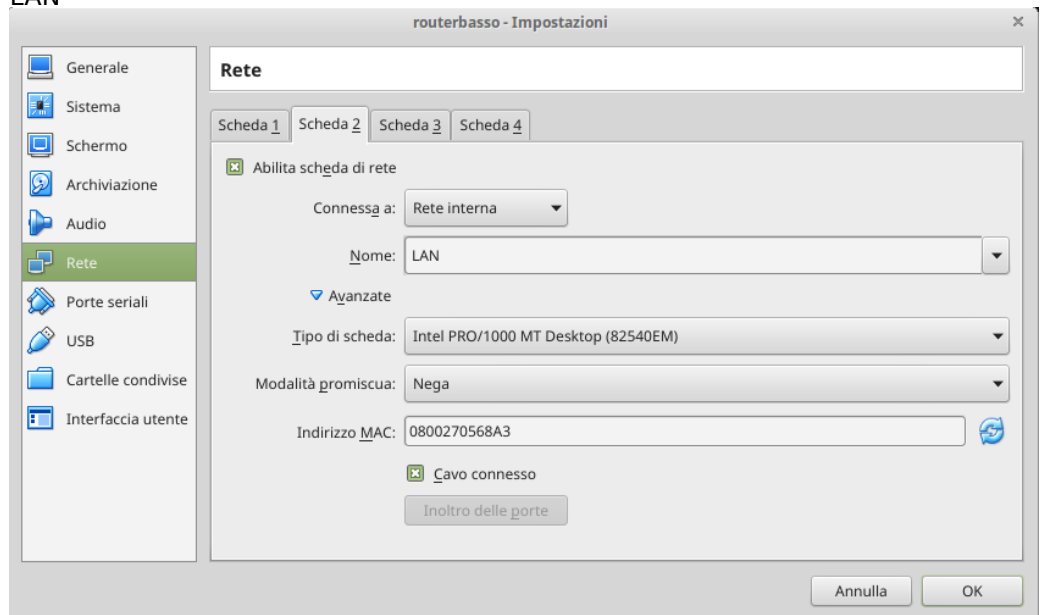
### 1. br0 (a scuola)



## 7. Scheda di rete 2

### 1. Rete interna

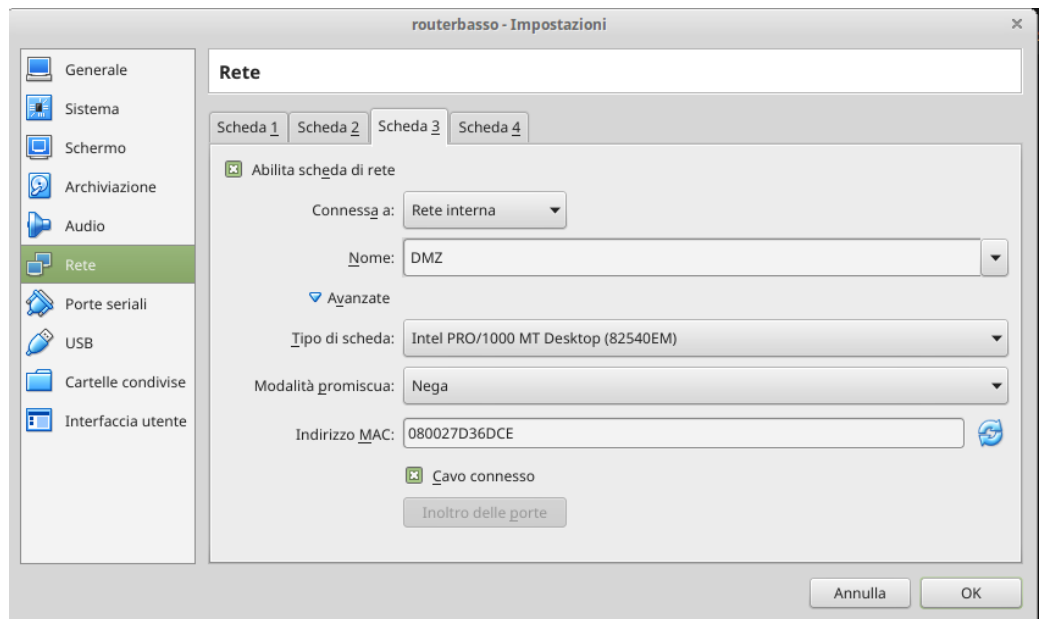
#### 1. LAN



## 8. Scheda di rete 3

### 1. Rete interna

#### 1. DMZ



9. riconosce che esiste un HDD non visualizzando la voce 7 dal menu
10. Non sono etichettate le porte LAN, WAN e DMZ
  1. 1 (Interfaces: assign network ports) (ci devono essere 3 interfacce: em0 em1 em2)

```
m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number: 1

Valid interfaces are:

em0      08:00:27:55:d8:23   (up)   Intel(R) PRO/1000 Legacy Network Connect...
em1      08:00:27:05:68:a3   (up)   Intel(R) PRO/1000 Legacy Network Connect...
em2      08:00:27:d3:6d:ce   (up)   Intel(R) PRO/1000 Legacy Network Connect...

Note that wireless LAN interfaces are not included in the list above;
they can be set up through the webGUI later on.

Do you want to set up VLANs first?
If you're not going to use VLANs, or only for optional interfaces, you
should say no here and use the webGUI to configure VLANs later, if required.

Do you want to set up VLANs now? (y/n) |
```

2. osservare i MAC address nelle impostazioni di rete di VirtualBox se sono in ordine come su monowall
3. richiesta di abilitare VLAN? n (è possibile avere monowall con 1 sola interfaccia e con VLAN attive per avere più reti)
4. LAN interface: em1
5. WAN interface: em0 (monowall si accontenta di 2 interfacce, ma useremo anche la DMZ)
6. opzionali: em2
7. ENTER
8. confermare? y (punto delicato: a casa usa DHCP, in laboratorio viene aggiunto un server DHCP in più, creando caos nello stesso dominio di broadcast. Però due server DHCP possono distribuire una porzione di indirizzi)

```

auto-detection. In that case, disconnect all interfaces before you begin,
and reconnect each one when prompted to do so.

Enter the LAN interface name or 'a' for auto-detection: em1

Enter the WAN interface name or 'a' for auto-detection: em0

Enter the Optional 1 interface name or 'a' for auto-detection
(or nothing if finished): em2

Enter the Optional 2 interface name or 'a' for auto-detection
(or nothing if finished):

The interfaces will be assigned as follows:

LAN    -> em1
WAN    -> em0
OPT1   -> em2

The firewall will reboot after saving the changes.

Do you want to proceed? (y/n) y

The firewall is rebooting now.

```

9. ENTER (per dare un'indirizzo IP alla WAN, monowall ha inviato una richiesta DHCP nella rete presente)

```

built on Wed Jan 15 13:32:38 CET 2014 for generic-pc
Copyright (C) 2002-2014 by Manuel Kasper. All rights reserved.
Visit http://m0n0.ch/wall for updates.

LAN IP address: 192.168.1.1
WAN IP address: (unknown)

Port configuration:

LAN    -> em1
WAN    -> em0
OPT1   -> em2 (OPT1)

m0n0wall console setup
*****
1) Interfaces: assign network ports
2) Set up LAN IP address
3) Reset webGUI password
4) Reset to factory defaults
5) Reboot system
6) Ping host

Enter a number:

```

10. Ora bisogna configurare gli host

## Grafica sul Client ↑

1. Avviare il clientcognome
  1. entrare con uds
  2. sudo bash
  3. serve gestore login grafico o desktop manager (mdm = mint desktop manager, lightdm = light desktop manager, kdm = kde desktop manager, nodm = avvia in automatico la sessione)
  4. serve un desktop enviro1. Creazione macchina virtualement (mate, lxqt, kde)
  5. serve il browser (firefox-esr è il nome del pacchetto creato per un litigio tra Mozilla e Debian per il logo (panda rosso))
    1. apt install lightdm mate firefox—esr

```

Debian GNU/Linux 10 clientbasso tty1

clientbasso login: uds
Password:
Last login: Thu Sep 26 12:27:43 CEST 2019 on tty1
Linux clientbasso 4.19.0-6-amd64 #1 SMP Debian 4.19.67-2+deb10u1 (2019-09-20) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
uds@clientbasso:~$ sudo bash
[sudo] password di uds:
root@clientbasso:/home/uds# apt install lightdm mate firefox
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
Nota, viene selezionato "mate-desktop-environment" al posto di "mate"
Il pacchetto firefox non ha versioni disponibili, ma è nominato da un altro
pacchetto. Questo potrebbe indicare che il pacchetto è mancante, obsoleto
oppure è disponibile solo all'interno di un'altra sorgente

E: Il pacchetto "firefox" non ha candidati da installare
root@clientbasso:/home/uds# apt install lightdm mate firefox-esr

```

2. S

3. apt install firefox-esr-l10n-it (lingua italiana)

```

Elaborazione dei trigger per initramfs-tools (0.133+deb10u1)...
update-initramfs: Generating /boot/initrd.img-4.19.0-6-amd64
Elaborazione dei trigger per dictionaries-common (1.28.1)...
Elaborazione dei trigger per libc-bin (2.28-10)...
Elaborazione dei trigger per systemd (241-7~deb10u1)...
Elaborazione dei trigger per udev (241-7~deb10u1)...
Elaborazione dei trigger per mime-support (3.62)...
Elaborazione dei trigger per menu (2.1.47+b1)...
Elaborazione dei trigger per ca-certificates (20190110)...
Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Elaborazione dei trigger per dbus (1.12.16-1)...
Elaborazione dei trigger per libgdk-pixbuf2.0-0:amd64 (2.38.1+dfsg-1)...
root@clientbasso:/home/uds# apt install firefox-esr-l10n-it
Lettura elenco dei pacchetti... Fatto
Generazione albero delle dipendenze
Lettura informazioni sullo stato... Fatto
I seguenti pacchetti aggiuntivi saranno inoltre installati:
  hunspell-it
Pacchetti suggeriti:
  hunspell libreoffice-writer
I seguenti pacchetti NUOVI saranno installati:
  firefox-esr-l10n-it hunspell-it
0 aggiornati, 2 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 971 kB di archivi.
Dopo quest'operazione, verranno occupati 2.339 kB di spazio su disco.
Continuare? [S/n] s
Scaricamento di:1 http://ftp.it.debian.org/debian buster/main amd64 hunspell-it all 1:6.2.0-1 [539 k
B]
Scaricamento di:2 http://security.debian.org/debian-security buster/updates/main amd64 firefox-esr-l
10n-it all 60.9.0esr-1~deb10u1 [432 kB]
Recuperati 971 kB in 0s (10,8 MB/s)
Selezionato il pacchetto firefox-esr-l10n-it non precedentemente selezionato.
(Lettura del database... 90%

```

6. ora i pacchetti non servono più

1. apt clean

7. Linux quando parte c'è il kernel che passa il comando ad un gestore di sistema (init) che lancia una serie di script, ora esiste systemd, basato su un eseguibile parallelo

8. E' possibile manovrare i singoli servizi da amministratori con:

1. in /etc/init.d/... ci sono vari file eseguibili con configuratori (console-setup) e anche processi grafici

2. /etc/init.d/lightdm status (gestito da systemd)

