A.D. 1308
unipg
UNIVERSITÀ DEGLI STUDI
DI PERUGIA

Gandalf Sax Corporation

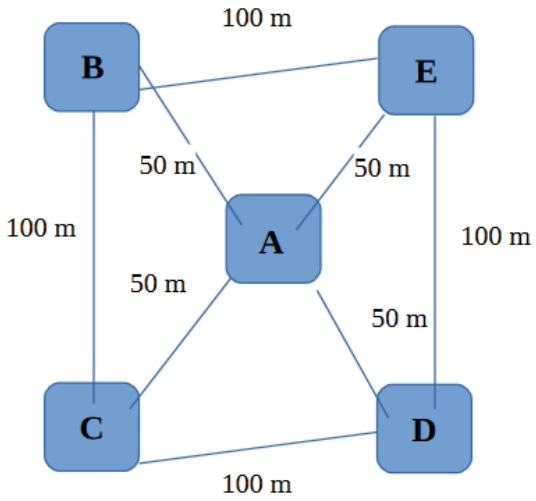
RETI DI CALCOLATORI: PROTOCOLLI | SERGIO TASSO

Filippo Notari | Francesco Brizi
330606 | 350038 | A. A 2023/2024

Sommario

Descrizione del Progetto

La ditta *Gandalf Sax Corporation* ha deciso di collegare in rete tutti i suoi reparti ed uffici e vi ha contattato per disegnare, installare e gestire l'intera rete. Quest'ultima può essere così schematizzata:



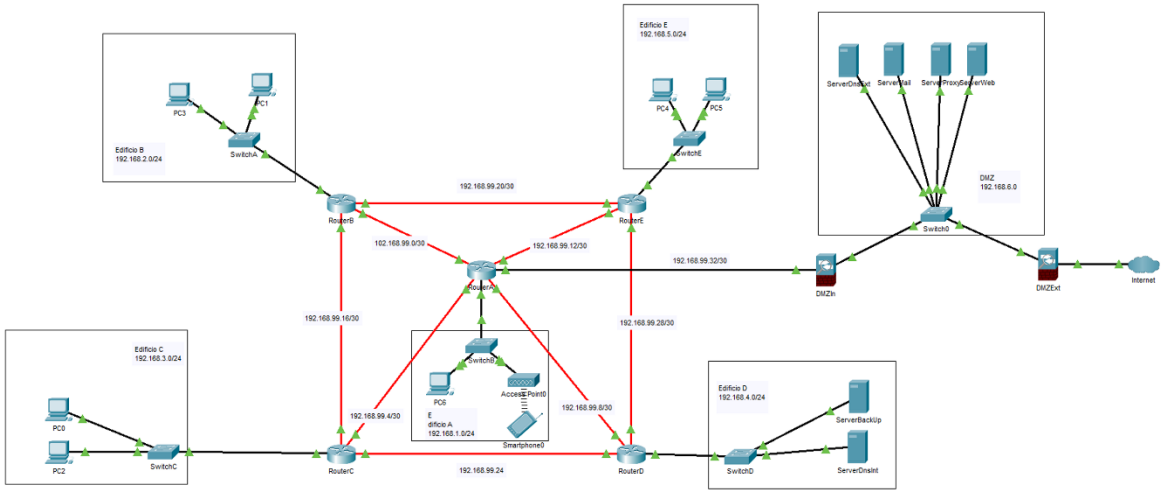
Ed ha le seguenti caratteristiche:

Edificio	*Uffici & Reparti*	*Num. Utenti*	*Num. Server*	*Copertura Wi-Fi*
A		100		SI
B		100		NO
C		100		NO
D		100		NO
E		100		NO

All'interno dell'azienda devono essere presenti i seguenti *Server*:

Server	*Quantità*
MAIL	1
WEB	1
DNS	>=2
PROXY	1
BACKUP	1

Schema fisico della rete



Considerazioni

Lo schema della rete è stato creato in *Cisco Packet Tracer,* che ci ha permesso di creare la nostra rete e testare se le configurazioni erano corrette.

La nostra rete è suddivisa in cinque edifici: A, B, C, D ed E, in una topologia a *maglia parziale*, dove a differenza di una *maglia completa* ogni nodo non è connesso direttamente a ogni altro nodo.

