**SISTEMI E RETI**

*FTP server su Ubuntu 18*

Aggiornare le repo

sudo apt-get update

installare il servizio chiamato vsftpd

sudo apt-get install vsftpd

per controllare il corretto funzionamento

sudo service vsftpd status

*LAMP Server (Apache2, MySql, PHP) su Ubuntu 18*

Installare apache

sudo apt install -y apache2 apache2-utils

per controllare se è partito il servizio

systemctl status apache2

per controllare il corretto funzionamento nel browser digitare localhost nella barra di ricerca e se funziona verrà restituita una schermata con scritto apache2 e “it works”

in caso contrario il firewall blocca la porta 80 e si dovrà attivare

con “iptables firewall”

sudo iptables -I INPUT -p tcp --dport 80 -j ACCEPT

con “UFW firewall”

sudo ufw allow http

ora impostare lo user apache come possessore della directory delle pagine web apache

sudo chown www-data:www-data /var/www/html/ -R

Installare MariaDB (MySql)

sudo apt install mariadb-server mariadb-client

far partire lo script di sicurezza post installazione

sudo mysql\_secure\_installation

Installare PHP7.2

sudo apt install php7.2 libapache2-mod-php7.2 php7.2-mysql php-common php7.2-cli php7.2-common php7.2-json php7.2-opcache php7.2-readline

attivare il modulo apache php7.2 e riavviare apache2

sudo a2enmod php7.2

sudo systemctl restart apache2

*Samba server su Ubuntu 18*

Aggiornare le repo

sudo apt-get update

installare il servizio

sudo apt install samba samba-common-bin

controllare se e’ attivo

sudo service smbd status

creare una condivisione privata di samba. Modificare il file /etc/samba/smb.conf.

sudo nano /etc/samba/smb.conf

Nella sezione [global], assicurarsi che il valore workgroup sia lo stesso con le impostazioni del gruppo di lavoro dei computer Windows.

Alla fine del file aggiungere le seguenti righe

[Private]

comment = needs username and password to access

path = /srv/private/

browseable = yes

guest ok = no

writable = yes

valid users = @samba

salvare e chiudere il file.

Ora creare un utente linux per samba

sudo adduser username

dopo il comando precedente verrà chiesta una password per il nuovo utente che non verrà usata per samba perché si utilizzerà una password samba

sudo smbpasswd -a username

ora creare il gruppo samba

sudo groupadd samba

aggiungere l’utente appena creato al gruppo

sudo gpasswd -a username samba

creare la cartella privata per la condivisione

sudo mkdir /srv/private/

Il gruppo samba deve avere permessi di lettura, scrittura ed esecuzione della cartella condivisa

sudo setfacl -R -m "g:samba:rwx" /srv/private/

controllare se sono presenti errori

testparm

riavviare il servizio

sudo systemctl restart smbd

creare una condivisione pubblica di samba. Modificare il file /etc/samba/smb.conf.

sudo nano /etc/samba/smb.conf

Nella sezione [global], assicurarsi che il valore workgroup sia lo stesso con le impostazioni del gruppo di lavoro dei computer Windows.

Alla fine del file aggiungere le seguenti righe

[public]

comment = public share, no need to enter username and password

path = /srv/public/

browseable = yes

writable = yes

guest ok = yes

salvare e chiudere il file

creare la cartella pubblica per la condivisione

sudo mkdir /srv/public

dare i permessi all’utente anonimo sulla cartella

sudo setfacl -R -m "u:nobody:rwx" /srv/public/

riavviare il servizio

sudo systemctl restart smbd

*Mail server su Ubuntu 18*

Aggiorniamo le repo

Sudo apt update

Installare postfix

sudo apt install postfix

fai un backup del file di configurazione principale

sudo cp /etc/postfix/main.cf /etc/postfix/main.cf.backup

apri il file main.cf

sudo nano /etc/postfix/main.cf

modificare il file inserendo $mydomain = il domonio, $myhostname = l’hostname

# Dns principale del server

myhostname = mail.domain.com

mydomain = domain.com

myorigin = $mydomain

#Parametri per l’interfaccia su cui far ascoltare la porta:

inet\_interfaces = localhost

inet\_protocols = ipv4

mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain

mynetworks = 127.0.0.0/8

relay\_domains =

# Directory di appoggio per salvare le caselle di posta

home\_mailbox = Maildir/

salva e chiudi il file.