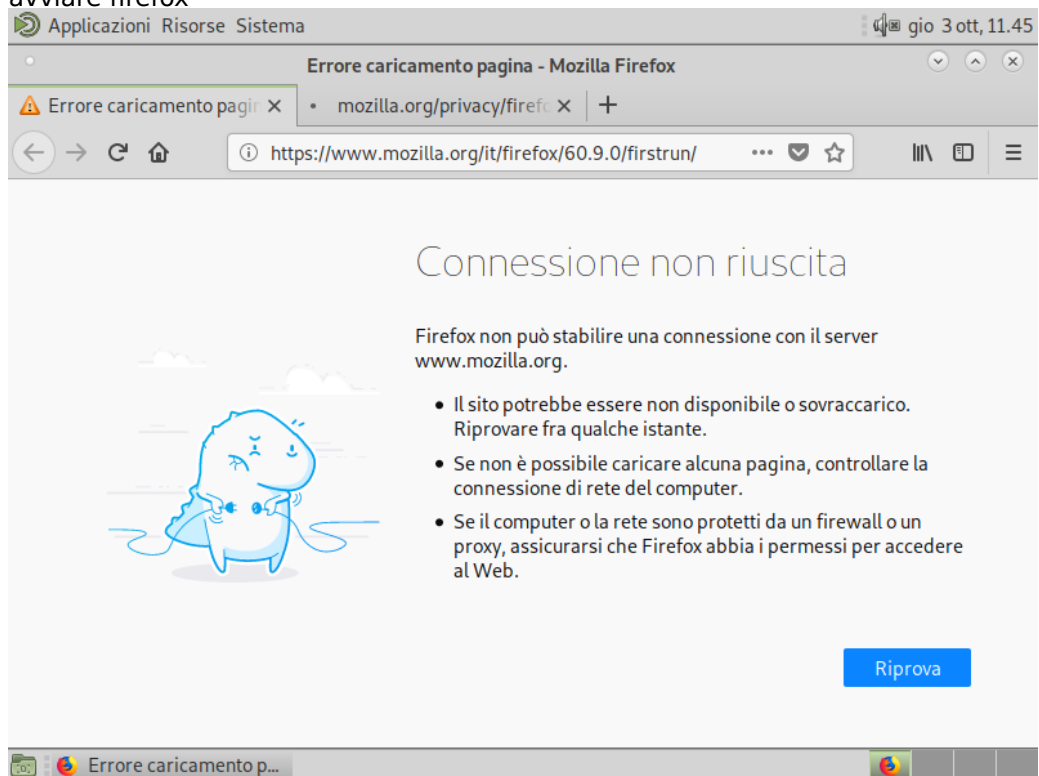
9. /etc/init.d/lightdm restart (avvia l'interfaccia grafica)

```

I seguenti pacchetti NUOVI saranno installati:
  firefox-esr-110n-it hunspell-it
0 aggiornati, 2 installati, 0 da rimuovere e 0 non aggiornati.
È necessario scaricare 971 kB di archivi.
Dopo quest'operazione, verranno occupati 2.939 kB di spazio su disco.
Continuare? [S/n] s
Scaricamento di:1 http://ftp.it.debian.org/debian buster/main amd64 hunspell-it all 1:6.2.0-1 [539 kB]
Scaricamento di:2 http://security.debian.org/debian-security buster/updates/main amd64 firefox-esr-110n-it all 60.9.0esr-1~deb10u1 [432 kB]
Recuperati 971 kB in 0s (10,8 MB/s)
Selezionato il pacchetto firefox-esr-110n-it non precedentemente selezionato.
(Lettura del database... 136929 file e directory attualmente installati.)
Preparativi per estrarre .../firefox-esr-110n-it_60.9.0esr-1~deb10u1_all.deb...
Estrazione di firefox-esr-110n-it (60.9.0esr-1~deb10u1)...
Selezionato il pacchetto hunspell-it non precedentemente selezionato.
Preparativi per estrarre .../hunspell-it_1%3a6.2.0-1_all.deb...
Estrazione di hunspell-it (1:6.2.0-1)...
Configurazione di firefox-esr-110n-it (60.9.0esr-1~deb10u1)...
Configurazione di hunspell-it (1:6.2.0-1)...
root@clientbasso:/home/uds# apt clean
root@clientbasso:/home/uds# /etc/init.d/
alsa-utils      dbus            lightdm         procps          x11-common
apparmor        hwclock.sh     networking     rsyslog
console-setup.sh keyboard-setup.sh plymouth        sudo
cron            kmod           plymouth-log   udev
root@clientbasso:/home/uds# /etc/init.d/
alsa-utils      dbus            lightdm         procps          x11-common
apparmor        hwclock.sh     networking     rsyslog
console-setup.sh keyboard-setup.sh plymouth        sudo
cron            kmod           plymouth-log   udev
root@clientbasso:/home/uds# /etc/init.d/lightdm status
• lightdm.service - Light Display Manager
   Loaded: loaded (/lib/systemd/system/lightdm.service; indirect; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:lightdm(1)
root@clientbasso:/home/uds#

```

1. accedere come uds
2. avviare firefox



3. andare sulle impostazioni di rete del client di Virtualbox
  1. Collegare Rete interna e mettere LAN
4. aprire terminale MATE
  1. ip addr
  2. sudo bash
  3. /etc/init.d/networking stop



```
uds@clientbasso: ~  
File Modifica Visualizza Cerca Terminale Aiuto  
valid_lft forever preferred_lft forever  
uds@clientbasso:~$ sudo bash  
[sudo] password di uds:  
root@clientbasso:/home/uds# /etc/init.d/networking restart  
[ ok ] Restarting networking (via systemctl): networking.service.  
root@clientbasso:/home/uds# /etc/init.d/networking stop  
[ ok ] Stopping networking (via systemctl): networking.service.  
root@clientbasso:/home/uds# /etc/init.d/networking start  
[ ok ] Starting networking (via systemctl): networking.service.  
root@clientbasso:/home/uds# ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group d  
efault qlen 1000  
    link/ether 08:00:27:bb:3a:d9 brd ff:ff:ff:ff:ff:ff  
root@clientbasso:/home/uds# dhclient enp0s3
```

Fare clic per iniziare a trascinare «uds@clientbasso: ~»

4. (PLEASE WAIT UNTIL OUR PROF RESOLVE THE PROBLEM...)
5. lanciare a mano la richiesta DHCP
  1. dhclient enp0s3
  2. viene assegnato 192.168.1.100 (ciascuno è dentro la propria rete LAN distac-  
cata da quella del laboratorio)

```
uds@clientbasso: ~  
File Modifica Visualizza Cerca Terminale Aiuto  
valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST> mtu 1500 qdisc pfifo_fast state DOWN group d  
efault qlen 1000  
    link/ether 08:00:27:bb:3a:d9 brd ff:ff:ff:ff:ff:ff  
root@clientbasso:/home/uds# dhclient enp0s3  
root@clientbasso:/home/uds# ip addr  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state  
UP group default qlen 1000  
    link/ether 08:00:27:bb:3a:d9 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.1.100/24 brd 192.168.1.255 scope global dynamic enp0s3  
        valid_lft 7196sec preferred_lft 7196sec  
    inet6 fe80::a00:27ff:febb:3ad9/64 scope link  
        valid_lft forever preferred_lft forever  
root@clientbasso:/home/uds#
```

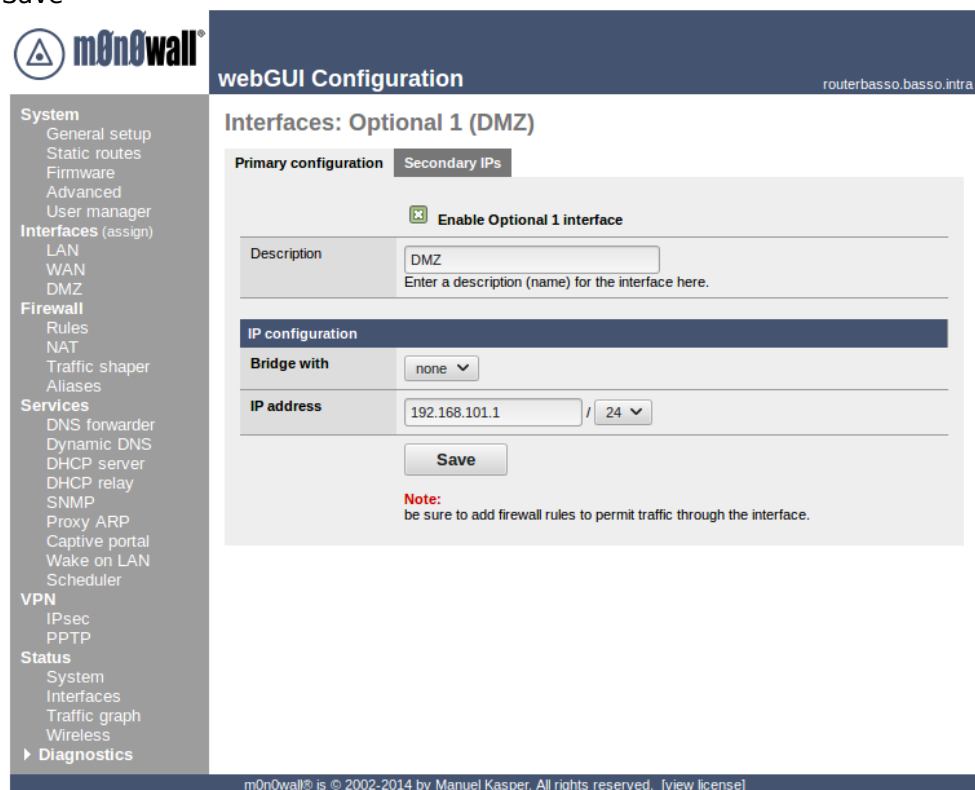
## Configurazione M0n0wall ↑

1. tornare su Firefox
  1. 192.168.1.1 sulla barra di ricerca per accedere alla pagina di gestione del router m0n0wall



1. admin
2. mono
3. possibilità di configurazione del router via web attraverso il client o i computer presenti in LAN
4. per questione di sicurezza è possibile modificare le impostazioni del router tramite una regola di controllo da parte del PC ospitante
  1. Firewall -> rules -> (e)
    1. disabilitare spunta Block.. (infondo)
  2. Firewall -> rules -> +
    1. Single host or alias
    2. Destination: WAN address
    3. inserire proprio IP
    4. porte from: 80 to: 80
    5. Description: Allow: ....
  3. Apply changes
5. Andare sul browser dell'host e scrivere l'indirizzo della WAN da Status -> Interfaces
  1. Impostare proxy su auto su firefox
  2. accedere con admin mono
  3. System -> general setup
    1. hostname: routercognome
    2. domain: cognome.intra
    3. lasciare spunta Allow DNS...
    4. user: admin
    5. password: lasolita
    6. time zone: Europe/Rome
    7. Save
    8. loggare con admin lasolita
  4. firmware: possibilità di aggiornare monowall via web
  5. System -> Advanced
    1. possibilità di attivare la modalità access point
  6. System -> User manager

1. permette di creare un gruppo di utenti con delle regole di accesso, per creare voucher e altro
7. Interfaces (assign)
  1. permette di ricalibrare le interfacce di rete, VLAN e WLAN
8. Interfaces -> LAN
  1. permette di modificare il range di indirizzi
9. Interfaces -> WAN
  1. DHCP -> hostname: routercognome
  2. Save
10. Interfaces -> OPT1
  1. Enable
  2. DMZ (è possibile mettere in bridge monowall, ma DMZ deve essere indipendente dalla LAN)
  3. IP address: 192.168.101.1 / 24
  4. Save



5. "Note: be sure to add firewall rules to permit traffic through the interface." (da configurare il firewall)
11. Firewall -> Rules -> LAN
  1. (valido solo per BSD e non per iptables) Le regole sono valutate in ordine discendente (da sopra a sotto)
  2. Default: permette tutto
12. Firewall -> Rules -> DMZ -> +

**System**

General setup  
Static routes  
Firmware  
Advanced  
User manager

**Interfaces (assign)**

LAN  
WAN  
DMZ

**Firewall**

Rules  
NAT  
Traffic shaper  
Aliases

**Services**

DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP  
Proxy ARP  
Captive portal  
Wake on LAN  
Scheduler

**VPN**

IPsec  
PPTP

**Status**

System  
Interfaces  
Traffic graph  
Wireless

**Diagnostics**
**Firewall: Rules: Edit**

<b>Action</b>	<input type="button" value="Block"/> <p>Choose what to do with packets that match the criteria specified below. Hint: the difference between block and reject is that with reject, a packet (TCP RST or ICMP port unreachable for UDP) is returned to the sender, whereas with block the packet is dropped silently. In either case, the original packet is discarded. Reject only works when the protocol is set to either TCP or UDP (but not "TCP/UDP") below.</p>
<b>Disabled</b>	<input type="checkbox"/> <b>Disable this rule</b> Set this option to disable this rule without removing it from the list.
<b>Interface</b>	<input type="button" value="DMZ"/> <p>Choose on which interface packets must come in to match this rule.</p>
<b>Protocol</b>	<input type="button" value="any"/> <p>Choose which IP protocol this rule should match. Hint: in most cases, you should specify <i>TCP</i> here.</p>
<b>ICMP type</b>	<input type="button" value="any"/> <p>If you selected ICMP for the protocol above, you may specify an ICMP type here.</p>
<b>Source</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <input type="button" value="DMZ subnet"/> Address: <input type="text"/> / <input type="button" value="v"/>
<b>Source port range</b>	from: <input type="button" value="(other)"/> <input type="text"/> to: <input type="button" value="(other)"/> <input type="text"/> <p>Specify the port or port range for the source of the packet for this rule. This is usually not equal to the destination port range (and is often "any"). Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
<b>Destination</b>	<input type="checkbox"/> <b>not</b> Use this option to invert the sense of the match. Type: <input type="button" value="LAN subnet"/> Address: <input type="text"/> / <input type="button" value="v"/>
<b>Destination port range</b>	from: <input type="button" value="(other)"/> <input type="text"/> to: <input type="button" value="(other)"/> <input type="text"/> <p>Specify the port or port range for the destination of the packet for this rule. Hint: you can leave the 'to' field empty if you only want to filter a single port</p>
<b>Fragments</b>	<input type="checkbox"/> <b>Allow fragmented packets</b> Hint: this option puts additional load on the firewall and may make it vulnerable to DoS attacks. In most cases, it is not needed. Try enabling it if you have troubles connecting to certain sites.
<b>Log</b>	<input type="checkbox"/> <b>Log packets that are handled by this rule</b> Hint: the firewall has limited local log space. Don't turn on logging for everything. If you want to do a lot of logging, consider using a remote syslog server (see the <a href="#">Diagnostics</a> ).

