La sicurezza dei dati in ambiente clinico: l'esperienza dell'Istituto di Fisiologia Clinica

Raffaele Conte
13.11.2003

Dimensioni della rete dati in IFC

- 5 reti locali
- 2 router di frontiera
- oltre 20 server
- circa 1000 indirizzi registrati
- oltre 530 utenti

Estensione della rete dati in IFC

distribuita sulle sedi di:

- ☑ Pisa (area CNR e V. Trieste)
- ☑ Massa (Ospedale “Pasquinucci”)
- ☑ Lecce
- ☑ Roma *(solo servizi)*

I servizi di rete in IFC *1/2*

- ☑ DNS
- ☑ Posta elettronica
  - POP/IMAP/SMTP
  - Webmail
  - Sistemi di filtraggio Antivirus/Antispam
  - Mailing list
- ☑ Web Server
  - Pubblico
  - Clinico
    - per uso interno
    - per servizi forniti a terzi *(Grosseto, Castelnuovo Garf., Firenze, Lucca)*

I servizi di rete in IFC *2/2*

- FTP
- NTP
- DataBase Clinico

  (nel 2002: 3805 ricoveri, 45358 accessi agli ambulatori)
- File Sharing *(Ambulatori)*
- LDAP *(autenticazione centralizzata)*
- Proxy Web

Problematiche di una rete particolare

- Conciliare la “libertà” tipica di un ambiente di ricerca con la necessità di riservatezza dei dati sensibili
- Ridotta disponibilità di risorse economiche

Sicurezza in un sistema informativo

Secondo la definizione ISO la sicurezza di un sistema informativo è l'insieme delle misure atte a garantire

- ☑ la disponibilità,
- ☑ l'integrità,
- ☑ la riservatezza,

delle informazioni gestite.

Tutte caratteristiche critiche in IFC!!

Obiettivo della sicurezza

- ☑ Ridurre al minimo le possibilità di compromissione del sistema informativo
- ☑ Essere preparati a ripristinare il servizio in tempi rapidi *(disaster recovery)*

L'approccio al problema *1/2*

Individuare le risorse da proteggere e gli eventi indesiderati

- Per ogni cella della matrice è possibile individuare almeno una vulnerabilità

- La riservatezza non DEVE dipendere da possibili eventi accidentali!!

	Eventi accidentali		Eventi dolosi	
	Fisici	Logici	Fisici	Logici
Disponibilità	x	x	x	x
Integrità	x	x	x	x
Riservatezza	!	!	x	x

L'approccio al problema 2/2

	Eventi accidentali		Eventi dolosi	
	Fisici	Logici	Fisici	Logici
Disponibilità	1	2	3	4
Integrità	1	2	3	4
Riservatezza	!	!	3	4

1. *Fallimenti hardware, interruzione dei sistemi di alimentazione o condizionamento, disastri*
2. *Errori umani*
3. *Furti o danneggiamenti di strumenti o supporti di memorizzazione*
4. *Intrusioni, intercettazioni (sniffing), attacchi di disturbo (virus, worm, Denial of Service)*

