Università degli Studi Di Perugia
Dipartimento Di Matematica e Informatica

Anno Accademico 2017/2018

PROGETTO DI RETI DI CALCOLATORI: PROTOCOLLI

Prof. Sergio Tasso

Sabbatini Jessica
Taccucci Daniel

INDICE:

1. SCHEMA FISICO

L'Ospedale preso in esame è il "Life Hospital". Si richiede la progettazione e la configurazione di una rete aziendale.
L'Ospedale è dislocato in 5 edifici. Sono richiesti 1 server di posta elettronica, 1 server Web, almeno 2 server DNS, 1 server per applicazioni aziendali, 1 server Proxy e 1 server di Backup.
Tutte le postazioni devono essere collegate in rete, devono poter usufruire di tutti i servizi della rete, dell'accesso a internet e della possta elettronica; la rete deve essere protetta da firewall.

EDIFICIO	UFFICI & REPARTI	NUM. UTENTI	NUM. SERVER	COPERTURA WI-FI
A	Sala operatoria	100	0	No
B	RM	100	0	No
C	Reception	200	4	Sì
D	Ambulatorio	300	2	No
E	Garage ambulanze	50	1	No

Distanze tra gli edifici:

EDIFICI	DISTANZA
A – B	100 m
A – C	50 m
B – C	50 m
C – D	3 km
D – E	100 m

2. SCHEMA LOGICO

Edificio A – Sala operatoria

Sottorete con indirizzo 192.168.1.0/25 appartenente alla classe C, si divide la rete nel seguente modo:
Interior router "Venere" con l'indirizzo 192.168.1.1

Utente	Nome	Indirizzo IP
Utente 1	Postazione 1	192.168.1.2
...	...	...
Utente 100	Postazione 100	192.168.1.101

Edificio B – RM

Sottorete con indirizzo 192.168.2.0/25 appartenente alla classe C, si divide la rete nel seguente modo:
Interior router "Saturno" con l'indirizzo 192.168.2.1

Utente	Nome	Indirizzo IP
Utente 1	Postazione 1	192.168.2.2
...	...	...
Utente 100	Postazione 100	192.168.2.101

Edificio C – Reception

Sottorete con indirizzo 192.168.3.0/25 appartenente alla classe C, si divide la rete nel seguente modo:
Interior router "Terra" con l'indirizzo 192.168.3.1

Utente	Nome	Indirizzo IP
DMZ	DMZ	192.168.7.0
Server DNS	server-dns1	192.168.7.1
Server mail	server-mail	192.168.7.2
Server Web	server-web	192.168.7.3
Server Proxy	server-proxy	192.168.7.4
Exterior Router	exterior-router	201.123.15.0
Server DHCP	server-dhcp	192.168.3.2

Router Wi-Fi	router-wifi	192.168.3.3
Utente 1	Postazione 1	192.168.3.4
...	...	...
Utente 200	Postazione 200	192.168.3.203

Edificio D – Ambulatorio

Sottorete con indirizzo 192.168.4.0/25 appartenente alla classe C, si divide la rete nel seguente modo:
Interior router "Giove" con l'indirizzo 192.168.4.1
In questo edificio sono presenti 300 utenti, quindi una quantità superiore al numero di indirizzi assegnabili con 8 bit. Per risolvere questo problema, si utilizza uno switch da 52 porte per assegnare gli indirizzi rimasti.

Utente	Nome	Indirizzo IP
Server per Applicazioni Aziendali	server-appaz	192.168.4.2
Server DNS	server-dns2	192.168.4.3
Utente 1	Postazione 1	192.168.4.4
...	...	...
Utente 251	Postazione 251	192.168.4.254
Switch	switch1	192.168.4.255
Utente 252	Postazione 252	192.168.5.0
...	...	...
Utente 300	Postazione 300	192.168.5.47

Edificio E – Garage Ambulanze

Sottorete con indirizzo 192.168.6.0/25 appartenente alla classe C, si divide la rete nel seguente modo:
Interior router "Marte" con l'indirizzo 192.168.6.1

Utente	Nome	Indirizzo IP
Server backup	server-backup	192.168.6.2
Utente 1	Postazione 1	192.168.6.3
...	...	...
Utente 50	Postazione 50	192.168.6.52

RIEPILOGO

Sottoreti con indirizzi di broadcast e subnet masks.

Edificio	Indirizzo di rete	Subnet mask	Indirizzo di Broadcast	Nome rete
A	192.168.1.1	255.255.255.0	192.168.1.255	Rete A
B	192.168.2.1	255.255.255.0	192.168.2.255	Rete B
C	192.168.3.1	255.255.255.0	192.168.3.255	Rete C
D	192.168.4.1	255.255.255.0	192.168.4.255	Rete D
D	192.168.5.1	255.255.255.0	192.168.5.255	Rete D Switch
E	192.168.6.1	255.255.255.0	192.168.6.255	Rete E
DMZ	192.168.7.0	255.255.255.248	192.168.7.255	Rete DMZ

Collegamenti punto-punto tra gli interior router.

Sottorete	Indirizzo IP sottorete
Sala operatoria – RM (A – B)	192.168.10.0/30
Sala operatoria – Reception (A – C)	192.168.20.0/30
RM – Reception (B – C)	192.168.30.0/30
Reception – Ambulatorio (C – D)	192.168.40.0/30
Ambulatorio – Garage ambulanze (D - E)	192.168.50.0/30

3. COMPONENTI UTILIZZATI

Cavi di rete
Necessari per le connessioni tra gli host dei singoli edifici ed utilizzate per collegare edifici distanti fino a 100 metri.

Fibra ottica di tipo monomodale
Utilizzata per collegare con alte velocità gli edifici con distanze superiori ai 100 metri (Edifici C – D).

Router/Firewall
Dispositivi presenti in ogni edificio necessari per instradare i pacchetti nella rete verso la corretta destinazione, svolgendo pure varie funzioni di sicurezza essendo comprensivi anche di firewall per garantire maggiore sicurezza sui dati sensibili in entrata o in uscita.

Access Point Wireless
Fornisce un punto di accesso alla rete a tutti i dispositivi mobili in qualsiasi punto dell'edifico.