1. Action: block
  2. protocol: any
  3. Source: DMZ subnet
  4. Destination: LAN subnet
  5. Description: Block: DMZ to LAN
  6. Save
13. "+" sotto la (e)
1. Pass
  2. Destination: any
  3. Description: Allow: DMZ to any

LAN

WAN

DMZ

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> <span>✗</span>	*	DMZ net	*	LAN net	*	Block: DMZ to LAN
<input type="checkbox"/> <span>↑</span>	*	DMZ net	*	*	*	Allow: DMZ to any

↑ pass

↑ pass (disabled)

✗ block

✗ block (disabled)

✗ reject

✗ reject (disabled)

📄 log

📄 log (disabled)

←

⊖

+

←

⊖

+

←

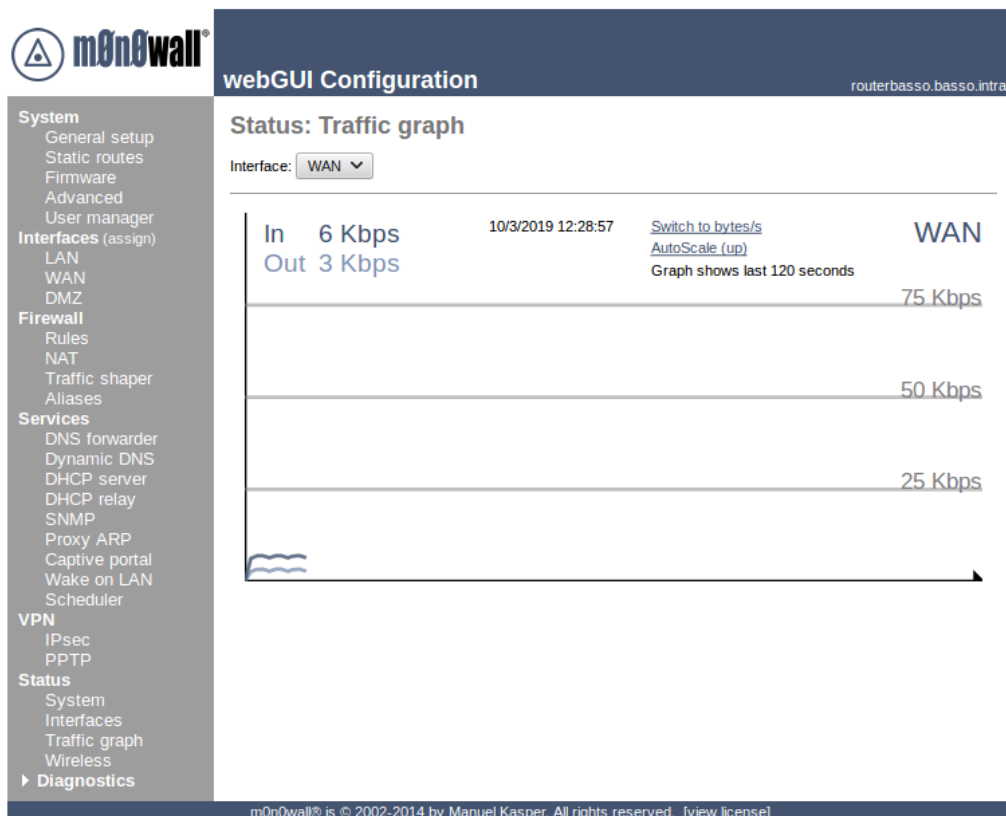
⊗

+

#### 14. Apply changes

- I computer DMZ possono andare su tutta internet? NO: se il DMZ viene “conquistato” bisogna bloccare le connessioni con un firewall che non cercano direttamente un proxy specificato o un DNS personale.

#### 15. Status -> traffic graph



#### 16. Diagnostics -> Logs

#### 17. Diagnostics -> DHCP leases ()

#### 18. Diagnostics -> ARP table (MAC registrati)

## System

General setup  
Static routes  
Firmware  
Advanced  
User manager

## Interfaces (assign)

LAN  
WAN  
DMZ

## Firewall

Rules  
NAT  
Traffic shaper  
Aliases

## Services

DNS forwarder  
Dynamic DNS  
DHCP server  
DHCP relay  
SNMP  
Proxy ARP  
Captive portal  
Wake on LAN  
Scheduler

## VPN

IPsec  
PPTP

## Status

System  
Interfaces  
Traffic graph  
Wireless

## Diagnostics

Logs  
DHCP Leases  
CPU Graph  
IPsec  
Ping/Traceroute  
ARP Table  
Firewall states  
Reset state  
Backup/Restore  
Factory Defaults  
Reboot system

## Diagnostics: ARP table

IP address	MAC address	Hostname	Interface
<input type="checkbox"/> 192.168.101.1	08:00:27:d3:6d:ce		DMZ
<input type="checkbox"/> 192.168.1.1	08:00:27:05:68:a3		LAN
<input type="checkbox"/> 192.168.1.100	08:00:27:bb:3a:d9	clientbasso	LAN
<input type="checkbox"/> 172.30.4.254	00:15:60:a6:bb:02		WAN
<input type="checkbox"/> 172.30.4.11	00:40:f4:79:86:17		WAN
<input type="checkbox"/> 172.30.4.104	08:00:27:55:d8:23		WAN

## Hint:

IP addresses are resolved to hostnames if "Resolve IP addresses to hostnames" is checked on the [Diagnostics: Logs](#) page.

19. Diagnostics -> Backup/Restore (XML)

1. Download configuration

20. Diagnostics -> Factory Defaults (pulisce l'intera configurazione)

## Configurare la rete ↑

### Impostare l'ip del client

1. Rilanciare il router
2. Svegliare il client
  1. apt install anacron (opzionale)
  2. dal browser
    1. 192.168.1.1
    2. admin lasolita
    3. Services -> DHCP Server -> DMZ -> [x] Enable
    4. Range: 192.168.101.100 al 192.168.101.199
    5. Save

## Services: DHCP server



The static mapping configuration has been changed.  
You must apply the changes in order for them to take effect.

Apply changes

LAN

DMZ

Enable IPv4 DHCP server on DMZ interface

Enable

Deny unknown clients

☐ Only respond to reserved clients listed below.

Subnet

192.168.101.0

Subnet mask

255.255.255.0

Available range

192.168.101.1 - 192.168.101.254

Range

192.168.101.100 to 192.168.101.199

WINS servers

Default lease time

seconds

This is used for clients that do not ask for a specific expiration time.  
The default is 7200 seconds.

Maximum lease time

seconds

This is the maximum lease time for clients that ask for a specific expiration time.  
The default is 86400 seconds.

Next server

Specify the server from which clients should load the boot file. This is usually only needed with PXE booting and some VoIP phones, and can usually be left empty.

Filename

Specify the name of the boot file on the server above. This is usually only needed with PXE booting and some VoIP phones, and can usually be left empty.

Save

### Note:

The DNS servers entered in [System: General setup](#) (or the [DNS forwarder](#), if enabled) will be assigned to clients by the DHCP server.

The DHCP lease table can be viewed on the [Diagnostics: DHCP leases](#) page.

### Reservations

MAC address	IP address	Description
08:00:27:b3:8c:84	192.168.101.250	IP statico del server



## Impostare DMZ nel router ↑

1. Configurare il server
  1. Rete -> Scheda 1 -> Rete interna DMZ
2. Avviare il server
  1. uds lasolita
  2. testare la rete con ping 1.1.1.1
3. FASE DI COLLAUDO:
  1. CONTROLLARE STACK ISO/OSI DAL LIVELLO 0
    1. scheda di rete fisica
    2. arp
    3. ping

- 4. servizi
- 5. dns e ip
- 6. software
- 2. essendoci delle regole di firewall bisogna collaudarlo (ordine delle righe sbagliate, DMZ, regole di blocco)
- 3. sul router Diagnostics -> DHCP leases
- 4. sul client pingare il server
  - 1. ping 192.168.101.100
- 5. testare se server pinga il client
  - 1. ping 192.168.1.100
- 6. test dei nomi di dominio nel client ([x] riuscita)
  - 1. ping www.e—fermi.it
- 7. test dei nomi di dominio nel server
  - 1. ping www.e—fermi.it
- 4. **/etc/resolv.conf**
  - 1. file ad attuazione immediata, serve per i programmi per trovare il DNS
  - 2. modifica manuale, ma il DHCP va a riscrivere tutto il file (usare solo in caso di disattivazione di DHCP)
  - 3. mostra dominio
  - 4. mostra quale server viene usato come dns (client .1.1, server .101.1), la regola di firewall vieta l'accesso alla DMZ verso la 192.168.1.x
- 3. installare sul client e sul server
  - 1. sudo apt install ssh (metapacchetto, crea solo dipendenze come openssh client e server e altro)(dropbear alternativa ad ssh)
- 4. verificare la possibilità di fare ssh da client a server e l'impossibilità di fare ssh dal server al client
  - 1. client
    - 1. ssh uds@192.168.101.100
    - 2. certificato SHA256: yes (usato per verificare l'autenticità del server)
  - 2. server
    - 1. ssh uds@192.168.1.100 (non deve funzionare)

## Applicare modifiche della rete ↑

- 1. Riavviare macchine virtuali
- 2. Il client deve identificare il server sempre con lo stesso indirizzo
  - 1. ip addr sul client: 192.168.1.100 e mostra il mac
  - 2. ip addr sul server: 192.168.101.100 e mostra il mac
- 3. sulla configurazione del router:
  - 1. Diagnostics -> ARP table
  - 2. Services -> DHCP Server -> DMZ -> Reservations
  - 3. Possibilità di assegnare lo stesso ip ad una macchina specifica tramite indirizzo MAC
    - 1. MAC del server
    - 2. 192.168.101.250 (fuori dal range DHCP poichè al server necessita un indirizzo ip statico anche per i successivi riavvii)
    - 3. Ip statico del server
    - 4. "Deny unknown clients" Only respond to reserved clients listed below. LASCIARE DISATTIVATA (il firewall si occupa degli indirizzi esterni, DMZ per il range di indirizzi locali, no MAC, no IP)



## Aggiungere regole in M0n0wall ↑

### 1. aliases:

#### 1. Firewall -> Rules

1. WAN ha solo il PC fisico
2. Possibilità di aggiungere più regole di firewall allo stesso indirizzo IP, senza andare a modificare tutte le regole di firewall riguardanti quell'IP

#### 3. Firewall -> Aliases

1. host-pcospitante
2. 172.30.4.x
3. Il computer da cui opero

### Firewall: Aliases: Edit alias

Name	<input type="text" value="host-pcospitante"/> <small>The name of the alias may only consist of the characters a-z, A-Z, 0-9 and '-' (dash).</small>
Type	<input type="button" value="Host"/> ▾
Address	<input type="text" value="172.30.4.11"/> / <input type="button" value="▾"/> <small>The address that this alias represents.</small>
Description	<input type="text" value="Il computer da cui opero"/> <small>You may enter a description here for your reference (not parsed).</small>

#### 4. tornare in Firewall -> Rules

#### 5. modificare la regola WAN

1. Source
2. Type: Single host or alias
3. host-pcospitante

#### 6. Tutti con regole uguali, ma con alias diversi. Questo permette di configurare diversamente i router ma con alias uguali. D'ora in poi le regole di firewall vanno fatte con alias standardizzati: WAN-descrizione LAN-descrizione HOST-descrizione-interfaccia

#### 7. creare un altro alias:

1. lan-labsistemi
2. Network
  1. 172.30.4.0/24 (a casa 192.168.1.1/24)
3. La rete in cui appoggia la mia WAN

### Firewall: Aliases: Edit alias

Name	<input type="text" value="lan-labsistemi"/> <small>The name of the alias may only consist of the characters a-z, A-Z, 0-9 and '-' (dash).</small>
Type	<input type="button" value="Network"/> ▾
Address	<input type="text" value="172.30.4.0"/> / <input type="button" value="24"/> ▾ <small>The address that this alias represents.</small>
Description	<input type="text" value="La rete in cui appoggia la mia WAN"/> <small>You may enter a description here for your reference (not parsed).</small>

## 2. Studiare la migrazione stagionale degli indirizzi completa del laboratorio senza console server e router, temporizzare i riavvii con cambi di opzioni di monowall, client avrà indirizzo corretto al rinnovo richiesta DHCP

1. socchiudere monowall
2. server via ssh, quindi exit e socchiudere il server

3. lasciare aperto solo il client
  4. usare ssh sul client e web
  5. attenzione: timing DHCP, ordine degli eventi, documentare tutto
  6. SNAPSHOT di tutte le macchine virtuali, salvare configurazione monowall nel client e in piattaforma (Istantanea 1, descrizione: pre-antartide)
  7. 192.168.x.0/24 LAN lab virtuale (192.168.11./24)
  8. 192.168.100+x.0/24 DMZ lab virtuale (192.168.111.0/24)
3. Impostare IP statico:
1. nano /etc/network/interfaces
  2. dhcp to static
  3. address 192.168.x.2/24
  4. gateway 192.168.x.1

```

uds@clientbasso: ~
File Modifica Visualizza Cerca Terminale Aiuto
GNU nano 3.2 /etc/network/interfaces

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
allow-hotplug enp0s3
iface enp0s3 inet static
address 192.168.11.2/24
gateway 192.168.11.1

[ Lette 14 righe ]
^G Guida      ^O Salva      ^W Cerca      ^K Taglia      ^J Giustifica
^X Esci       ^R Inserisci  ^\ Sostituisci ^U Incolla     ^T Ortografia