Edifici:

- Edificio A:
  - Contiene un router, tre *switch* per garantire il collegamento di cento utenti e almeno un *access point* per avere una rete wireless
  - Al suo interno è presente anche un'area riservata per la DMZ, progettata per isolare i server che devono essere accessibili da Internet, proteggendo al contempo la rete interna da potenziali minacce esterne.

    - Per isolare la DMZ vengono usati due Firewall, In e Out, e al suo interno sono presenti quattro server: Mail, DNS esterno, Proxy e server Web
- Edificio B:
    - Contiene un router, tre *switch* per garantire il collegamento di cento utenti
- Edificio C:
    - Contiene un router, tre *switch* per garantire il collegamento di cento utenti
- Edificio D:
    - Contiene un router, tre *switch* per garantire il collegamento di cento utenti, un server per gestire i DNS interni e un server per gestire il BACKUP
- Edificio E:
    - Contiene un router, tre *switch* per garantire il collegamento di cento utenti

Cablaggio

- Il collegamento tra i vari router avverrà tramite un cavo in Fibra Ottica Multimodale.
- Ogni router verrà connesso ai relativi switch dell'edificio mediante un cavo STP (Shielded Twisted Pair).
- I DTE si connetteranno agli switch per via di un semplice cavo UTP (Unshielded Twisted Pair).

Schema logico della rete

Classi e indirizzi IP

Abbiamo scelto di usare come classe degli indirizzi IP la classe C.

Quindi la **subnet** usata è 255.255.255.0 che ci permette di ottenere 254 sottoreti, composte da 254 **host**, più che abbastanza dato che a noi servono 6 reti per 100 **host** l'una.

Segue la tabella delle varie sottoreti:

Edificio	Network
Edificio A	192.168.1.0/24
Edificio B	192.168.2.0/24
Edificio C	192.168.3.0/24
Edificio D	192.168.4.0/24
Edificio E	192.168.5.0/24
DMZ	192.168.6.0/24

Router-Router

Per il collegamento fra router abbiamo deciso di utilizzare dei collegamenti punto a punto.

Così abbiamo usato la rete 192.168.99.0, con **subnet** 255.255.255.252.

Questa rete ci permette di ottenere **subnet** con un massimo di 2 **host**.

Segue la tabella delle **subnet** usate:

Router- Router	Network 192.168.99.0/30
B - A	192.168.99.0/30
B - C	192.168.99.16/30
B - E	192.168.99.20/30
C - A	192.168.99.4/30

C - D	192.168.99.24/30
D - A	192.168.99.8/30
D - E	192.168.99.28/30
E - A	192.168.99.12/30
A - DMZIn	192.168.99.32/30

Switch

Per ogni edificio sono utilizzati 3 switch da 40 porte così da avere a disposizione 100 porte per i vari end-user e 20 porte per altre cose, tra cui: il collegamento al router, il collegamento ai server e il collegamento ai firewall.

Router

Per ogni edificio è presente un router il quale avrà:

- L'interfaccia usata per il collegamento con lo switch avrà l'IP X.X.X.1 che sarà usato come default gateway.
- Le altre interfacce sono usate per connettersi con gli altri router.
- Il protocollo di Routing che abbiamo ritenuto più adeguato è RIP_v2

Configurazione interfacce

Per quanto riguarda le interfacce di rete, dobbiamo utilizzare il comando ifconfig che ci permette di specificare i valori che ci interessa impostare: Ip address, subnet mask e broadcast address.

Per la configurazione delle interfacce è stata utilizzato Cisco Packet Tracer.

Edificio A

- **N.HOST**:100
- **SUBNET**: 192.168.1.0/24
- **EDIFICI-COLLEGATI**: Edificio B, Edificio C, Edificio D, Edificio E

Configurazione Host

```
set pcname PCA10
ip 192.168.1.10/24 192.168.1.1
ip dns 192.168.4.2
```

```
set pcname PCWIFI
ip dhcp
```