Switch
Dispositivi situati in ogni sede, connettono tra di loro gli hosts indirizzando i pacchetti solo al corretto destinatario riducendo le collisioni.

4. CONFIGURAZIONE INTERFACCIA DI RETE

ifconfig.cf

#configurazione edificio A

#interior router "Venere"

ifconfig eth0 192.168.1.1 netmask 255.255.255.0 broadcast 192.168.1.255

#interfaccia verso sottorete locale

ifconfig eth1 192.168.10.0 netmask 255.255.255.0 broadcast 192.168.10.255

#interfaccia verso l'edificio B

ifconfig eth2 192.168.20.0 netmask 255.255.255.0 broadcast 192.168.20.255

#interfaccia verso l'edificio C

#SOTTORETE "Rete A"

ifconfig eth0 192.168.1.2 netmask 255.255.255.0 broadcast 192.168.1.255

#Postazione 1

...

ifconfig eth0 192.168.1.101 netmask 255.255.255.0 broadcast 192.168.1.255

#Postazione 100

#configurazione edificio B

#interior router "Saturno"

ifconfig eth0 192.168.2.1 netmask 255.255.255.0 broadcast 192.168.2.255

#interfaccia verso sottorete locale

ifconfig eht5 192.168.10.0 netmask 255.255.255.0 broadcast 192.168.10.255

#interfaccia verso l'edificio A

ifconfig eth6 192.168.30.0 netmask 255.255.255.0 broadcast 192.168.30.255

#interfaccia verso l'edificio C

#SOTTORETE "Rete B"

ifconfig eth0 192.168.2.2 netmask 255.255.255.0 broadcast 192.168.2.255

#Postazione 1

...

ifconfig eth0 192.168.2.101 netmask 255.255.255.0 broadcast 192.168.2.255

#Postazione 100

#configurazione edificio C

#configurazione DMZ

ifconfig eth0 192.168.7.1 netmask 255.255.255.0 broadcast 192.168.7.255

#Server DNS1

ifconfig eth0 192.168.7.2 netmask 255.255.255.0 broadcast 192.168.7.255

#Server MAIL

ifconfig eth0 192.168.7.3 netmask 255.255.255.0 broadcast 192.168.7.255

#Server WEB

ifconfig eth0 192.168.7.4 netmask 255.255.255.0 broadcast 192.168.7.255

#Server Proxy

ifconfig ehtl 201.123.15.0 netmask 255.255.255.0 broadcast 201.123.15.255

#Exterior Router

#ROUTER WIFI

ifconfig eth3 192.168.3.3 netmask 255.255.255.0 broadcast 192.168.3.255

#interior router "Terra"

ifconfig ethl 192.168.3.1 netmask 255.255.255.0 broadcast 192.168.3.255

#interfaccia verso sottorete locale

ifconfig ethl 192.168.20.0 netmask 255.255.255.0 broadcast 192.168.20.255

#interfaccia verso l'edificio A

ifconfig ethl 192.168.30.0 netmask 255.255.255.0 broadcast 192.168.30.255

#interfaccia verso l'edificio B

ifconfig ethl 192.168.40.0 netmask 255.255.255.0 broadcast 192.168.40.255

#interfaccia verso l'edificio D

#SOTTORETE "Rete C"

ifconfig eth0 192.168.3.4 netmask 255.255.255.0 broadcast 192.168.3.255

#Postazione 1

...

ifconfig eth0 192.168.3.203 netmask 255.255.255.0 broadcast 192.168.3.255

#Postazione 200

Configurazione DHCP

 # dhcp.conf per la sottorete "Rete C" dell'edificio C

default-lease-time 3600;

max-lease-time 86000;

ddns-update-style none;

option subnet-mask 255.255.255.0; **# netmask fornita ai client dal server**

option domain-name-servers 192.168.7.1, 192.168.4.3; **# dns da poter usare**

option domain-name "lifehospital.it"; **# Questa opzione specifica il dominio**

 # che verrà servito ai client come il dominio di default di ricerca

subnet 192.168.2.1 { **# pool di indirizzi ip da poter assegnare**

range 192.168.8.0 192.168.8.255;

};

#configurazione edificio D

#SERVER APPLICAZIONI AZIENDALI

ifconfig eth0 192.168.4.2 netmask 255.255.255.0 broadcast 192.168.4.255

#SERVER DNS2

ifconfig eth1 192.168.4.3 netmask 255.255.255.0 broadcast 192.168.4.255

#interior router "Giove"

ifconfig eth0 192.168.4.1 netmask 255.255.255.0 broadcast 192.168.4.255

#interfaccia verso sottorete locale

ifconfig eth2 192.168.40.0 netmask 255.255.255.0 broadcast 192.168.40.255

#interfaccia verso l'edificio C

ifconfig eth3 192.168.50.0 netmask 255.255.255.0 broadcast 192.168.50.255

#interfaccia verso l'edificio E

#SOTTORETE "Rete D"

ifconfig eth0 192.168.4.4 netmask 255.255.255.0 broadcast 192.168.4.255

#Postazione 1

…

ifconfig eth0 192.168.4.254 netmask 255.255.255.0 broadcast 192.168.4.255

#Postazione 251

ifconfig eth0 192.168.5.0 netmask 255.255.255.0 broadcast 192.168.5.255

#Postazione 252

...

ifconfig eth0 192.168.5.47 netmask 255.255.255.0 broadcast 192.168.5.255

#Postazione 300

#configurazione edificio E

#SERVER BACKUP

ifconfig eth0 192.168.6.2 netmask 255.255.255.0 broadcast 192.168.6.255

#interior router "Marte"

ifconfig eth0 192.168.6.1 netmask 255.255.255.0 broadcast 192.168.6.255

#interfaccia verso sottorete locale

ifconfig eth2 192.168.50.0 netmask 255.255.255.0 broadcast 192.168.50.255

#interfaccia verso l'edificio D

#SOTTORETE "Rete E"

ifconfig eth0 192.168.6.3 netmask 255.255.255.0 broadcast 192.168.6.255

#Postazione 1

...

ifconfig eth0 192.168.6.52 netmask 255.255.255.0 broadcast 192.168.6.255

#Postazione 50

5. CONFIGURAZIONE ROUTING

Per il routing all'interno della rete privata abbiamo deciso di usare un routing dinamico configurando il protocollo RIP (Routing Information Protocol). RIP è un protocollo di routing interno basato su una metrica vettore-distanza, molto leggero da eseguire ed ormai standard in ambito Unix. È gestito o dal demone routed o da quello gated, da noi utilizzato. Di seguito i file di configurazione gated.conf dei vari router.