Prime soluzioni adottate

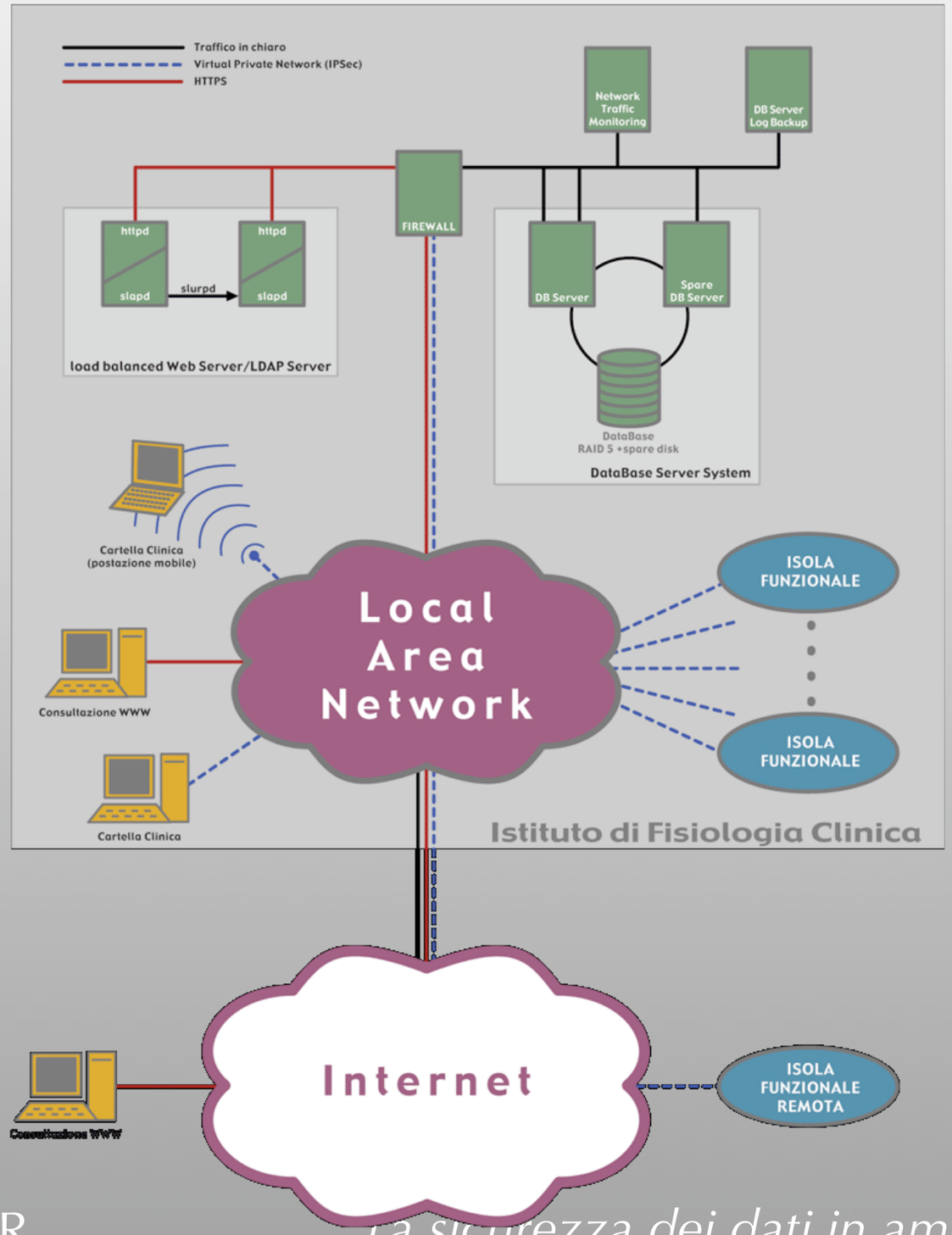
Sicurezza fisica

- ☑ ups su “linea rossa”
- ☑ siti ad accesso limitato
- ☑ sistemi duplicati in siti distanti e su linee elettriche diverse
- ☑ sist. di condizionamento aggiuntivi
- ☑ backup su nastro
- ☑ ridondanza hw (macchine di backup, RAID ecc.)