```

4. Pure nel server, ma con 192.168.100+x.2/24 e gateway .1
5. In monowall
  1. Interfaces
  2. Ip di gateway di LAN e DMZ
  3. Server DHCP
    1. LAN cambiare range in .x.100 e .x.199
    2. LAN cambiare range in .100+x.100 e .100+x.199

## Migrazione IP ↑

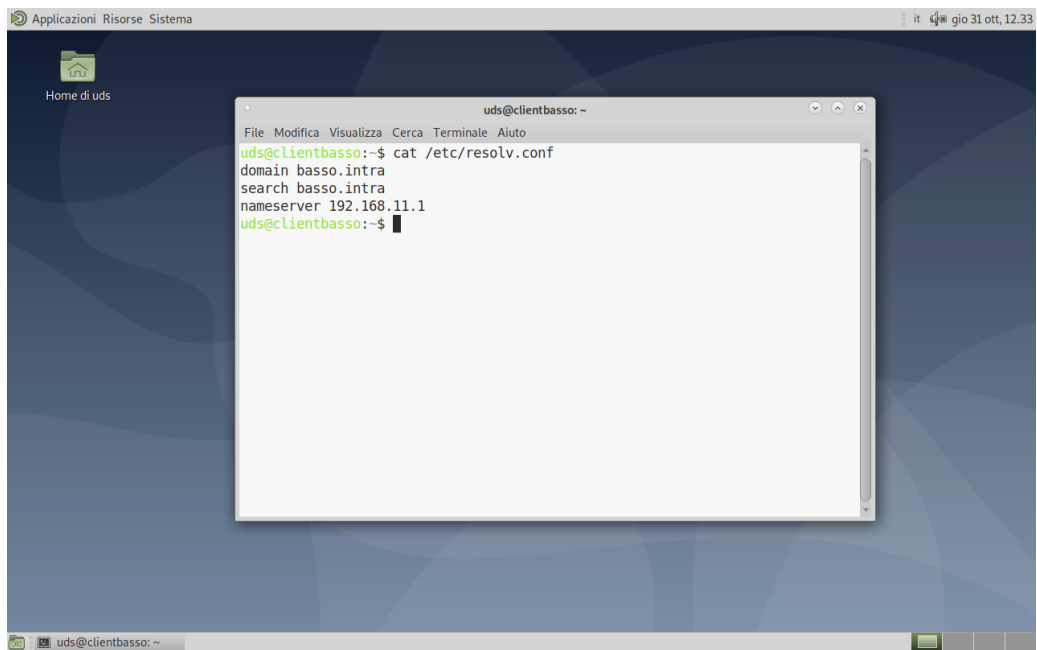
1. Nel SERVER da client in ssh
  1. ssh uds@192.168.101.250
  2. su —
  3. nano /etc/network/interfaces
    1. ... inet static
    2. address 192.168.100+x.250/24 gateway 192.168.100+x.1
    3. ifup enp0s3
2. In M0n0wall
  1. Interfaces -> DMZ

1. IP address = 192.168.111.1/24
2. Services -> DHCP Server -> DMZ
  1. Range 192.168.111.100 to 192.168.111.199
  2. Reservations da 192.168.101.250 a 192.168.111.250
3. Interfaces -> LAN (NON RIAVVIARE)
  1. IP 192.168.11.1/24
4. Services -> DHCP Server -> LAN
  1. Enable
  2. Range 192.168.11.100 to 192.168.11.199
5. Reboot system
3. Nel client
  1. ifup enp0s3
  2. testare il server
    1. ping 192.168.111.250
  3. testare la rete
    1. ping 1.1.1.1
  4. dal server pingare l'esterno
    1. ssh uds@192.168.111.250
    2. ping 1.1.1.1
- DHCP è debole:
  - boot da rete del lab: server fa anche da DHCP, si può osservare il server ufficiale, mandare un pacchetto UDP durante l'avvio che aggiunge le opzioni di avvio da rete del sistema operativo
  - nel caso di manutenzione di ip statici, questo stratagemma permette di ottenere sempre lo stesso indirizzo del DHCP

## Restrizioni aggiuntive sul firewall ↑

### Condizioni

- Sia il client che il server devono essere protetti da virus (cercano di inibire chi li sconfigge, anti-antivirus)
- Firewall esterno devono proteggere sia LAN che DMZ anche nel caso uno dei due o entrambi siano stati attaccati e vogliono diffondersi
- Da LAN a WAN: DNS riceve un nome e restituisce l'IP (elenco del telefono per la nonnina)
  - **IMPEDIRE IL CAMBIO DEL DNS**
  - chiamata telefono fisso tradizionale: il chiamante occupa il chiamato anche se il chiamato mette giù il telefono = truffa vecchio stile
  - Un client riceve il DNS dal router tramite la richiesta DHCP (dns livello applicazione, dhcp livello IP)
  - Client scrive il server DNS nel file /etc/resolve.conf, file continuamente riscritto dal router  
Nel client cat /etc/resolv.conf



- LAN deve permettere al servizio DNS di andare solo nel M0n0wall lato LAN, le altre richieste TCP/UDP per il DNS da tagliare
- Creare alias per host-server, host-router-lan, host-router-dmz

#### Firewall: Aliases: Edit alias

Name	host-router-lan	The name of the alias may only consist of the characters a-z, A-Z, 0-9 and '-' (dash).
Type	Host	
Address	192.168.11.1	The address that this alias represents.
Description	Router M0n0wall LAN	You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/>		

#### Firewall: Aliases: Edit alias

Name	host-router-DMZ	The name of the alias may only consist of the characters a-z, A-Z, 0-9 and '-' (dash).
Type	Host	
Address	192.168.111.1	The address that this alias represents.
Description	Router M0n0wall DMZ	You may enter a description here for your reference (not parsed).
<input type="button" value="Save"/>		

## Firewall: Aliases: Edit alias

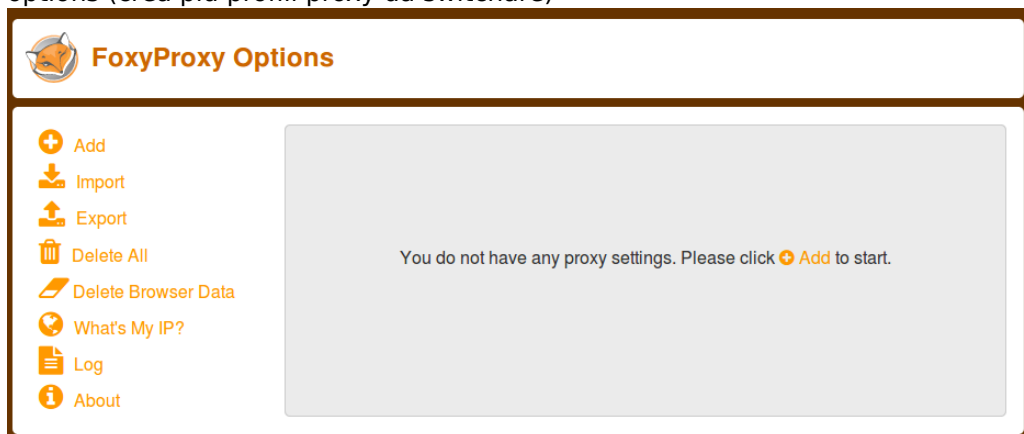
Name	<input type="text" value="host-server"/> <small>The name of the alias may only consist of the characters a-z, A-Z, 0-9 and '-' (dash).</small>
Type	<input type="button" value="Host"/>
Address	<input type="text" value="192.168.111.250"/> / <input type="button" value="v"/> <small>The address that this alias represents.</small>
Description	<input type="text" value="Server in DMZ"/> <small>You may enter a description here for your reference (not parsed).</small>

- LAN e WAN verso DMZ
  - DMZ esce solo con la porta 80 (ora solo porta 22 per SSH)
  - LAN può essere infettata
  - DMZ zona sicura dall'accesso sia da WAN che da LAN
  - DMZ deve dare accesso ad una lista di servizi, mentre il resto no (ora c'è Allow: DMZ to any)
  - permetti tutto dalla LAN alla DMZ disabilitata e da attivare in caso di manutenzione (descrizione: NORMALMENTE INATTIVA)
- DMZ verso LAN **PROIBITO**
- DMZ verso WAN
  - potrebbe ricevere attacchi anche da un ping fraudolento
  - Server ha bisogno di *rispondere* ad internet, non di *andare* verso internet
  - **VIETARE TRAFFICO IN BASE AL SERVIZIO**
    - minimo traffico ICMP
    - DNS verso il server giusto
    - NTP per l'orario (tempo in rete è importante, solo orologi fidati)
    - aggiornamenti, regola a scuola è differente da casa (apt-cache porta 3142 ip 172.30.1.199), a casa /etc/apt/sources ci sono gli indirizzi
    - /etc/apt/sources.list.d e il file pbiso.list aggiunge una fonte aggiuntiva oltre a sources, durante gli aggiornamenti controllerà anche questa repo
    - per windows esistono degli host per windows update
- Monowall -> Services -> Scheduler
  - Permette di limitare i servizi in certe fasce orarie
- Collaudare il DNS Testare la rete anche con DNS diversi


host www.casettamia.it 8.8.8.8

- Al posto di bloccare le chiamate DNS illecite, si può redirezionare con DNAT e rispondere con il server DNS ufficiale.
- NAT
  - indirizzi privati non possono andare su internet, poichè gli altri host non sanno come rispondere

- IP sorgente dell'host privato viene sostituito con quello del router privato -> esce con IP pubblico -> traffico torna verso il router -> router ritorna il traffico all'ip privato dell'host
- DNAT
  - altero la destinazione
  - nel router si chiama port-forwarding, virtual-server, server-port, port-mapping, ...
  - DMZ con indirizzo pubblico, oppure se ha un indirizzo privato = ho solo l'ip pubblico del router
  - m0n0wall -> Firewall -> NAT -> Inbound
    - Regola di controllo del server da rete esterna (per teleassistenza, con la possibilità di accesso da solo alcuni IP statici (o aziendali o da server redirect))
    - from: SSH
    - NAT IP: host-server (accetta alias, ma attenzione)
    - Description: Server in SSH
    - Auto-add a firewall rule to permit traffic through this NAT rule (crea una regola permissiva da poi adattare nel firewall, solo in fase di creazione)
  - m0n0wall -> Firewall -> Rules
    - si vede l'aggiunta della regola di NAT
    - da modificare che permette di accedere al server solo dal pc ospitante (edit -> host-pcospitante)
- Installare il plugin Foxyproxy Standard sia nel pc ospitante che nel client
  - options (crea più profili proxy da switchare)



- diretto
- #000000
- Type: Direct (no proxy)



## Add Proxy

Title or Description (optional)

Color

#66cc66

Pattern Shortcuts

Enabled On

Add whitelist pattern to match all URLs Off

Do not use for localhost and intranet/private IP addresses Off

Proxy Type

HTTP

Proxy IP address or DNS name ★


172.30.1.199

Port ★

3128

Username (optional)

username

Password (optional) 

\*\*\*\*\*

Cancel

Save & Add Another

Save & Edit Patterns

Save

- scuola
- #66cc66
- 172.30.1.199
- 3128
- diretto -> patterns
  - se l'ip ha una forma usa un certo proxy, altrimenti usa l'altro
  - New White
    - Pattern: 192.168.\*
  - permette di usare un proxy per gli ip locali, mentre
  - In firefox -> Preferenze -> nessun proxy

Impostazioni di connessione

### Configurazione dei proxy per l'accesso a Internet

☒ Nessun proxy

☐ Individua automaticamente le impostazioni proxy per questa rete

☐ Utilizza le impostazioni proxy del sistema

☐ Configurazione manuale dei proxy

Proxy HTTP

Porta

0

☐ Utilizza lo stesso proxy per tutti i protocolli

Proxy SSL

Porta

0

Proxy FTP

Porta

0

Host SOCKS

Porta

0

☐ SOCKS v4

☒ SOCKS v5

☐ Configurazione automatica dei proxy (URL)

Ricarica

Nessun proxy per

Esempio: .mozilla.org, .net.nz, 192.168.1.0/24

Le connessioni verso localhost, 127.0.0.1 e ::1 non usano mai proxy.

☐ Non richiedere l'autenticazione se la password è salvata

☐ DNS proxy per SOCKS v5

☐ Attiva DNS over HTTPS

Utilizza provider

Cloudflare (predefinito)

?