- **gated.conf**

#Router Venere

```
interfaces {
        interface 192.168.1.1 passive;          # Evita di chiudere l'accesso alla sottorete
                                                # per timeout
        interface 192.168.10.0 active;          # Verso l'edificio B
        interface 192.168.20.0 active;          # Verso l'edificio C
};
#dalle interfacce ricevo le informazioni del router
rip yes {
        broadcast;
        interface 192.168.10.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.20.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
```

```
#esporto il tutto alle reti
export proto rip metric 0 {
        proto direct interface 192.168.1.1 {
                network 192.168.1.0;
        };
};
```

#Router Saturno

```
interfaces {
        interface 192.168.2.1 passive;          # Evita di chiudere l'accesso alla sottorete
                                                # per timeout
        interface 192.168.10.0 active;          # Verso l'edificio A
        interface 192.168.30.0 active;          # Verso l'edificio C
};
#dalle interfacce ricevo le informazioni del router
rip yes {
        broadcast;
        interface 192.168.10.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.30.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
#esporto il tutto alle reti
export proto rip metric 0 {;
        proto direct interface 192.168.2.1 {
```

```
        network 192.168.2.0;
    };
};
```

#Router Terra

```
interfaces {
    interface 192.168.3.1 passive;          # Evita di chiudere l'accesso alla sottorete
                                            # per timeout
    interface 192.168.7.0 active;           # Verso server DMZ
    interface 192.168.7.1 active;           # Verso server DNS1 nella DMZ
    interface 192.168.7.2 active;           # Verso server MAIL nella DMZ
    interface 192.168.7.3 active;           # Verso server WEB nella DMZ
    interface 192.168.7.4 active;           # Verso server proxy nella DMZ
    interface 201.123.15.0 active;          # Verso exterior router
    interface 192.168.3.2 active;           # Verso server DHCP
    interface 192.168.3.3 active;           # Verso router WIFI
    interface 192.168.20.0 active;          # Verso l'edificio A
    interface 192.168.30.0 active;          # Verso l'edificio B
    interface 192.168.40.0 active;          # Verso l'edificio D
};
#dalle interfacce ricevo le informazioni del router
rip yes {
    broadcast;
    interface 192.168.3.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
    };
    interface 192.168.7.0 {
        version 2;
        multicast;
```

```
        authentication simple "RIPauth";
};
interface 192.168.7.1 {
        version 2;
        multicast;
        authentication simple "RIPauth";
};
interface 192.168.7.2 {
        version 2;
        multicast;
        authentication simple "RIPauth";
};
interface 192.168.7.3 {
        version 2;
        multicast;
        authentication simple "RIPauth";
};
interface 192.168.7.4 {
        version 2;
        multicast;
        authentication simple "RIPauth";
};
interface 201.123.15.0 {
        version 2;
        multicast;
        authentication simple "RIPauth";
};
interface 192.168.3.2 {
        version 2;
        multicast;
```

```
                authentication simple "RIPauth";
        };
        interface 192.168.3.3 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.20.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.30.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.40.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
#esporto il tutto alle reti
export proto rip metric 0 {;
        proto direct interface 192.168.3.1 {
                network 192.168.3.0;
        };
};
```

#Router Giove

```
interfaces {
        interface 192.168.4.1 passive;          # Evita di chiudere l'accesso alla sottorete
                                                # per timeout
        interface 192.168.4.2 active;           # Verso applicazione aziendale
        interface 192.168.4.3 active;           # Verso server DNS2
        interface 192.168.40.0 active;          # Verso l'edificio C
        interface 192.168.50.0 active;          # Verso l'edificio E
};
#dalle interfacce ricevo le informazioni del router
rip yes {
        broadcast;
        interface 192.168.4.2 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.4.3 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.40.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.50.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
```

```
        };
};
#esporto il tutto alle reti
export proto rip metric 0 {;
        proto direct interface 192.168.4.1 {
                network 192.168.4.0;
        };
};
```

#Router Marte

```
interfaces {
        interface 192.168.6.1 passive;          # Evita di chiudere l'accesso alla sottorete
                                                # per timeout
        interface 192.168.6.2 active;           # Verso server BACKUP
        interface 192.168.50.0 active;          # Verso l'edificio D
};
#dalle interfacce ricevo le informazioni del router
rip yes {
        broadcast;
        interface 192.168.6.2 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
        interface 192.168.50.0 {
                version 2;
                multicast;
                authentication simple "RIPauth";
        };
};
```

#esporto il tutto alle reti

```
export proto rip metric 0 {;
        proto direct interface 192.168.6.1 {
                network 192.168.6.0;
        };
};
```

6. CONFIGURAZIONE DNS

I DNS forniscono la risoluzione dei nomi degli hosts per la rete. I due server DNS presenti nella nostra rete, DNS1 eDNS2, sono l'uno slave dell'altro.
Il DNS1, situato nell'area DMZ della Reception, gestisce i nomi degli hosts presenti nella DMZ ed accessibili dall'esterno. Si occupa della risoluzione dei nomi nella rete locale.
Il DNS2 si occupa invece della rete interna.

