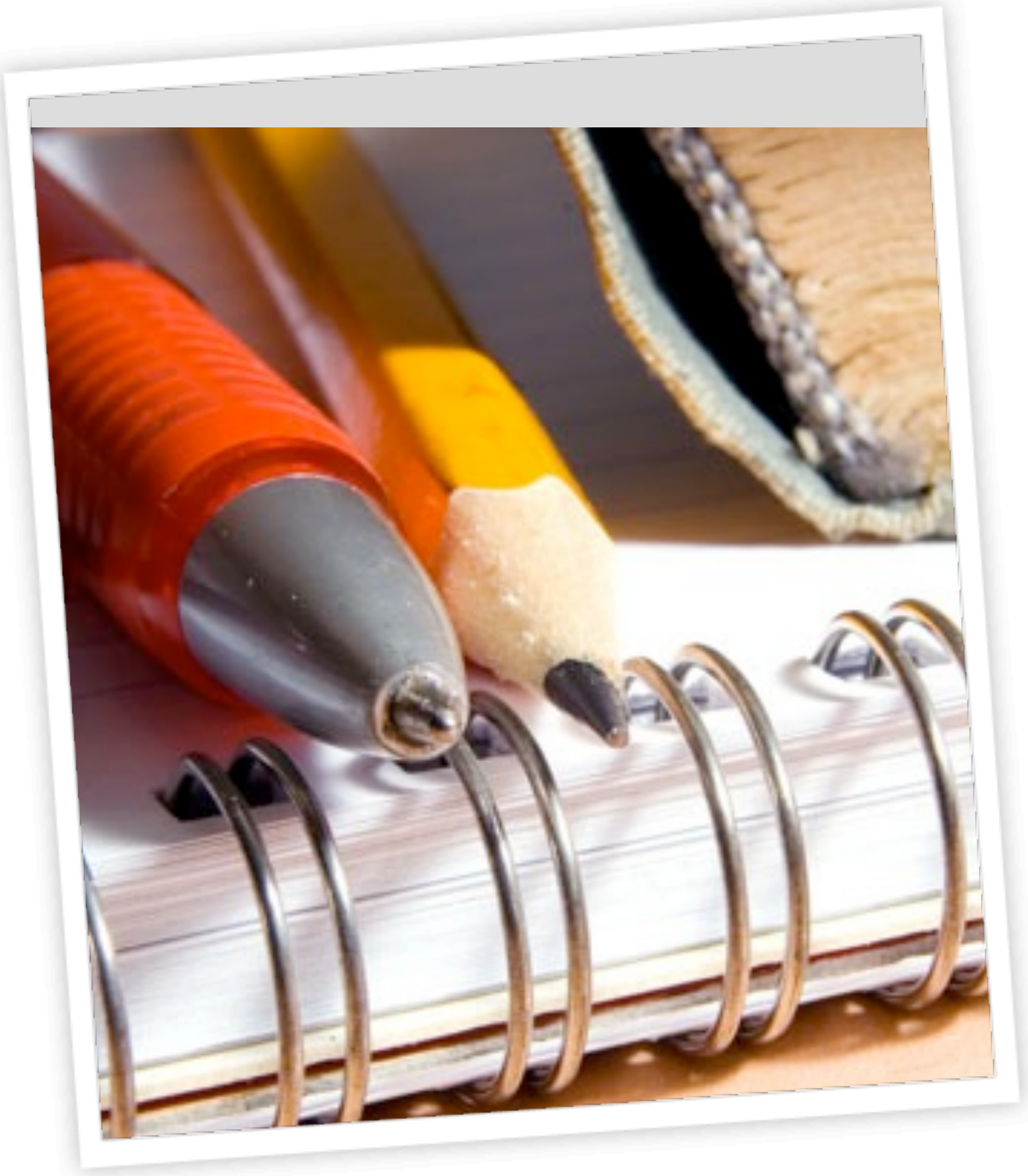
Una Rete Open Source in Sanità

Giuseppe Augiero - Alessandro Mazzarisi

1 ottobre 2011

TECNOWORKSHOP lucca2011

Fondazione Toscana Gabriele Monasterio
PER LA RICERCA MEDICA E DI SANITÀ PUBBLICA



Agenda

- La nostra realtà.
- L'Open Source in un modello di business.
- L'infrastruttura da realizzare.
- Gli aspetti tecnici.
- Conclusioni.