Annulla

OK

## Schema

da/a	LAN	WAN	DMZ
<b>LAN</b>	v	v(dns)	v*2
<b>WAN</b>	x	v	v*2(dnat)
<b>DMZ</b>	x	v(dns,ntp,http)	v

## Realizzazione

## Regole di NAT

If	Proto	Ext. Port range	NAT IP	Int. port range	Descrizione
WAN	TCP	22 (SSH)	host-server	22 (SSH)	Server in SSH

## Alias del firewall

Nome	Indirizzo	Descrizione
host-pcospitante	172.30.4.11	Il computer da cui opero



Nome	Indirizzo	Descrizione
host-router-dmz	192.168.111.1	Router M0n0wall DMZ
host-router-lan	192.168.11.1	Router M0n0wall LAN
host-server	192.168.111.250	Server in DMZ
lan-labsistemi	172.30.4.0/24	La rete in cui appoggia la mia WAN

### Regole firewall LAN

Attivo	Proto	Source	Port	Destination	Port	Descr
X	TCP/UDP	LAN net	*	! host-router-lan	52 (DNS)	Block: LAN to LAN attack - DNS

### Regole firewall WAN

Attivo	Proto	Source	Port	Destination	Port	Descr
V	TCP	host- pcospitante	*	WAN address	80 (HTTP)	Allow: accesso web al m0n0wall dal PC ospitante

### Regole firewall DMZ

Attivo	Proto	Source	Port	Destination	Port	Descr
X	*	DMZ net	*	LAN net	*	Block: DMZ to LAN any

## Servizi per il server ↑

### Apache

- Indiscusso re del mercato del middleware, ora sono arrivati lighthttpd, nginx
- Servono a gestire i grandi flussi di dati e utenti con migliaia di richieste al secondo
- I contenuti dinamici forniti da vari server, mentre le parti statiche da altri server con tecnologie diverse (grande uso di cache)


### Configurare la rete e le porte ↑

Sito web consultabile dall'esterno tramite l'IP del router, ora c'è M0n0wall in porta 80 **deve rimanere tale per la LAN.**




Dall'esterno deve essere possibile vedere la pagina del server, senza togliere la gestione del M0n0wall dall'esterno tramite porta 8080.

da/a	apache	M0n0wall
LAN	80	80
WAN	80 restrict	8080 restrict

## Firewall: NAT: Inbound

 The changes have been applied successfully.


**Inbound** **Server NAT** **1:1** **Outbound**








	If	Proto	Ext. port range	NAT IP	Int. port range	Description	
<input type="checkbox"/>	WAN	TCP	22 (SSH)	host-server	22 (SSH)	Server in SSH	  

**Note:**  
It is not possible to access NATed services using the WAN IP address from within LAN (or an optional network).

Figure 4: Screenshot


## Firewall: Aliases

 The changes have been applied successfully.


	Name	Address	Description	
<input type="checkbox"/>	host-pcospitante	172.30.4.11	Il computer da cui opero	
<input type="checkbox"/>	host-router-DMZ	192.168.111.1	Router M0n0wall DMZ	
<input type="checkbox"/>	host-router-lan	192.168.11.1	Router M0n0wall LAN	
<input type="checkbox"/>	host-server	192.168.111.250	Server in DMZ	
<input type="checkbox"/>	lan-labsistemi	172.30.4.0/24	La rete in cui appoggia la mia WAN	  

**Note:**  
Aliases act as placeholders for real IP addresses and can be used to minimize the number of changes that have to be made if a host or network address changes. You can enter the name of an alias instead of an IP address in all address fields that have a blue background. The alias will be resolved to its current address according to the list below. If an alias cannot be resolved (e.g. because you deleted it), the corresponding element (e.g. filter/NAT/shaper rule) will be considered invalid and skipped.

Figure 5: Screenshot

 The changes have been applied successfully.

**LAN** **WAN** **OPT1**

	Proto	Source	Port	Destination	Port	Description
<input type="checkbox"/> 	TCP	172.30.4.11	*	WAN address	80 (HTTP)	Allow: accesso web al m0n0wall dal PC ospitante









 pass  block  reject  log  
 pass (disabled)  block (disabled)  reject (disabled)  log (disabled)

Figure 6: Screenshot

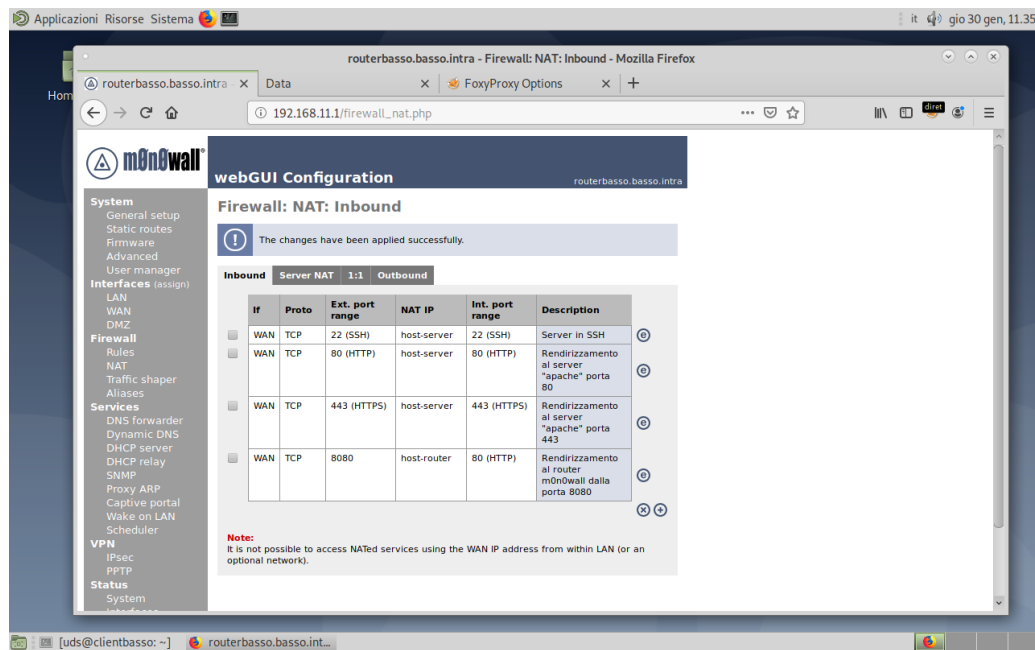


Figure 7: Screenshot

## Installazione apache ↑

```
sudo apt install apache2
```

Modificare la pagina index

```
sudo nano /var/www/html/index.html
```

## Configurazione apache con HTTPS ↑

Creare il certificato

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/ssl/private/apache-selfsig
```

- IT
- Italy
- Bassano del Grappa
- ITIS Enrico Fermi
- 5AI
- lab4-pc11.fermi.intra (hostname -f nel pc ospitante)
- email

Abilitare ssl su apache2

```

sudo cp /etc/apache2/sites-available/default-ssl.conf /etc/apache2/sites-available/default-ssl.conf
sudo nano /etc/apache2/sites-available/default-ssl.conf
# modificare ServerAdmin e ServerName con l'ip del server
# SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
# SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key
#
# decommentare le ultime righe:
#BrowserMatch "MSIE [2-6]" \
#
#                                nokeepalive ssl-unclean-shutdown \
#                                downgrade-1.0 force-response-1.0

```

Abilitare il redirect dell HTTPS

```

sudo nano /etc/apache2/sites-available/000-default.conf
# <VirtualHost *:80>
#   Redirect "/" "https://your_domain_or_IP/"
# </VirtualHost>

```