#file di configurazione resolv.conf del resolver, che comprende la lista dei name server da interrogare

- **resolv.conf**

```
domain lifehospital.it          # nome del dominio di default
nameserver 127.0.0.1            # local-host
nameserver 192.168.7.1          # server DNS1
nameserver 192.168.4.3          # server DNS2
```

#file named.conf e relativi zone files per la rete locale, usati dal daemon named per rispondere alle query

- **named.conf**

```
options {                       # definizione delle impostazioni globali di BIND
        directory "/etc/named/";        # directory di lavoro
        pid-file "named.pid";           # inserimento dei file pid nella directory di lavoro
        allow-query { any; };           # accetta query da qualsiasi host
        recursion no;                   # no servizio ricorsivo
};
zone "." {
        type hint;
        file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
        notify no;
```

```
};

//Sala Operatoria
zone "salaOperatoria.lifehospital.it" {
        type master;
        file "salaOperatoria.hosts";
        allow-transfer { };
};
zone "1.168.192.in-addr.arpa" {
        type master;
        file "salaOperatoria.rev";
        allow-transfer { };
};

//RM
zone "RM.lifehospital.it" {
        type master;
        file "RM.hosts";
        allow-transfer { };
};
zone "2.168.198.in-addr.arpa" {
        type master;
        file "RM.rev";
        allow-transfer { };
};

//Reception
zone "reception.lifehospital.it" {
        type master;
        file "reception.hosts";
        allow-transfer { };
```

```
};
zone "3.168.192.in-addr.arpa" {
        type master;
        file "reception.rev";
        allow-transfer { };
};

//Ambulatorio
zone "ambulatorio.lifehospital.it" {
        type master;
        file "ambulatorio.hosts";
        allow-transfer { };
};
zone "4.168.192.in-addr.arpa" {
        type master;
        file "ambulatorio.rev";
        allow-transfer { };
};
zone "5.168.192.in-addr.arpa" {
        type master;
        file "ambulatorio.rev";
        allow-transfer { };
};

//Garage Ambulanze
zone "garageAmbulanze.lifehospital.it" {
        type master;
        file "garageAmbulanze.hosts";
        allow-transfer { };
};
zone "6.168.192.in-addr.arpa" {
```

```
        type master;
        file "garageAmbulanze.rev";
        allow-transfer { };
};
```

- **named.ca**

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache . <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;           file                /domain/named.cache
;           on server           FTP.INTERNIC.NET
;       -OR-                    RS.INTERNIC.NET
;
;       last update: September 4, 2018
;       related version of root zone: 2018090400
;
; formerly NS.INTERNIC.NET
;
.                                   3600000  NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.         3600000  A 198.41.0.4
A.ROOT-SERVERS.NET.         3600000  AAAA 2001:503:ba3e::2:30
;
; FORMERLY NSI.ISI.EDU
;
.                                   3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.         3600000 A 192.228.79.201
B.ROOT-SERVERS.NET.         3600000 AAAA 2001:500:84::b
```

```
;
; FORMERLY C.PSI.NET
;
.                       3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000 A 192.33.4.12
C.ROOT-SERVERS.NET.     3600000 AAAA 2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                       3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000 A 199.7.91.13
D.ROOT-SERVERS.NET.     3600000 AAAA 2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                       3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.     3600000 A 192.203.230.10
E.ROOT-SERVERS.NET.     3600000 AAAA 2001:500:a8::e
;
; FORMERLY NS.ISC.ORG
;
.                       3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.     3600000 A 192.5.5.241
F.ROOT-SERVERS.NET.     3600000 AAAA 2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.                       3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.     3600000 A 192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                       3600000 NS H.ROOT-SERVERS.NET.
```

```
H.ROOT-SERVERS.NET.      3600000 A 198.97.190.53
H.ROOT-SERVERS.NET.      3600000 AAAA 2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000 A 192.36.148.17
I.ROOT-SERVERS.NET.      3600000 AAAA 2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.                        3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000 A 192.58.128.30
J.ROOT-SERVERS.NET.      3600000 AAAA 2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
.                        3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.      3600000 A 193.0.14.129
K.ROOT-SERVERS.NET.      3600000 AAAA 2001:7fd::1
;
; OPERATED BY ICANN
;
.                        3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.      3600000 A 199.7.83.42
L.ROOT-SERVERS.NET.      3600000 AAAA 2001:500:9f::42
;
; OPERATED BY WIDE
;
.                        3600000 NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.      3600000 A 202.12.27.33
M.ROOT-SERVERS.NET.      3600000 AAAA 2001:dc3::35
; End of File
```

- **named.local**

```
$TTL 86400
@       IN      SOA     localhost.              admin.lifehospital.it {
        2014051601              ;Serial
        28800                   ;Refresh
        14400                   ;Retry
        3600000                 ;Expire
        86400                   ;Minimum
}
        IN      NS      localhost.
1       IN      PTR     localhost.
```

- **salaOperatoria.hosts**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
```

; Definizione server DNS e mail

```
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
```

; Definizione host

```
Venere          IN      A       192.168.1.1         # Router
host_1          IN      A       192.168.1.2         # Host 1
   ...
host_100        IN      A       192.168.1.101       # Host 100
```

- **salaOperatoria.rev**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
1               IN      PTR     venere.salaOperatoria.lifehospital.it       # Router
2               IN      PTR     host_1.salaOperatoria.lifehospital.it       # Host 1
 ...
101             IN      PTR     host_100.salaOperatoria.lifehospital.it     # Host 100
```

- **RM.hosts**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
Saturno IN      A       192.168.2.1                 # Router
host_1  IN      A       192.168.2.2                 # Host 1
```

...

```
host_100  IN      A       192.168.2.101                   # Host 100
```

- **RM.rev**

```
$TTL 86400
@       IN      SOA             dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
1               IN      PTR     saturno.RM.lifehospital.it      # Router
2               IN      PTR     host_1.RM.lifehospital.it       # Host 1
...
101             IN      PTR     host_100.RM.lifehospital.it     # Host 100
```

- **reception.hosts**

```
$TTL 86400
@       IN      SOA             dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
```

Terra	IN	A	192.168.3.1	**# Router**
dns1	IN	A	192.168.7.1	**# Server DNS**
server-mail	IN	A	192.168.7.2	**# Server Mail**
server-dhcp	IN	A	192.168.3.2	**# Server DHCP**
host_1	IN	A	192.168.3.4	**# Host 1**
…				
host_200	IN	A	192.168.3.203	**# Host 200**

- **reception.rev**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
```

; **Definizione server DNS e mail**