Configurazione Router

```
Interface GigabitEthernet0/0
    Ip address 192.168.1.1 255.255.255.0
Interface GigabitEthernet0/2
    Ip address 192.168.99.33 255.255.255.252
Interface GigabitEthernet0/0/0
    Ip address 192.168.99.1 255.255.255.252
Interface GigabitEthernet0/1/0
    Ip address 192.168.99.13 255.255.255.252
Interface GigabitEthernet0/2/0
    Ip address 192.168.99.5 255.255.255.252
Interface GigabitEthernet0/3/0
    Ip address 192.168.99.9 255.255.255.252
Router rip
    version 2
    network 192.168.1.0
    network 192.168.99.0
    network 192.168.99.4
    network 192.168.99.8
    network 192.168.99.12
    network 192.168.99.32
end
Service dhcp
    Ip dhcp exclude-address 192.168.1.1 192.168.1.102
    Ip dhcp pool reteA
    Network 192.168.1.0 255.255.255.0
    Default-router 192.168.1.1
    Dns-server 192.168.4.2
    Lease 2
exit

ip domain-lookup
ip name-server 192.168.4.2
```

Edificio B

- **N.HOST**:100
- **SUBNET**: 192.168.2.0/24
- **EDIFICI-COLLEGATI**: Edificio A, Edificio C, Edificio E

Configurazione Host

```
set pcname PCB10
ip 192.168.2.10/24 192.168.2.1
ip dns 192.168.4.2
```

Configurazione Router

```
Interface GigabitEthernet0/0
        Ip address 192.168.2.1 255.255.255.0
Interface GigabitEthernet0/0/0
        Ip address 192.168.99.2 255.255.255.252
Interface GigabitEthernet0/1/0
        Ip address 192.168.99.21 255.255.255.252
Interface GigabitEthernet0/2/0
        Ip address 192.168.99.17 255.255.255.252
Router rip
        version 2
        network 192.168.2.0
        network 192.168.99.0
        network 192.168.99.16
        network 192.168.99.20
end

ip domain-lookup
ip name-server 192.168.4.2
```

Edificio C

- **N.HOST**:100
- **SUBNET**: 192.168.3.0/24
- **EDIFICI-COLLEGATI**: Edificio A, Edificio B, Edificio D

Configurazione Host

```
set pcname PCC10
ip 192.168.3.10 192.168.3.1/24
```

ip dns 192.168.4.2

Configurazione Router

Interface GigabitEthernet0/0
Ip address 192.168.3.1 255.255.255.0
Interface GigabitEthernet0/0/0
Ip address 192.168.99.18 255.255.255.252
Interface GigabitEthernet0/1/0
Ip address 192.168.99.6 255.255.255.252
Interface GigabitEthernet0/2/0
Ip address 192.168.99.25 255.255.255.252
Router rip
version 2
network 192.168.3.0
network 192.168.99.4
network 192.168.99.16
network 192.168.99.24
end

ip domain-lookup
ip name-server 192.168.4.2

Edificio D

- **N.HOST**:100
- **SUBNET**: 192.168.4.0/24
- **EDIFICI-COLLEGATI**: Edificio A, Edificio C, Edificio E

Codice	Tipo Dispositivo	Indirizzo Ip
PCD1	host	192.168.4.4
	…	
PCD100	host	192.168.4.104
DNS	Server	192.168.4.2
Backup	Server	192.168.4.3

Configurazione Host

set pcname PCD10
ip 192.168.4.10/24 192.168.4.1
ip dns 192.168.4.2

Configurazione Router

```
Interface GigabitEthernet0/0
    Ip address 192.168.4.1 255.255.255.0
Interface GigabitEthernet0/0/0
    Ip address 192.168.99.10 255.255.255.252
Interface GigabitEthernet0/1/0
    Ip address 192.168.99.26 255.255.255.252
Interface GigabitEthernet0/2/0
    Ip address 192.168.99.29 255.255.255.252
Router rip
    version 2
    network 192.168.4.0
    network 192.168.99.8
    network 192.168.99.24
    network 192.168.99.28
end

ip domain-lookup
ip name-server 192.168.4.2
```

Edificio E

- **N.HOST**:100
- **SUBNET**: 192.168.5.0/24
- **EDIFICI-COLLEGATI**: Edificio A, Edificio B, Edificio D

Configurazione Host

```
set pcname PCE10
ip 192.168.5.10/24 192.168.5.1
ip dns 192.168.4.2
```

Configurazione Router

```
Interface GigabitEthernet0/0
    Ip address 192.168.5.1 255.255.255.0
Interface GigabitEthernet0/0/0
    Ip address 192.168.99.30 255.255.255.252
Interface GigabitEthernet0/1/0
    Ip address 192.168.99.22 255.255.255.252
Interface GigabitEthernet0/2/0
```

```
        Ip address 192.168.99.14 255.255.255.252
    Router rip
        version 2
        network 192.168.5.0
        network 192.168.99.12
        network 192.168.99.20
        network 192.168.99.28
    end

    ip domain-lookup
    ip name-server 192.168.4.2
```