```

sudo a2enmod ssl
sudo a2enmod headers
sudo a2ensite default-ssl
sudo apache2ctl configtest

```

## Sostituzione FoxyProxy con SmartProxy ↑

- Estensione da installare: [addon smartproxy](#)
- Abilitare uso estensione
- Analizzatore DOM Inspector che fornisce contenuti di una pagina tramite vari proxy
- `ssh -D` Dynamic application-level port forwarding per simulare delle connessioni da remoto

## Link utili

[how-to-install-the-apache-web-server-on-ubuntu-16-04](#)

[how-to-create-a-self-signed-ssl-certificate-for-apache-in-ubuntu-16-04](#)

---

## VPN ↑

- Non installare software aggiuntivi per non farli accorgere dell'esistenza di VPN

VPN su m0n0wall crea una interfaccia di rete in più. Obiettivo: ping client1 verso client2

[m0n0wall handbook](#)

## PPTP ↑

Client deve avere il software per essere nella VPN.

Usato spesso negli ambienti aziendali.

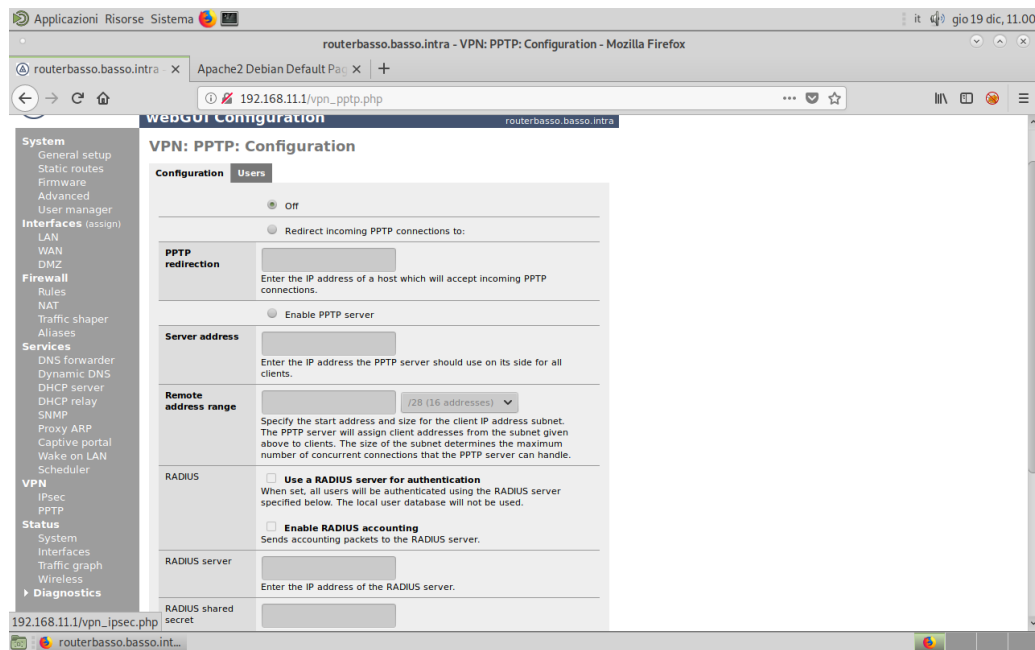
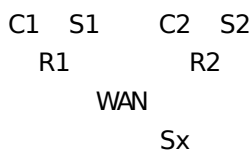


Figure 8: Screenshot

## IPsec ↑

Vecchio protocollo, nato prima del NAT.



1. C1 parla con C2
2. C1 deve andare a Sx
3. Il router parla in chiaro con Sx
4. Il router R1 conosce la rete R2
5. Il router sostituisce il livello 3 con IPsec
6. IPsec porta il resto del traffico ai livelli superiori ma cripta tutto dal livello 4 in su.
7. R2 riceve il pacchetto IPsec, e si conoscono entrambi i router
8. R2 decripta il pacchetto IPsec, non facendo accorgere ai client connessi della VPN

Da IPsec tradizionale a IPsec di tipo tunnel: Il pacchetto che nasce da C2 e arriva a C1, crea un livello 3 ISO/OSI in più:

- 1
- 2
- 3
  - 3 IPsec IP dei router
  - 3 livello IP criptato con IP privati di C1 e C2
- 4 pacchetto criptato
- ...

## Configurazione VPN in monowall ↑

1. VPN->IPsec->+

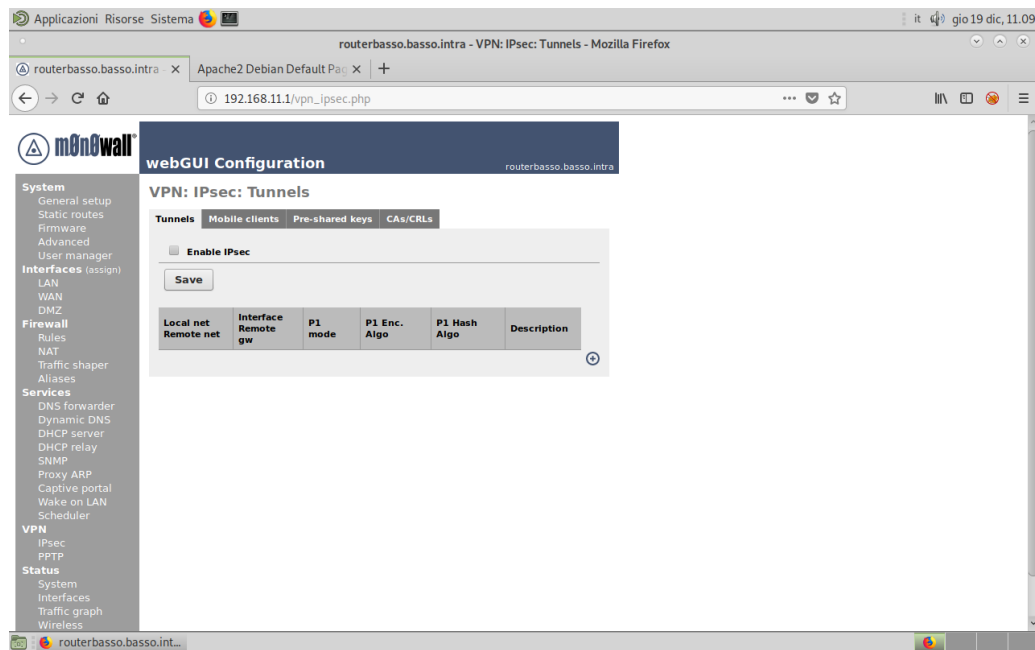


Figure 9: Screenshot

1. DPD Interval = 60 seconds
  2. Local subnet = LAN subnet
  3. Remote subnet = 192.168.12.1 (lan remota)
  4. Remote gateway = 172.30.4.95
  5. Description = Connessione VPN lab4-pc12 (NomeStudente)
  6. My identifier = My IP Address = 172.30.4.104
  7. Lifetime = 28800 seconds (standard CISCO)
  8. Pre-Shared Key = password scelta
  9. Lifetime = 28800 seconds
2. Enable IPsec

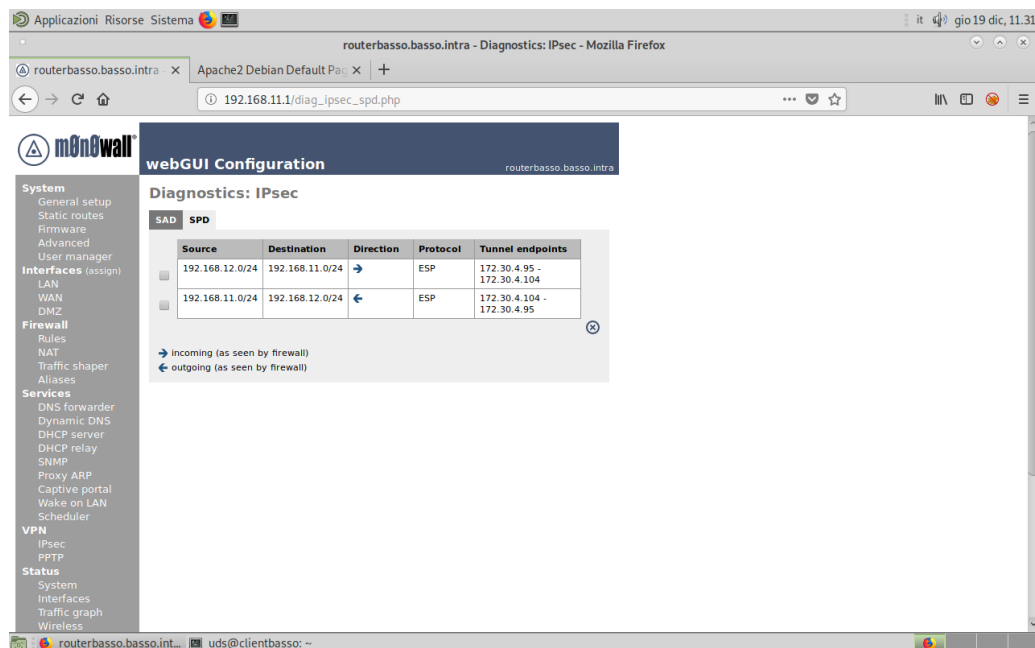


Figure 10: Screenshot

## Client e server ↑

- C1 può pingare S1?
- S1 può pingare S2?

## Sostituire IPsec con OpenVPN ↑

- IPsec lavora a livello di kernel (non sicuro)
- OpenVPN funziona in Userspace, e il kernel permette a questo programma di gestire la rete
- IPsec ha la modalità diretta e tunnelling con NAT (duplica il livello 3 IPsec e IP privati, router ofusca da livello IP in su, aggiunge livello IPsec e l'altro router lo estrae e ritorna in locale)
- OpenVPN lavora nei livelli 5, 6, 7.
- **Il traffico OpenVPN lavora in UDP porta 1194**

## Software OpenVPN ↑

- Riesce a portare pacchetti IP completi da 1 a 5 e in più poi da 3 a 7
- Ha varie funzionalità:
  - portare pacchetti IP
  - simulare trame Ethernet
- Kernel mette a disposizione delle interfacce **tun** e **tap**, dove il traffico passa per entrare nella rete locale.
  - tun: trame punto punto, traffico fuori standard attuale
  - tap: trame ethernet, traffico classico
  - 1 interfaccia fisica *eth0*
  - 1 interfaccia virtuale *tun0*

## Configurazione router ↑

- il router riceve traffico in porta 1194 UDP
- usare DNAT (port forwarding, virtual server)
- manda pacchetto a host con OpenVPN installato

## OpenVPN e la cifratura ↑

- Metodo semplice e coccoloso(fare questa)
  - connessioni di 2 host
  - usa una chiave simmetrica (da scambiare con qualche trippy)
  - [www.openvpn.net](http://www.openvpn.net)
  - `usr/share/doc/openvpn`
- Quello non semplice
  - connessioni multipunto (VPN di raccolta)
    - servizi aziendali locali usufruibili dall'esterno
  - uso di certificati [how-to-set-up-an-openvpn-server-on-ubuntu-18-04](#)

## Connessione punto punto

- comunicazione server <-> server
- l'interfaccia deve avere un suo indirizzo IP
- 192.168.200+x.1

- usare DNAT
- dentro il file di config mettere l'opzione log.append nomefile (direttiva nel file di configurazione di openVPN)

tail -f nomelog

## Creazione VPN con OpenVPN ↑

- **SERVER: 192.168.112.250**
- **CLIENT: 192.168.111.250**

### OpenVPN

[install-configure-openvpn-server-on-debian-9-linux](#)

[openvpn.net/community-resources/static-key-mini-howto](#)

1. scaricare openvpn

```
sudo apt update && sudo apt upgrade
sudo apt install openvpn
```

1. generare una chiave condivisa simmetrica nel server

```
#si trova in /etc/openvpn
openvpn --genkey --secret tun_lab.key
```

1. configurare tun0 nel server

```
nano -T 4 /etc/openvpn/tun_lab.conf
#dev tun10 ;livello applicativo
#port 1194
#proto udp #livello 4
#ifconfig 192.68.211.1 192.168.212.1 ;proprio - esterno ;livello 3
#remote 172.30.4.104
#secret /etc/openvpn/tun_lab.key
#log-append /var/log/openvpn-tun_lab.log
#comp-lzo ;comprime il traffico per ottimizzare il flusso dati
#cipher ;di default usa Blowfish, non affidabile
#keepalive 10 120 ;effettua un ping ogni 10 secondi
#route 192.168.11.0 255.255.255.0
#route 192.168.111.0 255.255.255.0
```

Si può mettere in ascolto il server su una precisa interfaccia con #listen IP1

1. copiare la chiave nel client con sftp tramite IPsec

```
sftp uds@TODO
#copiarla in /etc/openvpn sul client
```



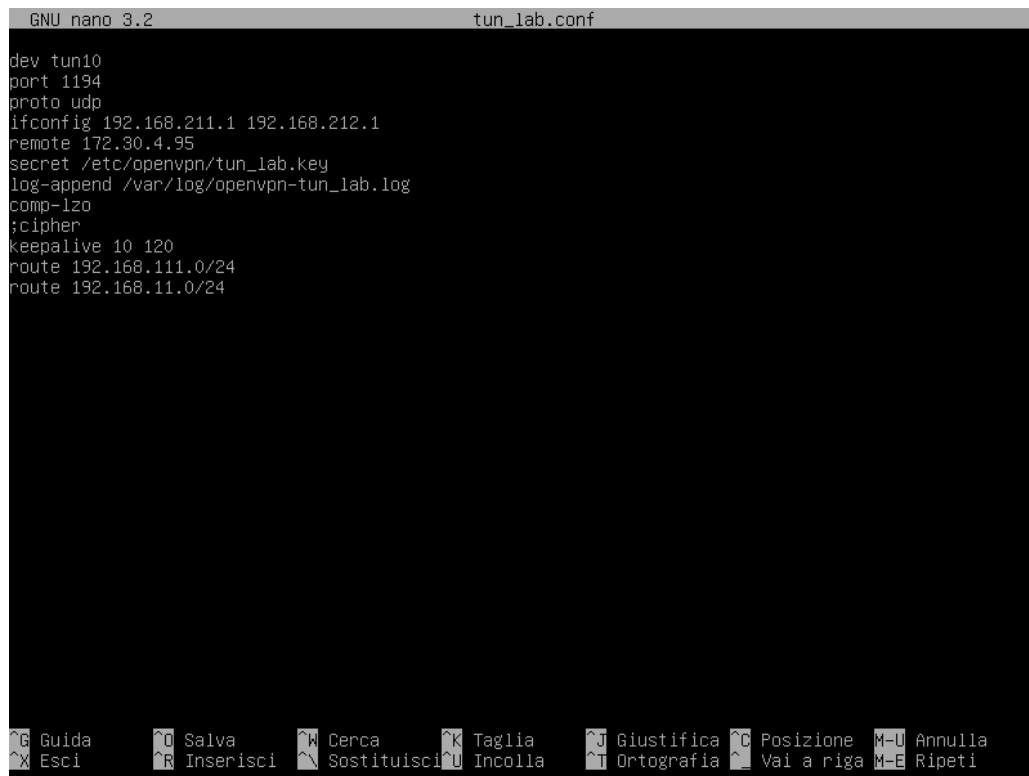
A screenshot of a terminal window showing the configuration of a file named `tun_lab.conf` using the `GNU nano 3.2` editor. The configuration lines are: `dev tun10`, `port 1194`, `proto udp`, `ifconfig 192.168.211.1 192.168.212.1`, `remote 172.30.4.95`, `secret /etc/openvpn/tun_lab.key`, `log-append /var/log/openvpn-tun_lab.log`, `comp-lzo`, `;cipher`, `keepalive 10 120`, `route 192.168.111.0/24`, and `route 192.168.11.0/24`. The bottom of the window shows a standard nano editor status bar with various keyboard shortcuts like `Guida`, `Salva`, `Cerca`, `Taglia`, `Giustifica`, `Posizione`, `Annulla`, `Esci`, `Inserisci`, `Sostituisci`, `Incolla`, `Ortografia`, `Vai a riga`, and `Ripeti`.

Figure 11: Screenshot

## 1. configurare tun0 nel client

```
nano -T 4 /etc/openvpn/tun_lab.conf
#remote 192.168.112.250
#dev tun10
#port 1194
#proto udp
#ifconfig 192.168.212.1 192.168.211.1 ;esterno — proprio
#remote 172.30.4.95 ;IPWAN del server livello 3
#secret /etc/openvpn/tun_lab.key
#log-append /var/log/openvpn-tun_lab.log
#comp-lzo ;comprime il traffico per ottimizzare il flusso dati
#cipher ;di default usa Blowfish, non affidabile
#keepalive 10 120 ;effettua un ping ogni 10 secondi
#route 192.168.12.0 255.255.255.0
#route 192.168.112.0 255.255.255.0
```

### 1. meccanismo di rotazione dei log

1. informa il processo con `kill -segno` di comunicazione che il file è occupato e deve usarne un altro
2. comprime il file e lo chiama `.1`
3. crea un nuovo file
4. giorno successivo muove log compresso `.1` in `.2`
5. a tot giorni

### 2. aprire le porte nel router *che così passa aria*

1. DNAT (Outbound NAT)
2. può funzionare anche senza regole di NAT, dove il traffico esce

- 1.
3. Firewall->WAN
  1. TCP/UDP
  2. from: any :1194
  3. to: 192.168.211.1/24 :1194
  4. Allow: WAN to OpenVPN
4. altra guida: [m0n0wall-port-forwarding-nat-help](#)
3. avviare openvpn da entrambe le parti con

openvpn —config /etc/openvpn/tun0.conf —verb 6 // verbose output

1. testare la VPN

1. sul server

```
ping 192.168.111.250
ping 192.168.211.250
```

1. sul client

```
ping 192.168.112.250
ping 192.168.212.250
```

1. il router fa un timeout per le connessioni VPN dalla parte del server che risponde al client tramite il NAT

2. Avviare openvpn

```
/etc/init.d/openvpn start
sysctl enable openvpn openvpn@serverconfig #crea un symlink
ip addr
```

3. Test dell'interfaccia

```
sudo apt install mtr
mtr -t
ip route #mostra che 200+x è raggiungibile da 200+y
ip addr
#ip route add 192.68.100+x.0/24 via 192.168.200+x.1 #test
#aggiunge/modifica nella tabella di routing locale ogni volta che la vpn viene attivata
```

4. Aggiungere le seguenti direttive al config di openVPN:

- route 100+x.0/24
- route x.0/24

5. per permettere di fare:

1. ping .100+y.250
2. verso .100+x.250

3. risponde a .200+y.1
6. Aggiungere rotte statiche a monowall per permettere alla LAN di raggiungere l'altra LAN
  1. raggiungere C2 da S1 aggiungere .206.1 e usa .105.250
  2. raggiungere C2 da C1 da .106.0 verso S1 .105.250
  3. aggiungere le rotte configurate nella VPN
7. Nei computer con Linux non fanno da router, per abilitarlo:



Figure 12: Screenshot

```
cd /proc/sys/net/ipv4
cat ip_forward
sudo echo 1 > ip_forward
```

Oppure a mano ogni volta:

```
cat /etc/sysctl.conf
#decommentare la riga net.ipv4.ip_forward = 1
```

Oppure usare systemctl:

```
net.ipv4.ip_forward = 1;

uds@serverbasso:/etc/sysctl.d$ ls
99-sysctl.conf  forwarding.conf  protect-links.conf  README.sysctl
uds@serverbasso:/etc/sysctl.d$ _
```

```
sudo nano /etc/sysctl.d/forwarding.conf
#Nome, abilito il forwarding (data)
net.ipv4.ip_forward=1
```

```
sysctl --system
cat /proc/sys/net/ipv4/ip_forward
mtr 192.168.1.z
mtr 192.168.x.z
```

## Schema della VPN [↑](#)

```
C1 .x.100
S1 .100+x.250
   .200+x.1
```

```
R1 .x.1
   .100+x.1
   172.30.4.x
```

LAN LAB ...