```
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
```

; **Definizione host**

1	IN	PTR	terra.reception.lifehospital.it	**# Router**
2	IN	PTR	dns1.reception.lifehospital.it	**# Server DNS**
3	IN	PTR	server-mail.reception.lifehospital.it	**# Server Mail**
4	IN	PTR	server-dhcp.reception.lifehospital.it	**# Server DHCP**
5	IN	PTR	host_1.reception.lifehospital.it	**# Host 1**
…				
204	IN	PTR	host_200.reception.lifehospital.it	**# Host 200**

- **ambulatorio.hosts**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
```

```
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
Giove           IN      A       192.168.4.1         # Router
server-appaz    IN      A       192.168.4.2         # Server Applicazione Aziendale
dns2            IN      A       192.168.4.3         # Server DNS
host_1          IN      A       192.168.4.4         # Host 1
   ...
host_251        IN      A       192.168.4.254       # Host 251
host_252        IN      A       192.168.5.0         # Host 252
   ...
host_300        IN      A       192.168.5.47        # Host 300
```

- **ambulatorio.rev**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
1               IN      PTR     giove.ambulatorio.lifehospital.it       # Router
```

2	IN	PTR	server-appaz.ambulatorio.lifehospital.it	**# Server app. aziendale**
3	IN	PTR	dns2.ambulatorio.lifehospital.it	**# Server DNS**
4	IN	PTR	host_1.ambulatorio.lifehospital.it	**# Host 1**
…				
254	IN	PTR	host_251.ambulatorio.lifehospital.it	**# Host 251**
255	IN	PTR	host_252.ambulatorio.lifehospital.it	**# Host 252**
…				
303	IN	PTR	host_300.ambulatorio.lifehospital.it	**# Host 300**

- **garageAmbulanze.hosts**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
}
; Definizione server DNS e mail
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione host
Marte           IN      A       192.168.6.1             # Router
server-backup   IN      A       192.168.6.2             # Server Backup
host_1          IN      A       192.168.6.3             # Host 1
    …
host_50 IN      A       192.168.6.52                    # Host 50
```

- **garageAmbulanze.rev**

```
$TTL 86400
@       IN      SOA     dns2.reception.lifehospital.it      admin.lifehospital.it {
        2014051701              ;Serial
        86400                   ;Refresh
```

```
        3600                    ;Retry
        604800                  ;Expire
        86400                   ;Minimum
)
```

; Definizione server DNS e mail

```
IN NS dns2.ambulatorio.lifehospital.it
IN MX 10 server-mail.lifehospital.it
```

; Definizione host

```
1       IN      PTR     marte.garageAmbulanze.lifehospital.it           # Router
2       IN      PTR     server-backup.garageAmbulanze.lifehospital.it   # Server Backup
3       IN      PTR     host_1.garageAmbulanze.lifehospital.it          # Host 1
  ...
52      IN      PTR     host_50.garageAmbulanze.lifehospital.it         # Host 50
```

Il "DNS1" è situato nella DMZ e risolve i nomi dei vari servizi presenti in essa.

- **resolv.conf**

```
domain          lifehospital.it
nameserver      127.0.0.1
nameserver      192.168.7.1     #server-dns1
nameserver      192.168.4.3     #server-dns2
```

- **named.conf**

```
options {
        directory "/etc/namedb";
        pid-file "named.pid";
        allow-query { any; };
        recursion no;
};
zone "."{
        type hint;
        file "named.ca";
};
zone "localhost" IN {
```

```
        type master;
        file "localhost.zone";
        notify no;
};
zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
        notify no;
};
```

#DMZ

```
zone "lifehospital.it" {
        type master;
        file "DMZ.hosts";
        allow-transfer {};
};
zone "7.168.192.in-addr.arpa" {
        type master;
        file "DMZ.rev";
        allow-transfer {};
};
```

- **named.ca**

```
;       This file holds the information on root name servers needed to
;       initialize cache of Internet domain name servers
;       (e.g. reference this file in the "cache . <file>"
;       configuration file of BIND domain name servers).
;
;       This file is made available by InterNIC
;       under anonymous FTP as
;               file                /domain/named.cache
;               on server           FTP.INTERNIC.NET
;       -OR-                        RS.INTERNIC.NET
```

```
;
;            last update: September 4, 2018
;            related version of root zone: 2018090400
;
; formerly NS.INTERNIC.NET
;
.                                    3600000 NS A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.          3600000 A 198.41.0.4
A.ROOT-SERVERS.NET.          3600000 AAAA 2001:503:ba3e::2:30
;
; FORMERLY NSI.ISI.EDU
;
.                                    3600000 NS B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.          3600000 A 192.228.79.201
B.ROOT-SERVERS.NET.          3600000 AAAA 2001:500:84::b
;
; FORMERLY C.PSI.NET
;
.                                    3600000 NS C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.          3600000 A 192.33.4.12
C.ROOT-SERVERS.NET.          3600000 AAAA 2001:500:2::c
;
; FORMERLY TERP.UMD.EDU
;
.                                    3600000 NS D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.          3600000 A 199.7.91.13
D.ROOT-SERVERS.NET.          3600000 AAAA 2001:500:2d::d
;
; FORMERLY NS.NASA.GOV
;
.                                    3600000 NS E.ROOT-SERVERS.NET.
E.ROOT-SERVERS.NET.          3600000 A 192.203.230.10
```

```
E.ROOT-SERVERS.NET.      3600000 AAAA 2001:500:a8::e
;
; FORMERLY NS.ISC.ORG
;
.                        3600000 NS F.ROOT-SERVERS.NET.
F.ROOT-SERVERS.NET.      3600000 A 192.5.5.241
F.ROOT-SERVERS.NET.      3600000 AAAA 2001:500:2f::f
;
; FORMERLY NS.NIC.DDN.MIL
;
.                        3600000 NS G.ROOT-SERVERS.NET.
G.ROOT-SERVERS.NET.      3600000 A 192.112.36.4
;
; FORMERLY AOS.ARL.ARMY.MIL
;
.                        3600000 NS H.ROOT-SERVERS.NET.
H.ROOT-SERVERS.NET.      3600000 A 198.97.190.53
H.ROOT-SERVERS.NET.      3600000 AAAA 2001:500:1::53
;
; FORMERLY NIC.NORDU.NET
;
.                        3600000 NS I.ROOT-SERVERS.NET.
I.ROOT-SERVERS.NET.      3600000 A 192.36.148.17
I.ROOT-SERVERS.NET.      3600000 AAAA 2001:7fe::53
;
; OPERATED BY VERISIGN, INC.
;
.                        3600000 NS J.ROOT-SERVERS.NET.
J.ROOT-SERVERS.NET.      3600000 A 192.58.128.30
J.ROOT-SERVERS.NET.      3600000 AAAA 2001:503:c27::2:30
;
; OPERATED BY RIPE NCC
;
```

```
.                       3600000 NS K.ROOT-SERVERS.NET.
K.ROOT-SERVERS.NET.     3600000 A 193.0.14.129
K.ROOT-SERVERS.NET.     3600000 AAAA 2001:7fd::1
;
; OPERATED BY ICANN
;
.                       3600000 NS L.ROOT-SERVERS.NET.
L.ROOT-SERVERS.NET.     3600000 A 199.7.83.42
L.ROOT-SERVERS.NET.     3600000 AAAA 2001:500:9f::42
;
; OPERATED BY WIDE
;
.                       3600000 NS M.ROOT-SERVERS.NET.
M.ROOT-SERVERS.NET.     3600000 A 202.12.27.33
M.ROOT-SERVERS.NET.     3600000 AAAA 2001:dc3::35
; End of file
```