Edificio A-DMZ

- **N.HOST**:4
- **SUBNET**: 192.168.6.0/24
- **EDIFICI-COLLEGATI**: Firewall In, Firewall, Out

Codice	Tipo Dispositivo	Indirizzo Ip
DNS	server	192.168.6.3
Mail	server	192.168.6.4
Proxy	Server	192.168.6.5
Web	server	192.168.4.6
Firewall Out	Router-firewall	192.168.6.1
Firewall In	Router-Firewall	192.168.6.2

Configurazione DNS

```
set pcname DNS
ip 192.168.6.3/24 192.168.6.1
```

Configurazione MAIL

```
set pcname DNS
ip 192.168.6.4/24 192.168.6.1
ip dns 192.168.6.3
```

Configurazione PROXY

```
set pcname DNS
ip 192.168.6.5/24 192.168.6.1
ip dns 192.168.6.3
```

Configurazione PROXY

set pcname www
ip 192.168.6.6/24 192.168.6.1
ip dns 192.168.6.3

Firewall In

Interface GigabitEthernet0/0
    Ip address 192.168.6.2 255.255.255.0
Interface GigabitEthernet1/0
    Ip address 192.168.99.34 255.255.255.252
Router rip
    Version 2
    Network 192.168.6.0
    Network 192.168.99.32
End
Ip domain-lookup
Ip name-server 192.168.4.2

Firewall Out

Interface GigabitEthernet0/0
    Ip address 192.168.6.1 255.255.255.0
Interface GigabitEthernet1/0
    Ip address dhcp
Router rip
    Version 2
    Network 192.168.6.0
    Network 0.0.0.0
    Default-information originate
End
Ip domain-lookup
Ip name-server 192.168.6.3

Configurazione DNS e Posta

DNS Interno

/etc/resolv.conf

domain gandafsaxcorporation.it
search gandafsaxcorporation.it

```
# DNS Interno
nameserver 192.168.4.2
# DNS DMZ
nameserver 192.168.6.3
# Cloudflare DNS
nameserver 1.1.1.1
nameserver 8.8.8.8
```

/etc/named.conf

```
// Master
// DNS2 è master per la rete D
zone "reted. gandafsaxcorporation.it" {
        type master;
        file "/etc/bind/reted. gandafsaxcorporation.it.db";
};
zone "4.168.192.in-addr.arpa
" {
type master;
file "/etc/bind/4.168.192.in-addr.arpa.db";
};
// Slave
zone " gandafsaxcorporation.it" {
        type slave;
        file "/etc/bind/ gandafsaxcorporation.it.bk";
        masters { 192.168.6.3; };
};
zone "168.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/168.192.in-addr.arpa.bk";
        masters { 192.168.6.3; };
};
// DMZ
zone "dmz. gandafsaxcorporation.it" {
        type slave;
        file "/etc/bind/dmz.gandalfsaxcorporation.it.bk";
        masters { 192.168.6.3; };
};
zone "5.168.192.in-addr.arpa" {
```

```
        type slave;
        file "/etc/bind/5.168.192.in-addr.arpa.bk";
        masters { 192.168.6.3; };
};
```

/etc/named.conf.options

```
acl "trusted-nameservers" {
        localhost;
        192.168.4.2;
        192.168.6.3;
};
acl "trusted-networks" {
        localhost;
        192.168.1.0/24;
        192.168.2.0/24;
        192.168.3.0/24;
        192.166.4.0/24;
        192.168.5.0/24;
        192.168.6.0/24;
};
options {
        directory "/var/cache/bind";
        dnssec-validation auto;
        auth-nxdomain no;
        version "Not disclosed";
        notify yes;
        allow-transfer { trusted-nameservers; };
        allow-query { trusted-networks; };
        forwarders { 1.1.1.1; };
        recursion yes;
};
```