Sicurezza logica

- ☑ fw “a ridosso” delle macchine critiche
- ☑ tunneling ssl / https
- ☑ vpn

Architettura del sistema ARCA



Attività in corso

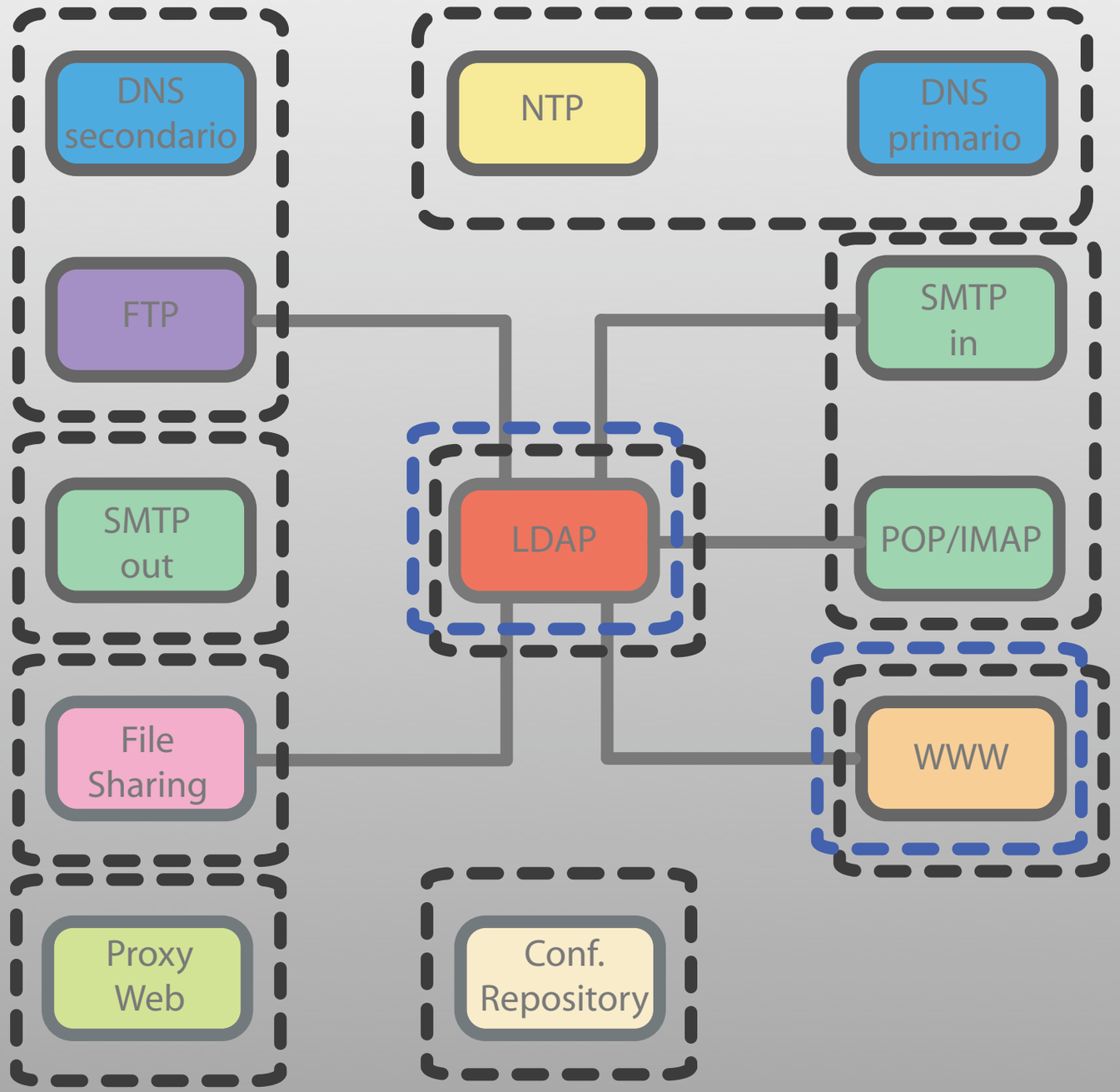
- ☑ riorganizzazione dei servizi di rete
- ☑ separazione del traffico VLAN
- ☑ sistemi di monitoraggio
- ☑ sistemi per autenticazione centralizzata e gestione dei diritti di accesso
- ☑ firma digitale

Riorganizzazione dei servizi di rete

- problema: minimizzare l'interruzione del servizio
- ☑ soluzione: servizi distribuiti su piccole numerose macchine
  - problema: aggiornamento dei sistemi e delle configurazioni
  - ☑ soluzione: sistema di repository con distribuzione automatica del sistema e delle configurazioni *(rdist, RH kickstart)*