- **named.local**

```
named.local
$TTL 86400
@       IN      SOA     localhost.                      admin.lifehospital.it {
        2014051601      ;Serial
        28800           ;Refresh
        14400           ;Retry
        3600000         ;Expire
        86400           ;Minimum
}
        IN      NS      localhost.
1       IN      PTR     localhost.
```

- **localhost.zone**

```
$TTL 86400
@       1D      IN      SOA     @       admin (
                2014052002      ;Serial
                36000           ;Refresh
                3600            ;Retry
                3600000         ;Expire
                36000           ;Minimum
)
                1D      IN      NS      @
                1D      IN      A       127.0.0.
```

- **dmz.hosts**

```
$TTL 86400
@       IN              SOA             dns1.lifehospital.it        admin.lifehospital.it (
                2014052002      ;Serial
                36000           ;Refresh
                3600            ;Retry
                3600000         ;Expire
                36000           ;Minimum
)
; Definizione dei server DNS e mail
IN NS dns1.reception.lifehospital.it
IN MX 10 server-mail.lifehospital.it
; Definizione hosts
dmz             IN      A       192.168.7.0     # Router
server-dns1     IN      A       192.168.7.1     # Server DNS1
dns 1           CNAME   A       server-dns1     # Alias del Server DNS1
server-mail     IN      A       192.168.7.2     # Server Mail
mail            CNAME   A       server-mail     # Alias Server Mail
server-web      IN      A       192.168.7.3     # Server Web
www             CNAME   A       server-web      # Alias Server Web
server-proxy    IN      A       192.168.7.4     # Server Proxy
```

proxy	CNAME	A	server-proxy	**# Alias Server Proxy**
exterior-router	IN	A	123.123.15.0	**# Exterior Router**
ext-router	CNAME	A	exterior-router	**# Alias Exterior Router**

- **dmz.rev**

$TTL 86400

@	IN	SOA	dns1.lifehospital.it	admin.lifehospital.it (
	2014052002	;Serial		
	36000	;Refresh		
	3600	;Retry		
	3600000	;Expire		
	36000	;Minimum		

)

; **Definizione dei server DNS e mail**

IN NS dns1.reception.lifehospital.it

IN MX 10 server-mail.lifehospital.it

; **Definizione hosts**

1	IN	PTR	dmz.lifehospital.it	**# Router**
2	IN	PTR	dns1.lifehospital.it	**# Server DNS1**
3	IN	PTR	server-mail.lifehospital.it	**# Server Mail**
4	IN	PTR	server-web.lifehospital.it	**# Server Web**
5	IN	PTR	server-proxy.lifehospital.it	**# Proxy**
6	IN	PTR	exterior-router.lifehospital.it	**# Exterior Router**

7. CONFIGURAZIONE SENDMAIL

Nella DMZ è presente un Server Mail per la gestione degli indirizzi di posta utilizzati nell'azienda. Utilizzeremo il programma sendmail, altamente personalizzabile.
Il programma usa due file (sendmail.cf e sendmail.mc) per la propria configurazione, più un file alias per la definizione degli indirizzi.

Cominciamo con la configurazione di "sendmail" utilizzato esclusivamente dai dipendenti dell'azienda.

- ***sendmail.cf***

/etc/sendmail.cf

 # Macro utente

(definizione obbligatoria, specifica le informazioni proprie della rete)

server-mail	**# Hostname**
lifehospital.it	**# Impostazione dominio**
Dj$w.$D	**# Nome del dominio**
De$j Sendmail $v ready at $	**# Messaggio iniziale SMTP**
DlFrom $g $d	**# Formato della UNIX**
DnMAILER-DAEMON	**# Messaggio d'errore**
Do.:%\@!^=/	**# Operatori validi indirizzi**
Dqg?x ($x)$.	**# Indirizzo del mittente**

 # Trusted users

(utenti fidati che possono cambiare l'indirizzo del mittente usando il FLAG-f)

Troot

Tdaemon

Tuucp

 # Priorità messaggi nelle code

Pfirst-class=0

Pspecial-delivery=100

Pbulk=-60

Pjunk=-100

 # Formato delle intestazioni

```
H?P?Return-Path: <$g>                    # Path del mailer
HReceived: $?sfrom $s $.by $j ($v/$Z)    # Ricevuta da
H?D?Resent-Date: $a                      # Data di partenza
H?D?Date: $ A
H?F?Resent-From: $?x$x <$g>$|$g$.        # Forward
H?F?From : $?x$x $|$g$.                  # Nome mittente
H?x?Full-Name: $x                        # Impostazione fullname
HPosted-Date: $a                         # Data di partenza
H?l?Received-Date: $b                    # Data
HSubject:
H?M?Resent-Message-Id: <$t.$i@$j>        # Ora attuale
H?M?Message-Id: <$t.$i@$j>               # Ora in formato-id della coda
```

 # Definizione delle options

(sezione che definisce le opzioni di sendmail)

```
OA/etc/alias                             # Definizione del file degli alias
OErrorHeader=/etc/sendmail.oE            # Messaggi di errore di header/file
OF0600                                   # Permesso per i temporary file
OHman=/usr/lib/sendmail.hf               # Help nel file di sendmail
OQueueDirectory=/var/spool/mqueue        # Directory queue
OTimeout.queuereturn=5d                  # Tempo di coda
OTimeout.queuewarn=4h
OStatusFile=/var/tmp/sendmail.st         # File di stato
OHostsFile=/etc/hosts                    # Hosts file
OPrivacyOptions=authwarnings,noexpn,novrfy  # Impediamo agli spammer di usare i
                                         # comandi di sendmail "EXPN" e
                                         # "VRFY" spesso sfruttati da questi
```