```
R2 .y.1
   .100+y.1
   172.30.4.y
```

C2 .y.100  
S2 .100+y.250  
.200+y.1

## Rete VPN tra LAN

1. OpenVPN attiva Server1 <-> Server2
  2. Direttive route in OpenVPN (altre reti locali)
  3. Abilitare routing del server (sysctl)
  4. Rotte statiche nei m0n0wall
  5. Verifica della VPN
- 

## SNMP ↑

Fornisce e ottiene informazioni dai dispositivi di rete che altrimenti no

Nella scuola è presente il software Cacti nel server *squattero*, che mostra dei grafici e statistiche di utilizzo della macchina.

Avere delle statistiche serve ai tecnici per rilevare delle anomalie, ma anche ai clienti una parvenza di controllo (anche reale se possibile).

Se viene installato in un server, si può centralizzare l'intero controllo dello stato della rete

## Installare sul server MRTG ↑

- MRTG è stato inventato da Tobi e si chiama Multi Router Traffic Grapher
- `sudo apt install mrtg`
  - vengono installati altri pacchetti accessori che contengono configurazioni aggiuntive
  - gira ogni 5 minuti e aggiorna i file database con i grafici
  - la pagina riassuntiva `/var/www/html/mrtg`
  - `/usr/share/mrtg` contiene info sulle configurazioni
  - Rendere `/etc/mrtg.cfg` sotto root? Sì
- `/etc/cron.d/mrtg` è un cron che aggiorna i grafici
- snmp esplora un albero delle interfacce con un sottoalbero per ogni interfaccia con ogni dato inviato/spedito
  - Usa gli OID con degli standard rispettato da tutte le apparecchiature che supportano l'SNMP
  - configurando il server `snmpd` fornisce solo alcuni sottoalberi
  - In caso di dati non standard si usano OID non ufficiali oppure richiedendo alla IANA per lo standard

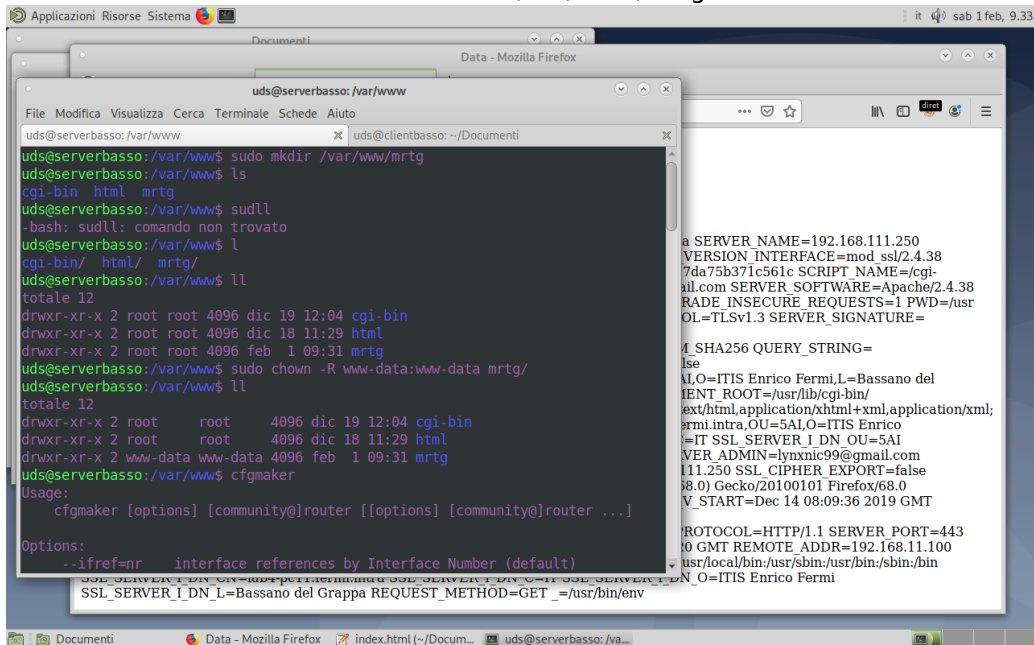
## Abilitare SNMP in M0n0wall

1. Services -> SNMP
  1. System location: `itis_lab_fermi`
  2. System contact: informazioni del cliente o dell'assistenza, basta che sia coerente in tutti i dispositivi
2. Aggiungere regola nel firewall per l'interrogazione del servizio SNMP (statistiche in UDP porta 161)

1. UDP | DMZ net | \* | host-router-dmz | 161 | Allow: DMZ to router - SNMP

## Configurare MRTG ↑

1. `sudo apt-get install mrtg -y`
2. `sudo mkdir /var/www/mrtg`
3. `sudo chown -R www-data:www-data /var/www/mrtg`

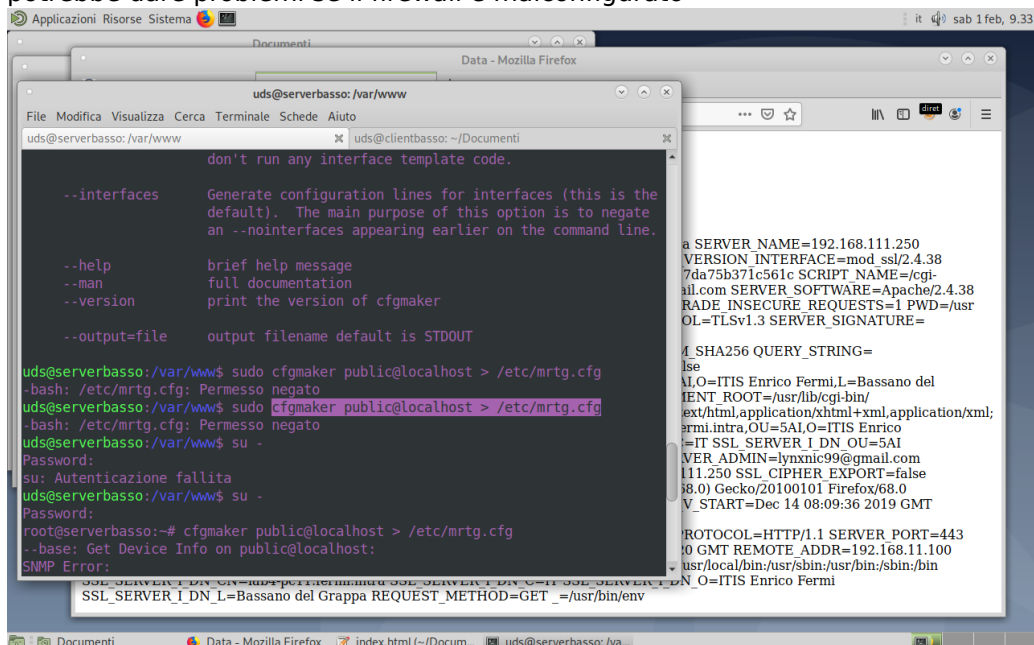


```
uds@serverbasso: /var/www$ sudo apt-get install mrtg -y
uds@serverbasso: /var/www$ sudo mkdir /var/www/mrtg
uds@serverbasso: /var/www$ ls
cgi-bin  html  mrtg
uds@serverbasso: /var/www$ sudo ll
-bash: sudo: comando non trovato
uds@serverbasso: /var/www$ ll
cgi-bin/  html/  mrtg/
uds@serverbasso: /var/www$ ll
totale 12
drwxr-xr-x 2 root root 4096 dic 19 12:04 cgi-bin
drwxr-xr-x 2 root root 4096 dic 18 11:29 html
drwxr-xr-x 2 root root 4096 feb 1 09:31 mrtg
uds@serverbasso: /var/www$ sudo chown -R www-data:www-data mrtg/
uds@serverbasso: /var/www$ ll
totale 12
drwxr-xr-x 2 root root 4096 dic 19 12:04 cgi-bin
drwxr-xr-x 2 root root 4096 dic 18 11:29 html
drwxr-xr-x 2 www-data www-data 4096 feb 1 09:31 mrtg
uds@serverbasso: /var/www$ cat /etc/mrtg.cfg
Usage:
  cfgmaker [options] [community@]router [[options] [community@]router ...]

Options:
  --ifref=nr      interface references by Interface Number (default)
  --server=dn     SSL_SERVER_DN_L=Bassano del Grappa REQUEST_METHOD=GET _=/usr/bin/env
```

4. `sudo cfgmaker public@192.168.111.1 > /etc/mrtg.cfg`

1. potrebbe dare problemi se il firewall è malconfigurato



```
uds@serverbasso: /var/www$ sudo cfgmaker public@192.168.111.1 > /etc/mrtg.cfg
-bash: /etc/mrtg.cfg: Permessi negati
uds@serverbasso: /var/www$ sudo cfgmaker public@192.168.111.1 > /etc/mrtg.cfg
-bash: /etc/mrtg.cfg: Permessi negati
uds@serverbasso: /var/www$ su -
Password:
su: Autenticazione fallita
uds@serverbasso: /var/www$ su -
Password:
root@serverbasso:~# cfgmaker public@192.168.111.1 > /etc/mrtg.cfg
--base: Get Device Info on public@192.168.111.1:
SNMP Error:
SSL_SERVER_DN_L=Bassano del Grappa REQUEST_METHOD=GET _=/usr/bin/env
```

5. `sudo indexmaker /etc/mrtg.cfg > /var/www/mrtg/index.html`

6. `sudo nano /etc/apache2/sites-available/mrtg.conf`

<VirtualHost \*:80>

ServerAdmin admin@yourdomain.com

```

DocumentRoot "/var/www/mrtg"
ServerName yourdomain.com
<Directory "/var/www/mrtg/">
Options None
AllowOverride None
Order allow,deny
Allow from all
Require all granted
</Directory>
TransferLog /var/log/apache2/mrtg_access.log
ErrorLog /var/log/apache2/mrtg_error.log
</VirtualHost>

```

7. sudo a2ensite mrtg
8. sudo systemctl restart apache2
9. cd /var/www/html
  1. ln -s ../mrtg .

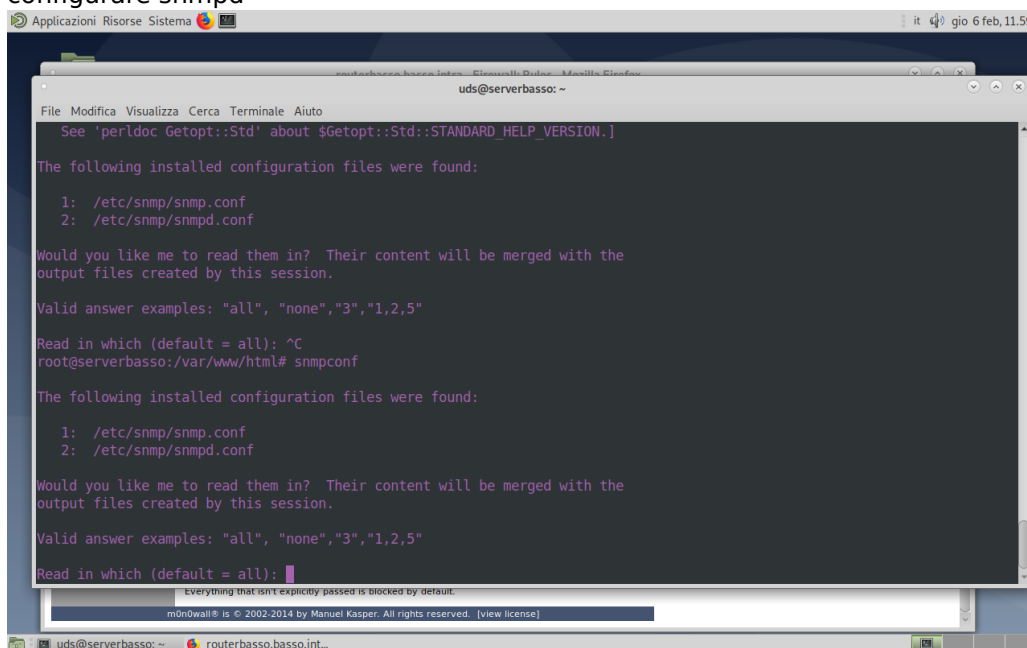
Pagina visitabile assiduamente all'indirizzo [172.30.4.97/mrtg](http://172.30.4.97/mrtg)

## Configurare SNMPD nel server ↑

1. Creare un altro file con cfgmaker e aggiungere nel file di monowall tutto quello che è stato generato a riguardo del server
  1. installare snmpd

