# RELAZIONE VIRTUALBOX

# Contents

**Virtualbox, Monowall e l'architettura client-server**

---

ITIS "E. Fermi" Bassano del Grappa
5^AI
Basso Nicola
aka Lince99

---

# INTRODUZIONE ↑

Descrizione VirtualBox


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 Monowall


Monowall logo

Monowall 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

---

# Utilità ↑

### 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. Creazione 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. Si
        2. 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 (Sì)
    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 telecontrollato 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
10. Manuale
    1. HDD nuovo da partizionare
       - ▷ 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)
       3. SCSI (0,0,0) (sda) - 10,7 GB
       4. msdos
    3. SPAZIO LIBERO
       1. Creare nuova paritzione
       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
          - 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. Yep
11. Sistema di base
    1. scelta del kernel: linux-image-amd64 (ultimo kernel stabile)
    2. generico (mappatura del disco all'avvio, driver autoconfigurati)
12. Gestore dei pacchetti
    1. No (solo software libero)
    2. Si Software contrib (software libero con parti non libere) (installazione di Adobe Flash Player (libreria), (Font proprietari Microsoft)
    3. No repository sorgenti APT
    4. Continua
13. Selezione installazione software:
    1. Deselezionare tutto
    2. Abilitare pacchetti VirtualBox
    3. Nessun auto update
    4. No partecipare alle statistiche
    5. Deseleziona tutto
14. 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
    2. Si
    3. /dev/sda
    4. Forzare l'installazione di GRUB su dispositivo rimovibile EFI? No

   - ▷ EFI: partizionamento da 100 MB nella prima parte del disco formattato in gpt
15. Terminare l'installazione
    1. Orologio di sistema da impostare su UTC? Si
       - ▷ Winzoz: locale
       - ▷ Linux: UTC
    2. 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
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)
   - 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 corrent
2. id uds : mostra i gruppi a cui appartiene all'utente
3. adduser uds sudo : iscrive un utente al gruppo
4. id uds : ricontrollo 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
    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
6. mettere servercognome invece di clientcognome
    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))
        1. 7 - Install on HDD
        2. ad0
        3. y
        4. al riavvio spegnere subito
    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)
    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. Peroò due server DHCP possono distribuire una porzione di indirizzi)
    9. ENTER (per dare un'indirizzo IP alla WAN, monowall ha inviato una richiesta DHCP nella rete presente)
    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 enviroment (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), ora include patch sia da )
        1. apt install lightdm mate firefox-esr
        2. S
        3. apt install firefox-esr-l10n-it (lingua italiana)
    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)
    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
        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 distaccata da quella del laboratorio)

**Configurazione Monowall ↑**

1. tornare su Firefox
    1. 192.168.1.1 sulla barra di ricerca per accedere alla pagina di gestione del router monowall
        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. hostaname: 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: possiblità 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 -> +
        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
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)
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

**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 Monowall ↑

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
    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
  2. 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
2. Studiare la migrazione 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
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 Monowall
    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 ↑

**Schema**

| da/a | LAN | WAN | DMZ |
|---|---|---|---|
| **LAN** | v | v(dns) | v*2 |
| **WAN** | x | v | v*2(dnat) |
| **DMZ** | x | v(dns,ntp,http) | v |

**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 Monowall lato LAN, le altre richieste TCP/UDP per il DNS da tagliare
- Creare alias per host-server, host-router-lan, host-router-dmz
- 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
  - monowall -> 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)
  - monowall -> 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)
    - ⋆ piu
      - ▷ diretto
      - ▷ #000000
      - ▷ Type: Direct (no proxy)
    - ⋆ piu
      - ▷ 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

**Realizzazione ↑**

- LAN to WAN: solo DNS in TCP/UDP

  - TCP/UDP from LAN port NOT host-router-lan to WAN port 53 (Block: LAN to WAN - DNS)

- LAN to DMZ: ammetti traffico HTTP e HTTPS solamente

  - TCP/UDP from LAN port any to DMZ port 80 (Pass: LAN to DMZ - HTTP)
  - TCP/UDP from LAN port any to DMZ port 443 (Pass: LAN to DMZ - HTTPS)

- WAN to DMZ: ammetti traffico HTTP e HTTPS solamente
  - TCP/UDP from WAN port any to DMZ port 80 (Pass: WAN to DMZ - HTTP)
  - TCP/UDP from WAN port any to DMZ port 443 (Pass: WAN to DMZ - HTTPS)
- WAN to LAN: blocca
- DMZ to WAN: ammetti traffico ICMP, DNS, NTP (UDP 123), aggiornamenti (3142)
  - protocol ICMP from DMZ port any to WAN port any (Pass: DMZ to WAN - ICMP)
  - TCP/UDP from DMZ port any to WAN port 53 (Pass: DMZ to WAN - DNS)
  - UDP from DMZ port any to WAN port 123 (Pass: DMZ to WAN - NTP)
  - TCP/UDP from DMZ port any to WAN port 3142 (Pass: DMZ to WAN - Updates)
- DMZ to client LAN port 2222
  - (in LAN) TCP from DMZ port 2222 to LAN port 22 (Pass: DMZ to LAN client - SSH port 2222 (normally disabled) )
  - (in DMZ) TCP from LAN client port 22 to DMZ port 2222 (Pass: DMZ to LAN client - SSH port 2222 (normally disabled) )
- Dal server DMZ per connettersi al client usare il NAT tramite porta 2222 (scelta)
- TEST:
  - client:
    - ping 1.1.1.1
    - TODO

---

# Utilità ↑

### 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 monowall
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. monowall e client a casa non funzionano per il problema della rete
    1. CREAZIONE DELLA RETE: scegliere 192.168.x.0 x = con uno pseudo-random (188 = BC <– oh c'mon)
    2. host www.facebook.com –> IPv6: face:b00c *oh c'mooooooon*

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

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

- Eseguibile su winzoz: avanti forever e poi viene installato il programma con le liberie 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, obbiettivo: risparmiare trasmissione dati, i pacchettatori prendevano i vari software esistenti per analizzarne le librerie richieste, senza avere il bisogno di riscaricarle anche negli aggiornamenti) (ci possono essere varie versioni nello stesso sistema) Android: il Play store colleziona software adatto al sistema insieme alle loro liberie
- 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
                           SW1 Ge1        Ge1   SW2
    1.200 access VLAN 200        VLAN100           VLAN 200
                                 VLAN200
        /                                             \
R3 .201                                                R3 .202
```

---

# 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.
- [ ] Fare regole firewall come indicato in **Restrizioni aggiuntive sul firewall**