 # Configurazione del mailer

(definisce le istruzioni usate da sendmail per invocare i programmi di spedizione di posta)

```
Mlocal, P=/bin/mail, F=rlsDFMmn, S=10, R=20, A=mail -d $u
Mprog, P=/bin/sh, F=lsDFMe, S=10, R=20, A=sh -c $u
Mtcpld, P=[ICP], F=mDFMueXLC, S=17, R=27, A=IPC $h, E=\r\n
```

Mtcp, P=[ICP], F=mDFMueXLC, S=14, R=24, A=IPC $h, E=\r\n

Muucp, P=/usr/bin/uux, F=DFMhuU, S=13, R=23, M=100000,

A=uux - -r -z -a$f -gC $h!rmail ($u)

- ***sendmail.mc***

```
divert(-1)
        This is the sendmail macro config file. If you make changes to this file,
        you need the sendmail-cf rpm installed and then have to generate a
        new /etc/sendmail.cf by running the following command:
        m4 /etc/mail/sendmail.mc > /etc/sendmail.cf
divert(0)
include(`/usr/share/sendmail-cf/m4/cf.m4')
VERSIONID(`linux')dnl
OSTYPE(`linux')
define(`confDEF_USER_ID',``8:12'')dnl
undefine(`UUCP_RELAY')dnl
undefine(`BITNET_RELAY')dnl
define(`confAUTO_REBUILD')dnl
define(`confTO_CONNECT', `1m')dnl
define(`confTRY_NULL_MX_LIST',true)dnl
define(`confDONT_PROBE_INTERFACES',true)dnl
define(`PROCMAIL_MAILER_PATH',`/usr/bin/procmail')dnl
define(`ALIAS_FILE', `/etc/aliases')dnl
dnl define(`STATUS_FILE', `/etc/mail/statistics')dnl
define(`UUCP_MAILER_MAX', `2000000')dnl
dnl define(`confUSERDB_SPEC', `/etc/mail/userdb.db')dnl
define(`confPRIVACY_FLAGS', `authwarnings,novrfy,noexpn,restrictqrun')dnl
define(`confAUTH_OPTIONS', `A')dnl
TRUST_AUTH_MECH(`DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
define(`confAUTH_MECHANISMS', `DIGEST-MD5 CRAM-MD5 LOGIN PLAIN')dnl
dnl define(`confTO_QUEUEWARN', `4h')dnl
dnl define(`confTO_QUEUERETURN', `5d')dnl
dnl define(`confQUEUE_LA', `12')dnl
dnl define(`confREFUSE_LA', `18')dnl
dnl FEATURE(delay_checks)dnl
MASQUERADE_AS('AziendaInformatica.it')dnl
```

```
FEATURE(`masquerade_enteir_domain')dnl
FEATURE(realy_based_on_MX)dnl
FEATURE('noverify')dnl
FEATURE('noexpn')dnl
FEATURE(`no_default_msa',`dnl')dnl
FEATURE(`smrsh',`/usr/sbin/smrsh')dnl
FEATURE(`mailertable',`hash -o /etc/mail/mailertable.db')dnl
FEATURE(`virtusertable',`hash -o /etc/mail/virtusertable.db')dnl
FEATURE(redirect)dnl
FEATURE(always_add_domain)dnl
FEATURE(use_cw_file)dnl
FEATURE(use_ct_file)dnl
FEATURE(local_procmail,`',`procmail -t -Y -a $h -d $u')dnl
FEATURE(`access_db',`hash -o /etc/mail/access.db')dnl
FEATURE(`dnsbl')dnl
EXPOSED_USER(`root')dnl
MAILER(SMTP)
dnl This changes sendmail to only listen on the loopback device 127.0.0.1
dnl and not on any other network devices. Comment this out if you want
dnl to accept email over the network.
dnl DAEMON_OPTIONS(`Port=smtp,Addr=127.0.0.1, Name=MTA')
dnl NOTE: binding both IPv4 and IPv6 daemon to the same port requires
```

- ***alias***

```
# Alias amministratori
amministratore_azienda:          admin@lifehospital.it
amministratore_salaOperatoria:   jessica.sabbatini@lifehospital.it
amministratore_RM:               daniel.taccucci@lifehospital.it
amministratore_reception:        giada.morosi@lifehospital.it
amministratore_ambulatorio:      giorgia.falo@lifehospital.it
amministratore_garageAmbuanze:   cristian.crispini@lifehospital.it

# Mailing list
admins:  admin@lifehospital.it,  daniel.taccucci@lifehospital.it,  giorgia.falo@lifehospital.it,
         jessica.sabbatini@lifehospital.it,  giada.morosi@lifehospital.it,  cristian.crispini@lifehospital.it
```

8. CONFIGURAZIONE FIREWALL

Abbiamo configurato i firewall sui due router che sono collegati alla DMZ, uno al suo ingresso e uno all'uscita. Come firewall abbiamo scelto iptables, un software Unix che consente una grande configurabilità.