File di zona per reted.gandalfsaxcorporation.it

```
$TTL 86400
$ORIGIN reted.gandalfsaxcorporation.it.
@ IN SOA dns.reted. gandalfsaxcorporation.it. root.reted.
gandalfsaxcorporation.it. (
        2024021401; serial
```

```
        43200 ; refresh
        3600 ; retry after 1 hour
        3600000 ; expire after 1000 hours
        2592000 ; default ttl
    )
    ; Definizione dei nameserver e dei server mail
    IN NS dns.dmz. gandalfsaxcorporation.it.
    IN NS dns.reted. gandalfsaxcorporation.it.
    IN NS dns.cloudflare.com.
    IN MX 10 mail. gandalfsaxcorporation.it.
    ; Host di Rete D
    RE IN A 192.168.4.1
    dns IN A 192.168.4.2
    backup IN A 192.168.4.3
```

DNS Esterno

/etc/resolv.conf

```
domain gandalfsaxcorporation.it
search gandalfsaxcorporation.it
nameserver 192.168.6.3
nameserver 192.169.4.2
nameserver 1.1.1.1
nameserver 1.0.0.1
```

/etc/named.conf

```
// Master
zone "gandalfsaxcorporation.it" {
        type master;
        file "/etc/bind/ gandalfsaxcorporation.it.db";
};
zone "168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/168.192.in-adr.arpa.db";
};
// DMZ
zone "dmz.gandalfsaxcorporation.it" {
        type master;
        file "/etc/bind/dmz. gandalfsaxcorporation.it.db";
```

```
};
zone "5.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/5.168.192.in-addr.arpa.db";
};
// Slave
zone "reted.gandalfsaxcorporation.it" {
        type slave;
        file "/etc/bind/reted. gandalfsaxcorporation.it.bk";
        masters { 192.168.4.2; };
};
zone "4.168.192.in-addr.arpa" {
        type slave;
        file "/etc/bind/1.168.192.in-addr.arpa.bk";
        masters { 192.168.4.2; };
};
```

/etc/named.conf.options

```
acl "trusted-nameservers" {
        localhost;
        192.168.6.3;
        192.169.4.2;
};
acl "trusted-networks" {
        localhost;
        192.168.1.0/24;
        192.168.2.0/24;
        192.168.3.0/24;
        192.168.4.0/24;
        192.168.5.0/24;
        192.168.6.0/24;
        };
options {
        directory "/var/cache/bind";
        dnssec-validation auto;
        auth-nxdomain no;
        version "Not disclosed";
        notify yes;
```

```
        allow-transfer { trusted-nameservers; };
        allow-query { "any"; };
        forwarders { 1.1.1.1; };
        recursion yes;
        allow-recursion {any;};
};
```

File di zona per dmz.gandalfsaxcorporation.it

```
$TTL 86400

$ORIGIN dmz. gandalfsaxcorporation.it.

@ IN SOA dns.dmz. gandalfsaxcorporation.it.root.dmz.
gandalfsaxcorporation.it. (

        2024021401; serial

        43200 ; refresh

        3600 ; retry after 1 hour

        3600000 ; expire after 1000 hours

        2592000 ; default ttl

)

; Definizione dei nameserver e dei server mail

IN NS dns.dmz. gandalfsaxcorporation.it.

IN NS dns.reted. gandalfsaxcorporation.it.

IN NS dns.cloudflare.com.

IN MX 10 mail.dmz. gandalfsaxcorporation.it.

; Host della DMZ

rdmz IN A 192.168.6.1

dns IN A 192.168.5.3

www IN A 192.168.5.6

mail IN A 192.168.5.4

proxy IN A 192.168.5.5
```

File di zona per 168.192.in-addr.arpa

```
$TTL 86400

$ORIGIN 168.192.in-addr.arpa.

@ IN SOA dns.gandalfsaxcorporation.it. root.dmz.gandalfsaxcorporation.it. (
        2024021401; serial
        43200 ; refresh
        3600 ; retry after 1 hour
        3600000 ; expire after 1000 hours
        2592000 ; default ttl
)
; Definizione dei nameserver e dei server mail
IN NS dns. gandalfsaxcorporation.it.
IN NS dns.cloudflare.com.
IN MX 10 mail. gandalfsaxcorporation.it.
; Sottodomini
0.5 IN PTR dmz. gandalfsaxcorporation.it.
0.4 IN PTR reted. gandalfsaxcorporation.it.
; Host
253.5 IN PTR mail. gandalfsaxcorporation.it.
252.5 IN PTR dns. gandalfsaxcorporation.it.
254.5 IN PTR www. gandalfsaxcorporation.it.
```