La Fondazione Toscana G. Monasterio

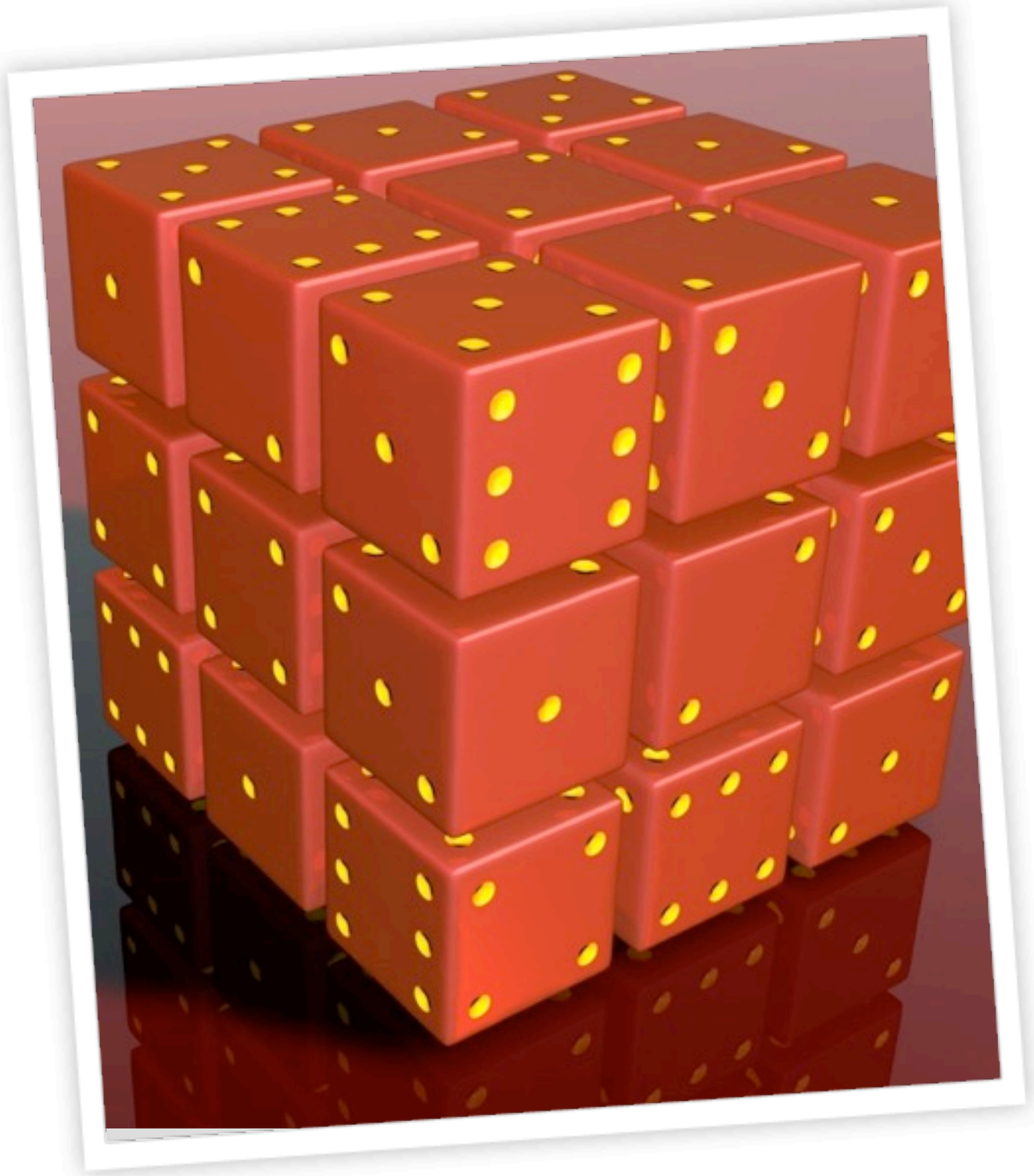
- La Fondazione Gabriele Monasterio nasce nel novembre 2007 da:
  - Cnr (Istituto Fisiologia Clinica).
  - Regione Toscana.
  - Università di Pisa, Firenze e Siena.

- La missione aziendale riguarda:
  - l'erogazione e sviluppo di assistenze sanitarie specialistiche relative alla Cardiologia e Cardiochirurgia .
  - incubatore tecnologico ICT per la Sanità.
  - l'attività di ricerca.

- Sedi:
  - **CNR** - Area della Ricerca di Pisa San Cataldo.
  - **Ospedale Pasquinucci** di Massa.
  - **Direzione** in via Trieste - Pisa.