- ***Exterior router***

 # Svuoto le catene

iptables -F FORWARD

iptables -F INPUT

iptables -F OUTPUT

iptables -F PREROUTING

iptables -F POSTROUTING

 # Regola base scarta i pacchetti

iptables -P FORWARD DROP

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -t nat -P PREROUTING DROP

iptables -t nat -P POSTROUTING DROP

 # Accetto le connessioni provenienti dalla DMZ

iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 201.123.7.1 -dport domain -j ACCEPT

 # Connessione al DNS con TCP

iptables -A FORWARD -i eth0 -o eth1 -p udp -s 201.123.7.1 -dport domain -j ACCEPT

 # Connessione al DNS con UDP

iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 201.123.7.2 -dport smtp -j ACCEPT

 # Connessione a Server Mail

iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 201.123.7.3 -dport www -j ACCEPT

 # Connessioni a Server Web

iptables -A FORWARD -i eth0 -o eth1 -p tcp -s 201.123.7.4 -dport www -j ACCEPT

 # Connessioni a Server Proxy

 # Accetta pacchetti di connessioni stabilite o correlate

iptables -A FORWARD -i eth0 -o eth1 -m state –state ESTABLISHED, RELATED -j ACCEPT

 # Evita di rimanere bloccato su porte chiuse

iptables -A FORWARD -i eth0 -o eth1 -p tcp -j REJECT –reject-with tcp-reset

 # Redirige le connessioni provenienti da Internet al giusto server

iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 201.123.7.0 -dport domain -j dnat –to-destination 192.168.7.1

 # Connessione al DNS con TCP

iptables -t nat -A PREROUTING -i eth1 -o eth0 -p udp -d 201.123.7.0 -dport domain -j dnat –to-destination 192.168.7.1

 # Connessione al DNS con UDP

iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 201.123.7.0 -dport smtp -j dnat –to-destination 192.168.7.2

 # Connessione a Server Mail

iptables -t nat -A PREROUTING -i eth1 -o eth0 -p tcp -d 201.123.7.0 -dport www -j dnat –to-destination 192.168.7.3

#Connessioni a Server Web

 # Fa da NAT, cioè fa uscire ogni messaggio dalla DMZ col proprio indirizzo

iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE

- ***Interior Router***

 # Svuoto le catene

iptables -F FORWARD

iptables -F INPUT

iptables -F OUTPUT

iptables -F PREROUTING

iptables -F POSTROUTING

 # Regola base scarta i pacchetti

iptables -P FORWARD DROP

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -t nat -P PREROUTING DROP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.2 -p tcp –dport smtp -j ACCEPT

 # Connessioni al Server Mail in SMTP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.2 -p tcp –dport pop3 -j ACCEPT

 # Connessioni al Server Mail in POP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.2 -p tcp –dport imap -j ACCEPT

 # Connessioni al Server Mail in IMAP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.1 -p tcp --dport domain -j ACCEPT

 # Connessioni al Server DNS con TCP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.1 -p udp –dport domain -j ACCEPT

 # Connessioni al Server DNS con UDP

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.3 -p tcp –dport www -j ACCEPT

 # Connessioni al Server Web

iptables -A FORWARD -i !eth1 -o eth1 -d 192.168.7.4 -p tcp –dport webcache -j ACCEPT

 # Connessioni al Server Proxy

 # Accetta pacchetti di connessioni stabilite o correlate

iptables -A FORWARD -m state –state ESTABLISHED, RELATED -j ACCEPT

 # Evita di rimanere bloccato su porte chiuse

iptables -A FORWARD -p tcp -j REJECT –reject-with tcp-reset

 # Se mi vengono richiesti accessi ad Internet li faccio passare per il Proxy

iptables -t nat -A PREROUTING -i !eth3 -p tcp --dport www -j DNAT --to 192.168.6.4:8080

9. TECNICHE ADOTTATE PER MONITORAGGIO RETE

Per proteggere il server per applicazioni aziendali inseriremo sul server stesso 3 file di hardening (il processo di messa in sicurezza di un sistema attraverso la riduzione della sua superficie di attacco). Più un sistema ha una superficie di attacco grande tante più funzionalità offre; come principio un sistema con una singola funzione è più sicuro di un sistema con molte funzioni. La riduzione dei veicoli di attacco disponibili tipicamente include la rimozione di software non necessario, di username non necessari e la disabilitazione o rimozione di servizi non necessari, così solo gli host autorizzati possono utilizzare il server. Inoltre viene bloccato l'utilizzo del servizio TelNet a tutti gli host della rete, perché:

- **nei daemon Telnet comunemente usati sono state trovate nel corso degli anni molte vulnerabilità.**
- **Telnet non cripta i dati inviati tramite la connessione (nemmeno le password), risulta quindi semplice catturare i dati scambiati.**
- **a Telnet manca uno schema di autenticazione che renda sicura e non intercettabile la comunicazione tra due host.**

 # HOSTS.ALLOW

 # Blocco del servizio telnet a tutti gli host della rete e abilitazione di tutti gli altri servizi

ALL: .lifehospital.it

EXCEPT in.telnetd

 # HOSTS.DENY

 # Si preferisce indicare "ALL: ALL" per una gestione più facile degli accessi.
 # In questo modo vengono bloccati tutti gli accessi non consentiti esplicitamente nel file /etc/hosts.allow.

 # Ogni tentativo di accesso non autorizzato viene registrato in: "access_deny.log"
 # Ciò che stiamo facendo è negare tutti i servizi a tutti i client e loggare i tentati accessi in un file.
 # %c indica di riportare quante più informazioni possibili sul client che ha tentato l'accesso

ALL: ALL: spawn /bin/date %c >> /var/log/access_deny.log

 # /etc/xinetd.conf
 # File principale di configurazione del demone xinetd che definisce le regole di validità generale.

```
defaults {
        instances = 60                  # numero massimo di istanze per ogni servizio
        log_type = SYSLOG authpriv      # tipo di logging
        log_on_success = HOST           # informazioni da inserire nei log
        log_on_failure = HOST           # informazioni da inserire nei log
```

```
        cps = 25 30                    # max connessioni per sec e tempo di attesa
    }
include dir /etc/xinetd.d              # directory per leggere i file di configurazione dei
                                       # singoli servizi
```

10. PREVENTIVO DI SPESA

COMPONENTE	MODELLO	QUANTITA'	PREZZO
Cavo di rete UTP	Cat. 6	2 x 50 m 2 x 100 m	33,50 € al pz. = 67 € 29,34 € al pz. = 58,68 €
Fibra ottica	Cavo Zip Cord 2 Fibre Monomodale	3 Km	1,05 € al m = 3.150 €
Switch 52 porte	Cisco Small Business SG300-52	15	1.196,50 € al pz. = 18.000 €
Router Cisco	Cisco 881 Ethernet Security	5	352 € al pz. = 1.760 €
Firewall	Cisco ASA 5505 Firewall Edition Bundle	1	423,47 €
Router wi-fi	Small Business RV325 - switch a 16 porte integrato	1	371,48 €

TOTALE SPESA

23.830,95 €

Fine