Riorganizzazione dei servizi di rete

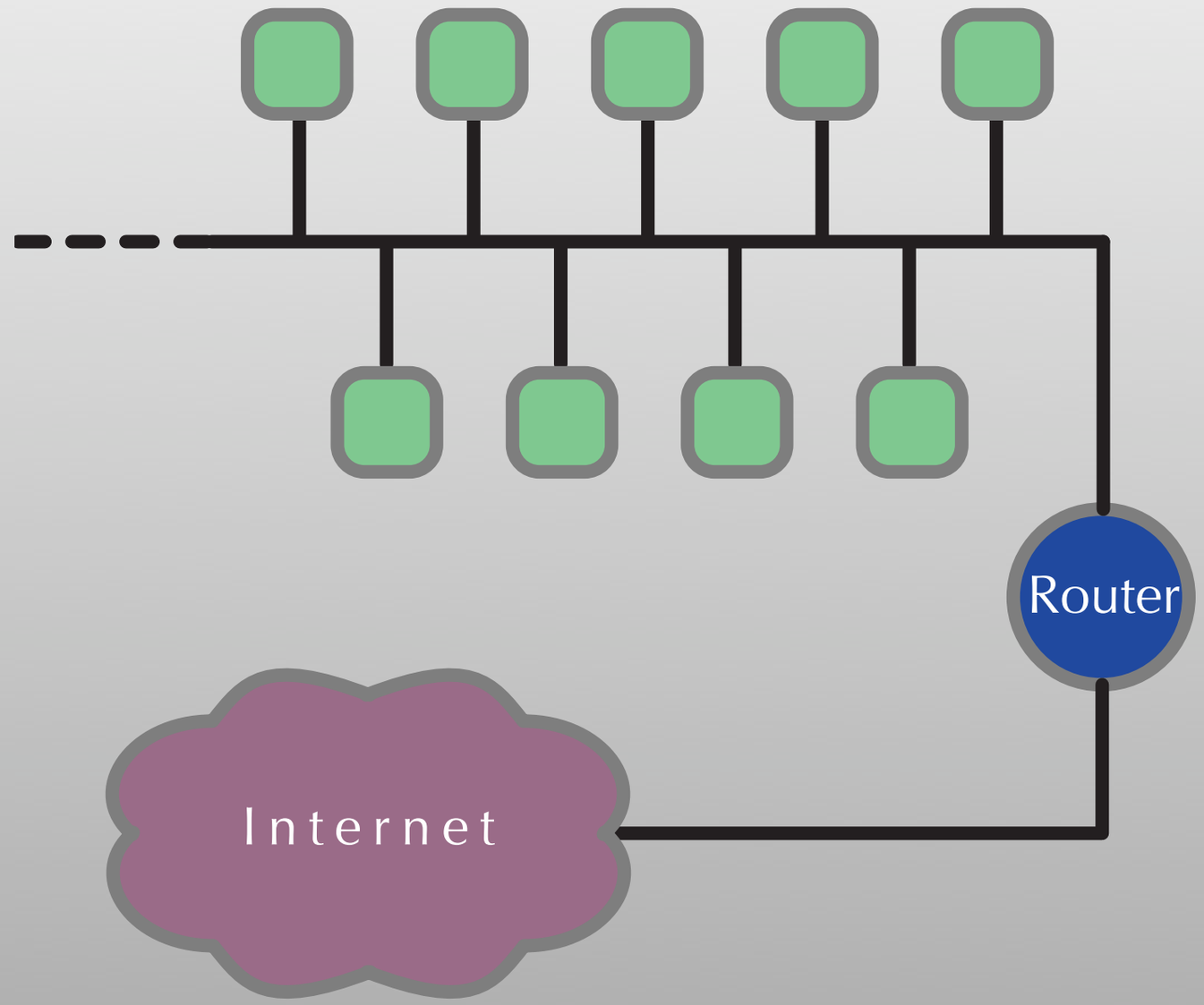
Distribuzione dei servizi sulle macchine