Fai partire il servizio

sudo systemctl enable postfix

sudo systemctl start postfix

ora configurare il firewall per garantire il traffico

sudo ufw allow "Postfix"

sudo ufw allow "Postfix SMTPS"

sudo ufw allow "Postfix Submission"

*OpenVPN server su Ubuntu 18*

Aggiorna le repo

sudo apt update

scarica e avvia openvpn-install.sh

wget [https://git.io/vpn -O openvpn-install.sh](https://git.io/vpn%20-O%20openvpn-install.sh)

diamo i permessi

chmod +x openvpn-install.sh

avviamo openvpn-install.sh e inseriamo i dati richiesti

sudo ./openvpn-install.sh

dopo aver seguito i passaggi restartare il servizio

questi sono comandi da utlizzare

sudo systemctl stop openvpn@server # <--- stop server

sudo systemctl start openvpn@server # <--- start server

sudo systemctl restart openvpn@server # <--- restart server

sudo systemctl status openvpn@server # <--- get server status

*Proxy server su Ubuntu 18*

Aggiornare le repo

sudo apt update

installare squid

sudo apt install squid

la configurazione di squid si trova dentro al file squid.conf

fare il backup del file di configurazione

sudo cp /etc/squid/squid.conf /etc/squid/squid.conf.backup

aprire il file

sudo nano /etc/squid/squid.conf

l’obiettivo e’ bloccare specifici siti web, quindi cambiare la riga “http\_acces deny all” in “http\_access deny ban\_domains”

ora editare il file ban\_domains.txt

sudo nano /etc/squid/ban\_domains.txt

aggiungere I siti che si vogliono bloccare

[www.google.it](http://www.google.it)

[www.youtube.com](http://www.youtube.com)

riavviare il servizio

sudo systemctl restart squid

*Cli Cisco*

Avere i privilegi di root

Enable

Spostarsi sulla modalità di configurazione globale

Configure terminal

Spostarsi sulla configurazione di un’interfaccia

Es: Interface fastethernet 0/0

Interface <nomeinterfaccia> <numerointerfaccia>

Assegnare indirizzo ip ad un’interfaccia

Es: ip address 192.168.1.1 255.255.255.0

Ip address <indirizzo ip> <maschera>

Evitare lo spegnimento di un’interfaccia

No shutdown

Impostare una rotta statica sul router

Ip route <rete > <maschera> <nexthop>

Eliminare una rotta statica dal router

no Ip route <rete > <maschera> <nexthop>

Visualizzare le rotte presenti nel router

Show ip route

Visualizzare le interfacce di rete disponibili

Show interfaces

Impostare un’ACL

Access-list <numero> <permit|deny> <ip> <maschera>

Eliminare un’ACL

No access-list <numero>

Impostare un’ACL estesa

Access-list <numero> <permit|deny> <protocollo> <da ip e maschera > <a ip e maschera> <numeroporta>

Visualizzare le ACL presenti nel router

Show access-lists

Creare una VLAN

vlan <numerovlan>

Assegnare una porta ad una VLAN

Interface <porta>

Switchport mode access

Switchport access vlan <numerovlan>

Impostare una porta in trunk

Interface <porta>

Switchport mode trunk

Switchport trunk allowed vlan add <numerovlan>

Switchport trunk allowed vlan add <numerovlanaltroswitch>

Entrare in una subinterface

Es: interface fastethernet 0/0.1

Interface <nomeinterfaccia> <numerointerfaccia>.<numerosottointerfaccia>

Tornare ad una precedente modalità

Es: dall’interfaccia di una porta alla configurazione globale

Exit

Uscire e tornare al comando Enable

End