File di zona per 5.168.192.in-addr.arpa

```
$TTL 86400

$ORIGIN 5.168.192.in-addr.arpa.

@ IN SOA dns.dmz. gandalfsaxcorporation.it. root.dmz.
gandalfsaxcorporation.it. (
        2024021401 ; serial
```

```
        43200 ; refresh
        3600 ; retry after 1 hour
        3600000 ; expire after 1000 hours
        2592000 ; default ttl
)
; Definizione dei nameserver e dei server mail
IN NS dns.dmz. gandalfsaxcorporation.it.
IN NS dns.reted. gandalfsaxcorporation.it.
IN NS dns.cloudflare.com.
IN MX 10 mail.dmz. gandalfsaxcorporation.it.
; Host
1 IN PTR rdmz.dmz. gandalfsaxcorporation.it.
253 IN PTR mail.dmz. gandalfsaxcorporation.it.
252 IN PTR dns.dmz. gandalfsaxcorporation.it.
254 IN PTR www.dmz. gandalfsaxcorporation.it.
```

File di zona per gandalfsaxcorporation.it

```
$TTL 86400
$ORIGIN gandalfsaxcorporation.it.
@ IN SOA dns.gandalfsaxcorporation.it. root. gandalfsaxcorporation.it. (
        2024021401 ; serial
        43200 ; refresh
        3600 ; retry after 1 hour
        3600000 ; expire after 1000 hours
        2592000 ; default ttl
)
; Definizione dei nameserver e dei server mail
```

IN NS dns. gandalfsaxcorporation.it.

IN NS dns.cloudflare.com.

IN MX 10 mail. gandalfsaxcorporation.it.

; Sottodomini

;dmz IN A 198.168.6.0

;reted IN A 198.168.4.0

; Host

mail IN A 198.168.6.4

dns IN A 198.168.6.3

IN A 192.168.5.254

www IN CNAME

Server MAIL

Creazione utenti

useradd --create-home -s /sbin/nologin elraton; passwd pass1
useradd --create-home -s /sbin/nologin breezee; passwd pass2

/etc/mail/local-host-names

localhost
mail.gandalfsaxcorporation.it
gandalfsaxcorporation.it
dmz. gandalfsaxcorporation.it
reted. gandalfsaxcorporation.it

/etc/mail/sendmail.mc

DAEMON_OPTIONS(`Family=inet, Name=MTA-v4, Port=smtp')dnl
Dopo l'ultimo include del file aggiungiamo
FEATURE(`relay_entire_domain')dnl #Sendmail consente al server di inoltrare le e-mail per l'intero dominio.

/etc/mail/virtusertable

elraton @ gandalfsaxcorporation.it elraton
breezee @ gandalfsaxcorporation.it breezee
postmaster@ gandalfsaxcorporation.it postmaster

admin@ gandalfsaxcorporation.it admin
dmz@ gandalfsaxcorporation.it dmz
reted@ gandalfsaxcorporation.it reted

/etc/mail/aliases

postmaster: elraton
admin: elraton, breezee
dmz: admin
reted: breezee
Aliases per gli utenti, in modo che possano ricevere una mail sotto diversi nomi

/etc/mail/access

Connect:192.168
GreetPause:192.168
ClientRate:192.168
ClientConn:192.168
emailto@reject REJECT
gandalfsaxcorporation.it RELAY
192.168 RELAY
la riga "192.168 RELAY" nel file /etc/mail/access indica che tutti gli host all'interno della rete locale con indirizzi IP che iniziano con "192.168" sono autorizzati a utilizzare il server Sendmail come relay per inviare e-mail

Configurazione Firewall

Per la configurazione del firewall, abbiamo ritenuto che la filosofia migliore da applicare fosse quella del **default deny**. Questo approccio implica che tutto ciò che non è espressamente permesso è proibito. Adottando questa filosofia, si limita notevolmente l'attività degli utenti, rendendo più difficile la violazione delle politiche di sicurezza.