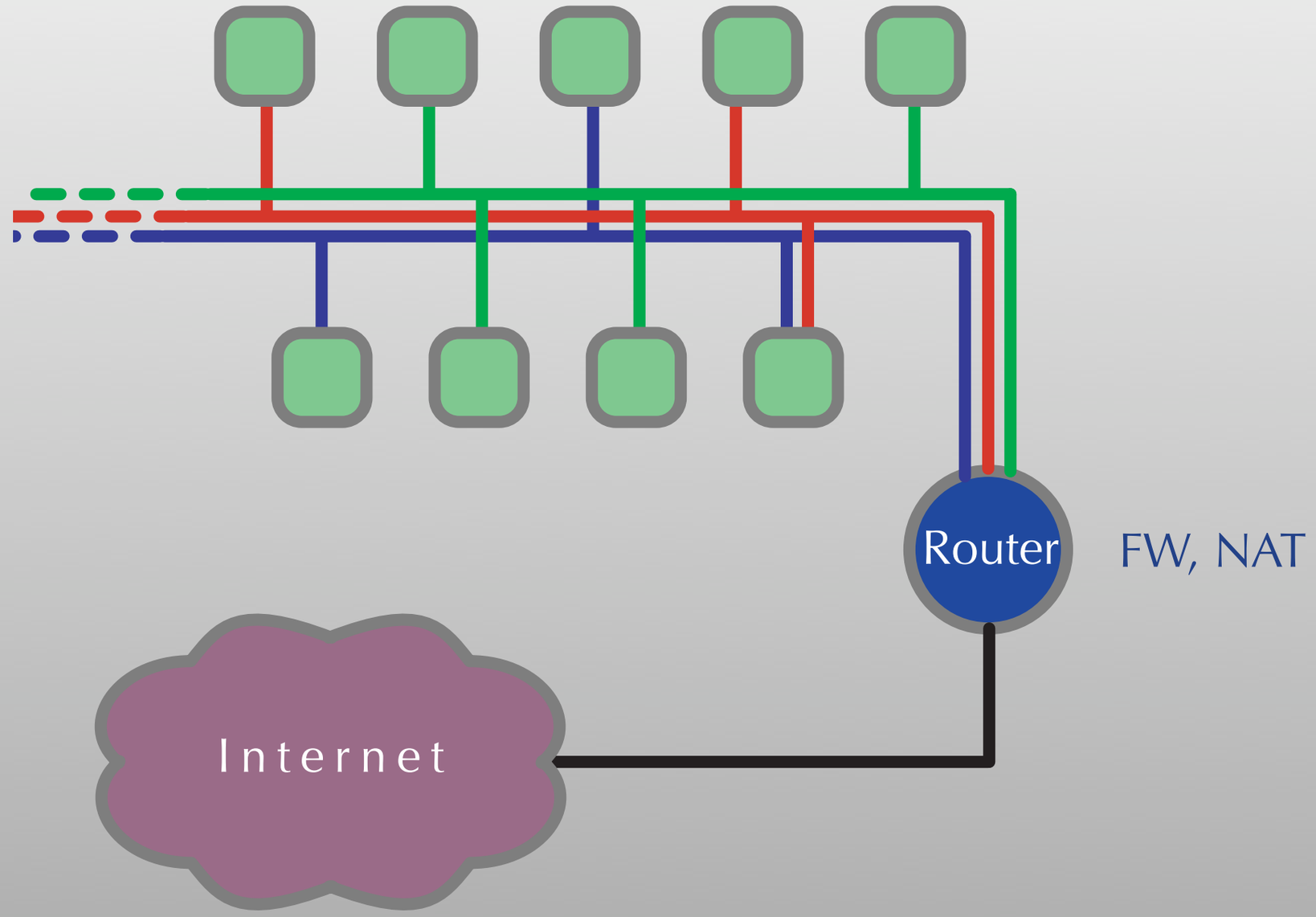
Separazione del traffico

- problema: separare il traffico di “ricerca”, dal traffico “clinico”, “ospiti”, “management”
- soluzione: VLAN (IEEE 802.1Q)

Sezionamento della rete: VLAN



Sezionamento della rete: VLAN



Monitoraggio del sistema

- ☐ problema: rallentamenti accesso ai servizi
- ☑ soluzione: monitoraggio costante di rete e server con strumenti di analisi dei log e generazione di report grafici e alert
  - tripwire
  - Nagios
  - sFlow (RFC 3176) / nTop
  - SNORT
  - Nessus

Autenticazione e Autorizzazione 1/2

- problema:
  - debolezza password
  - estrema variabilità del personale
  - assunzione di responsabilità

Autenticazione e Autorizzazione 2/2

- ☑ soluz:
  - LDAP (RFC 1777, RFC 2251)
    - inserimento e rimozione gestito dall'ufficio personale con gestione del "modulo di responsabilità"
    - autorizzazioni gestite dai responsabili dei servizi in funzione di particolari attributi (es. reparto, titolo ecc.) o mediante l'inclusione o l'esclusione da un gruppo
  - strong authentication