```
sudo apt install snmpd
```

2. configurare snmpd



1. usare snmpconf
2. all (snmp e snmpd)
3. 2 (snmpd.conf)
4. 1 (various)
5. 2 (disk usage)

6. / (mount point)
7. 100000 (minimum amount)
8. finished
9. finished
10. quit
3. sudo nano /etc/snmp/snmpd.conf
  1. rimuovere/commentare in una nuova riga: **-V systemonly** dalla riga *rocommunity public default*
  2. decommentare rocommunity local
4. sudo systemctl restart snmpd
5. sudo cfgmaker public@localhost > /etc/mrtg\_server.cfg
6. copiare il contenuto del file mrt\_server.cfg dentro mrtg.cfg
7. sudo indexmaker /etc/mrtg.cfg > /var/www/mrtg/index.html

## Cacti ↑

### Installare le dipendenze di cacti

1. installare il server
  1. installare mariadb e php

su —

apt update && sudo apt upgrade

apt install -y apache2 mariadb-server mariadb-client php-mysql libapache2-mod-php

apt install -y php-xml php-ldap php-mbstring php-gd php-gmp

apt install -y snmp php-snmp rrdtool librrds-perl

[how-to-install-cacti-on-ubuntu-18-04-lts-bionic-beaver](#)

2. configurare mysql 1.configurare il database

sudo nano /etc/mysql/mariadb.conf.d/50-server.cnf

1. Inserire il seguente contenuto dopo mysqld tra quadre

```
max_heap_table_size = 128M
tmp_table_size = 64M
join_buffer_size = 64M
innodb_file_format = Barracuda
innodb_large_prefix = 1
innodb_buffer_pool_size = 512M
innodb_flush_log_at_timeout = 3
innodb_read_io_threads = 32
innodb_write_io_threads = 16
innodb_io_capacity = 5000
innodb_io_capacity_max = 10000
```



### 3. configurare php

```
sudo nano /etc/php/7.3/apache2/php.ini  
sudo nano /etc/php/7.3/cli/php.ini
```

```
date.timezone = EU/Rome  
memory_limit = 512M  
max_execution_time = 60
```

### 4. riavvia il server sql

```
sudo systemctl restart mariadb
```

### 5. configurare il database

```
sudo mysql -u root -p
```

```
create database cacti;  
GRANT ALL ON cacti.* TO cactiuser@localhost IDENTIFIED BY 'cactipassword';  
flush privileges;  
exit
```

```
sudo mysql -u root -p mysql < /usr/share/mysql/mysql_test_data_timezone.sql  
sudo mysql -u root -p
```

```
GRANT SELECT ON mysql.time_zone_name TO cactiuser@localhost;  
flush privileges;  
exit
```

### 6. scaricare cacti

```
wget https://www.cacti.net/downloads/cacti-latest.tar.gz  
tar -zxvf cacti-latest.tar.gz  
sudo mv cacti-1* /opt/cacti
```

## Aggiungere un altro apparecchio nella rete [↑](#)

Switch: 172.30.1.100 — .125

- 117 lab sistemi

Server:

- .230 squattero

- .199
- .229

[how-to-install-and-configure-mrtg-on-ubuntu-18.04](#)

[linux-snmp-oids-for-cpumemory-and-disk-statistics](#)

---



---



---

## Utilità e curiosità ↑

### Possibili problemi

1. problemi di rete a casa
  1. cambiare gli IP
  2. riga di routing dettagliate da Cisco: "192.168.1.1/32 sono io" e "192.168.1.120/32 sono io", e **il router sceglierà le righe più dettagliate**
  3. riga di routing: "192.168.1.0/24 via LAN"
  4. router di casa riesce assegnare DHCP al m0n0wall
  5. riga di routing aggiunta: "192.168.1.0/24 via WAN"
  6. riga di routing aggiunta: "0.0.0.0/0 via 192.168.1.1" riga più generica, considerata per ultima dal router
  7. dal client arriva richiesta di andare verso .1.5, ma non arriva poichè monowall è sulla stessa rete di quella fisica
  8. verso la .1.7 il router Cisco decide in modalità round-robin, quindi è probabile che non arrivi il pacchetto
  9. verso la 1.7 il router Linux dedice in modalità cronologica, mandando sempre in LAN il pacchetto
  10. Anche la metrica viene usata per valutare delle indecisioni di routing (metrica minore viene usata)
  11. m0n0wall e client a casa non funzionano per il problema della rete
    1. CREAZIONE DELLA RETE: scegliere 192.168.x.0 x = con uno pseudorandom (188 = BC <- oh c'mon)
    2. host www.facebook.com -> IPv6: face:b00c *oh c'mooooooooon*

(WAN) <—> 1.120 (DMZ router1) <—> |rete diversa| (LAN router2) .2.1 <—> host

1. pacchetti da installare (per Debian/Ubuntu e derivate) che potrebbero mancare

```
sudo apt search virtualbox—*
#fare apt install di quelli desiderati
```

2. riconfigurazione schede di rete

ifup nomeintefraccia

ifdown nomeinterfaccia

## Curiosità varie ↑

- possibilità di aumentare la banda aumentando il numero di interfacce
- Cellulari, sia Android che iOS, hanno il problema di cercare di velocizzare l'utilizzo dello stesso:
  1. cellulare al posto di inviare lo standard RFC 0.0.0.0
  2. configura i parametri della nuova rete con la vecchia configurazione della rete precedente
  3. appena si attacca, farà traffico con i vecchi IP
  4. INCONVENIENTE: cellulare nella vecchia rete era 192.168.1.5, nella rete in cui si connette cerca 192.168.1.5, DHCP se ne accorge dopo secondi, creando disservizio
- cron (cronos, tempo)
  1. Serve per eseguire dei comandi in orari prefissati
  2. Compito da fare alle 4 con pc spento:
    1. Linux: salta l'esecuzione del compito
    2. Windows: lo esegue appena acceso
  3. cron utilizzato per compiti di manutenzione
    1. compiti orari, giornalieri, settimanali, mensili, senza un'ora precisa
- anacron
  1. collabora con cron e gestisce la periodicità dei compiti da fare
  2. cron daily: cerca di lanciarlo alle 6, se non è accesa, lo avvia alla prima ora disponibile
  3. Se un pc non viene avviato per un po si crea una coda di programmi in cron.
- FHS
  1. [Filesystem Hierarchy wikipedia](#)
  2. dove sono i file nel filesystem linux
  3. sotto /etc/apt/sources.list o cartella sources.list.d/...
    1. in Debian si trovano delle configurazioni modulari = installare un software ha eseguibili, configurazioni e .deb per la configurazione iniziale
    2. aggiunge alla configurazione precedente
    3. ESEMPIO: scaricare Firefox, plugin installabili in maniera centralizzata, passando la configurazione nella sottocartella del file di configurazione di Firefox.
    4. FILE SOURCES.LIST contiene le configurazioni di dove trovare gli aggiornamenti Debian
    5. Commentare riga contenente gli aggiornamenti via CD
  4. apt update: scarica l'elenco del software per il controllo delle versioni
  5. apt upgrade: scarica il software aggiornato, momento delicato poichè deve seguire una scaletta di dipendenze
  6. aggiornamento della versione di Debian: tutte le dipendenze rischiano di rompere l'upgrade (dependency hell)
    1. dist-upgrade: esegue l'upgrade senza dare peso alle dipendenze, però portando ad interruzioni di servizio
- Usando il CD a casa richiede se si vuole scaricare dal CD o dalla rete, per rendere indipendente la macchina dall'uso del CD: *source*
- echo \$TERM : stampa il nome del terminale
- CTRL+D : uscire dall'utente
- nano .bashrc:

case "\$TERM" in

```
xterm-color|linux|...
alias shutdown=/sbin/shutdown
```

## Funzionamento librerie ↑

- Eseguitibile su winzoz: avanti forever e poi viene installato il programma con le librerie necessarie per ogni programma (Firefox e Thunderbird hanno le stesse librerie, vengono scaricate 2 volte e vengono trattate in modo differente)
- Programma in linux: i gestori delle distribuzioni modificano le librerie per il proprio sistema con risoluzione di problemi di compatibilità, rendendole univoche nel sistema. (per Debian ci sono i tester, obiettivo: risparmiare trasmissione dati, i pacchettatori prendevano i vari software esistenti per analizzarne le librerie richieste, senza avere il bisogno di riscargarle anche negli aggiornamenti) (ci possono essere varie versioni nello stesso sistema) Android: il Play store colleziona software adatto al sistema insieme alle loro librerie
- DEBIAN usa .deb (creato da Ian Mardock, Deb "Deborah" Ian)
- **DPKG** gestore di file
  - vincoli di dipendenze (con limiti sulle versioni)
- **APT** altro gestore
  - utilizza dpkg
  - retrocompatibile con i comandi dpkg
- **deb**: i pacchetti includono sia il programma che i file configurazione standard per l'autoconfigurazione durante l'installazione
- **deborphan**: cerca le librerie orfane, non necessarie a nessun software deb auto... : rimuove le librerie inutilizzate in automatico

## File utili ↑

file password:

```
cat /etc/shadow
```

file con la configurazione del profilo utente

```
sudo nano /etc/profile
# aggiungere :/usr/sbin dopo PATH
```

1. In caso di problemi con monowall, basta riavviarlo
2. Le macchine virtuali possono modificare le schede di rete anche durante le esecuzione delle stesse

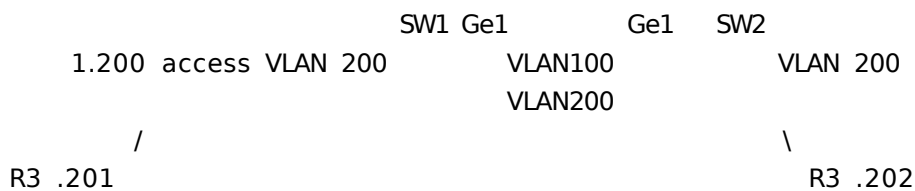
---

## Esercizio Cisco ↑

### SPERIMENTAZIONE VLAN CON ROUTER CISCO

192.168.3.0/24

```
R1 .101                                R2 .102
  \                                  /
1.100 access VLAN 100 .1             .2 VLAN 100
```



## Avvio di OS linux e init.d ↑

SystemV con vari run level

- run level 0: spegnimento
- run level 1: sistema avvio in manutenzione utente singole
- run level 3: uso comune in CLI
- run level 5: uso comune con GUI
- run level 6: riavvio in corso

Script che gestiscono i vari processi del PC: **/etc/init.d/**

Con SystemD ha un unico eseguibile che però è retrocompatibile:

`service apache2 status`

- Avvia più demoni contemporaneamente
- Gestisce i file di configurazione
- Ha degli ordini di priorità
- Usa linguaggi compilati, quindi aggiornare i processi all'avvio è diventato dispendioso ma hanno messo a disposizione il comando **systemctl**

`systemctl enable openvpn@nomeconfig.service #crea symlink al successo`

`systemctl start openvpn@nomeconfig.service`

Oppure si usa *la vecchia maniera* dopo aver usato systemctl

`./etc/init.d/openvpn status`

## Storia di CentOS ↑

- RedHat era inizialmente gratuito
- Prima viene fatta Mandrake, poi Mandriva
- Un gruppo decideva di comprare ogni versione per poi rimuovere quelle parti con licenza proprietaria
  - One cent operative system
  - Cent OS

## TODO ↑

- [x] clonare client, configurare clone e rinominarlo SERVER
- [x] cron e anacron

- [x] come viene gestito DHCP in LAN e come fare la DMZ
- [x] fare i sistemisti in Antartide nel mese invernale, il client è al caldo, il server e monowall sono nel container al freddo.  
Rinumerare rete IP di tutto con una procedura gestita solamente dal client. Scaletta delle cose da fare, ssh al server, web al monowall e testare la rete.
- [x] Fare regole firewall come indicato in **Restrizioni aggiuntive sul firewall**
- [x] Installare servizi nel server
- [x] configurare monitor delle risorse del server con mrtg
- [ ] Configurare cacti sul server