CONFIGURAZIONE FIREWALL IN

```
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT

iptables -P FORWARD DROP
```

```
iptables -P INPUT DROP
iptables -P OUTPUT DROP

# DNS
iptables -A FORWARD -p udp -d 192.168.6.3 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.3 --dport 53 -j ACCEPT
# MAIL
iptables -A FORWARD -p tcp -d 192.168.6.4 --dport 25 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.4 --dport 110 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.4  --dport 143 -m limit 100/s -j
ACCEPT
# HTTP
iptables -A FORWARD -p tcp -d 192.168.5.6 --dport 80 -m limit 100/s -j
ACCEPT
iptables -A FORWARD -p tcp -d 192.168.5.5 --dport 443 -m limit 100/s -j
ACCEPT

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

CONFIGURAZIONE FIREWALL OUT

```
iptables -F FORWARD
iptables -F INPUT
iptables -F OUTPUT

iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
# DNS, Mail, Proxy, Web:
iptables -A FORWARD -p tcp -d 192.168.6.4 --dport 25 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.4 --dport 110 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.4 --dport 143 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.3 --dport 53 -j ACCEPT
iptables -A FORWARD -p udp -d 192.168.6.3 --dport 53 -j ACCEPT
iptables -A FORWARD -p tcp -d 192.168.6.5 --dport 443 -j ACCEPT
```

```
iptables -A FORWARD -p tcp -d 192.168.6.6 --dport 80 -j ACCEPT

iptables -A FORWARD -m state --state ESTABLISHED, RELATED -j ACCEPT
iptables -A FORWARD -p tcp -j REJECT --reject-with tcp-reset


# NAT
iptables -t NAT -A PREROUTING -p tcp --dport 25 -j DNAT --to-destination
198.168.6.4
iptables -t NAT -A PREROUTING -p udp --dport 53 -j DNAT --to-
destination 198.168.5.3
iptables -t NAT -A PREROUTING -p tcp --dport 53 -j DNAT --to-destination
198.168.6.3
iptables -t NAT -A PREROUTING -p tcp --dport 443 -j DNAT --to-
destination 198.168.6.5
iptables -t NAT -A POSTROUTING -o eth1 -j MASQUERADE
```

Tecniche monitoraggio della rete

Per il monitoraggio dell'intera rete utilizzeremo il seguente software: **NAGIOS**.

Nagios è un'applicazione open source per il monitoraggio di computer e risorse di rete. La sua funzione base è quella di controllare nodi, reti e servizi specificati, avvertendo con degli *alert* quando questi non garantiscono il loro servizio o quando ritornano attivi.

Alcune delle funzionalità sono:

- monitoraggio di servizi di rete (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH);
- monitoraggio delle risorse di sistema;
- monitoraggio remoto supportato attraverso tunnel SSH o SSL;
- semplici plugin che permettono agli utenti di sviluppare facilmente nuovi controlli per i servizi in base alle proprie esigenze, usando Bash, C++, Perl, Ruby, Python, PHP, C#, ecc.;
- controlli paralleli sui servizi;
- capacità di definire gerarchie di nodi di rete usando nodi "*parent*", permettendo la distinzione tra nodi che sono down e nodi non raggiungibili;

- notifiche quando l'applicazione riscontra problemi o la loro risoluzione
- capacità di definire "event handler", ovvero azioni automatiche che vengono attivate all'apparire o alla risoluzione di un problema;
- rotazione automatica dei file di log;
- interfaccia web opzionale per la visualizzazione dell'attuale stato, notifiche, storico dei problemi, file di log, ecc.

Protezione BACKUP

Il server di Backup verrà posto, in una stanza apposita con un elevato sistema di sicurezza e di protezione. In questa stanza potranno accedervi solo gli utenti autorizzati: l'amministratore del sistema e i pochi tecnici incaricati della manutenzione.

Sarà dotata di un sistema antincendio all'avanguardia, di un sistema di refrigerazione consono per mantenere una temperatura ideale evitando surriscaldamenti che potrebbero inficiare sulle prestazioni e sull'integrità del server, un sistema di sorveglianza e di un allarme antintrusione.

Quando un Hard Disk presenterà segni di malfunzionamento, il tecnico incaricato si preoccuperà di sostituirlo per poi smagnetizzarlo e distruggerlo tramite l'apposita macchina.

Preventivo

Componente	Quantità	Prezzo Unitario	Prezzo Totale
Cavo Fibra Ottica Multimodale	1.000 m	€ 2,50/m	€ 2.500
Cavo STP	500 m	€ 1/m	€ 500
Cavo UTP	200 m	€ 0,50/m	€ 100
Router	5	€ 120/pz	€ 600
Switch	20	€ 250/pz	€ 5.000
Access Point	1	€ 90/pz	€ 90
Firewall	2	€ 800/pz	€ 1.600
		Tot:	€ 10.390