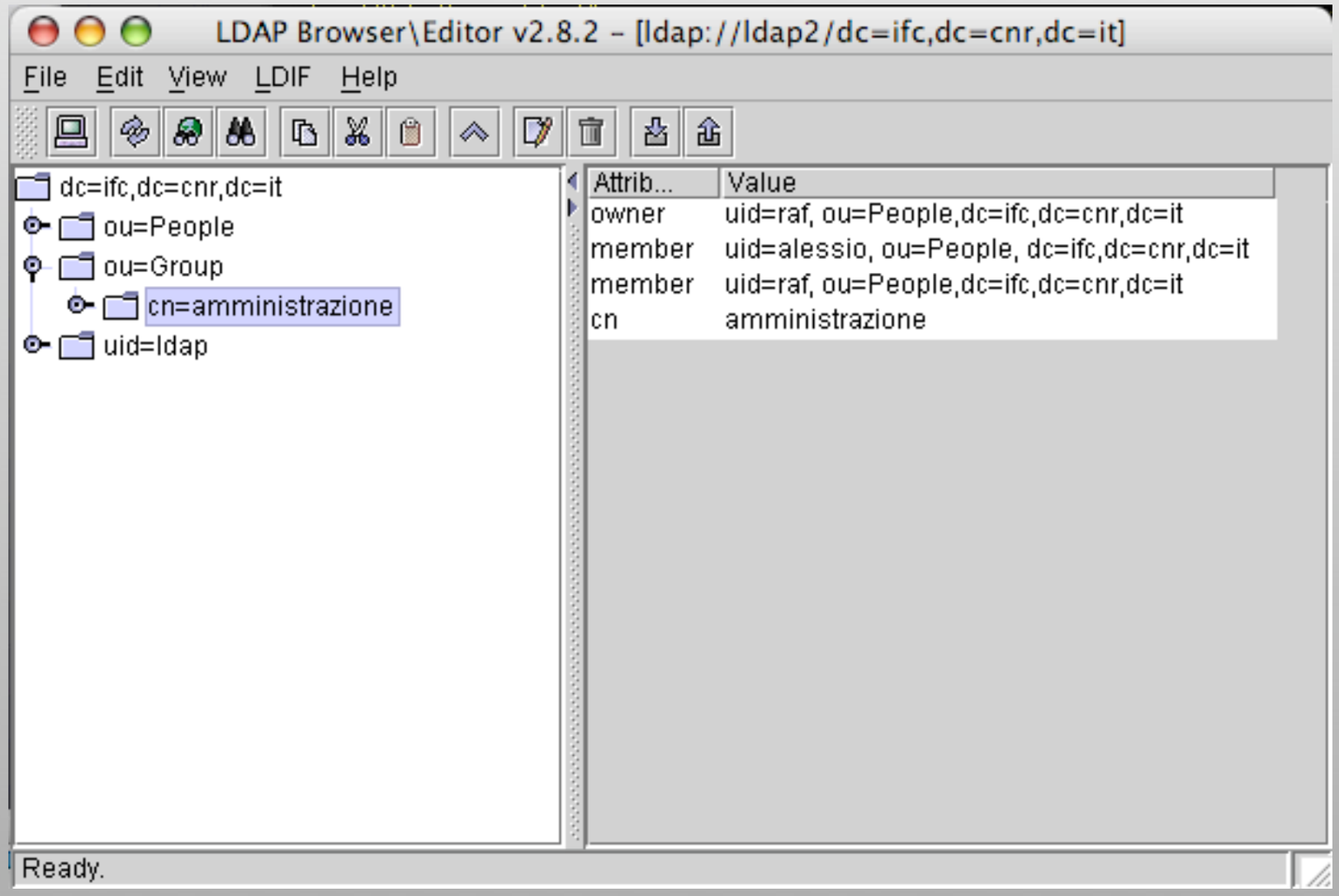
LDAP: esempio di configurazione 1/2

```
#######    Accesso all'attributo password
access to dn.children="ou=People,dc=ifc,dc=cnr,dc=it" attrs=userPassword
        by self write
        by group.exact="cn=amministrazione,ou=Group,dc=ifc,dc=cnr,dc=it" write
        by anonymous auth

#######    Accesso agli attributi modificabili dall'utente stesso e visibili
#######    da tutti (anonymous), solo dalla rete di IFC
access to dn.children="ou=People,dc=ifc,dc=cnr,dc=it"
                attrs=roomNumber,telephoneNumber,mail,jpegPhoto,facsimileTelephoneNumber
        by group.exact="cn=amministrazione,ou=Group,dc=ifc,dc=cnr,dc=it" write
        by self write
        by peername=146.48.(68|69|70|71).* read
        by domain=".*\.ifc\.cnr\.it\." read


                                #######    Gestione dei gruppi  ou=GROUP
                                access to dn="cn=amministrazione,ou=Group,dc=ifc,dc=cnr,dc=it"
                                        attrs=entry,member,owner,cn,businessCategory,description
                                    by peername=146.48.68.41 compare
                                    by dnattr=owner write
                                    by dnattr=member read
```

LDAP: esempio di configurazione 2/2



Firma digitale

- problema: garantire l'autenticità e la non ripudiabilità dei dati archiviati allo scopo di dare validità legale ai processi e documenti informatici *(cartelle cliniche, referti ecc.)*
- soluzione: firma digitale

  è necessario avere uno strumento sufficientemente sicuro da poter essere integrato nelle procedure in uso senza appesantirle

Riferimenti

- tripwire.org
- nagios.org
- sflow.org
- www.snort.org
- nessus.org
- openldap.org