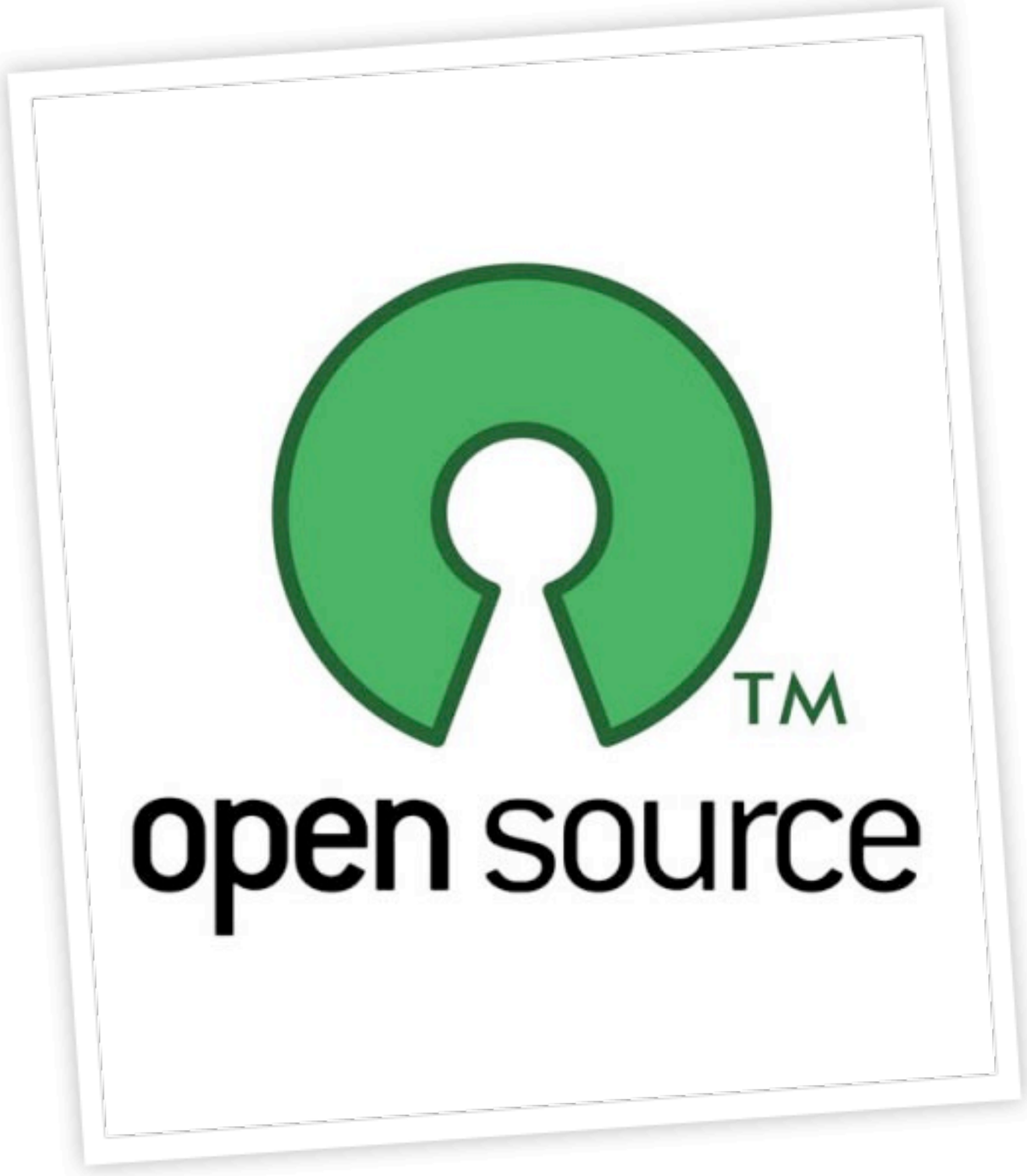
- Nel passaggio da Ente Accademico a Pubblica Amministrazione gli obiettivi aziendali sono stati:
  - Mantenere nel tempo la conformità dell'azienda a leggi e regolamenti.
  - Raggiungere un rapido ritorno degli investimenti tecnologici e infrastrutturali.
  - Partecipare con i risultati ottenuti al supporto all'innovazione.
- E' stato necessario gestire il rischio legato al cambiamento in atto andando a preservare e aumentare il valore della nostra Azienda.

Obiettivi Aziendali



Gestione del rischio

- Nella ristrutturazione dell'infrastruttura ICT è stato necessario andare ad adottare soluzioni per evitare che si interrompessero i servizi di business arrecando danni materiali, economici e di reputazione dell'azienda.
- Aree a rischio:
  - Accettazione e sistemi di prenotazione.
  - Attività degli sportelli al pubblico
  - Erogazione di cure al paziente.
  - Connettività intra ed inter-aziendale.
  - Connettività verso sistemi di governo centrale.
  - Connettività verso i fornitori di servizi.
  - Servizi per l'informazione al pubblico.



L’ipotesi Open Source

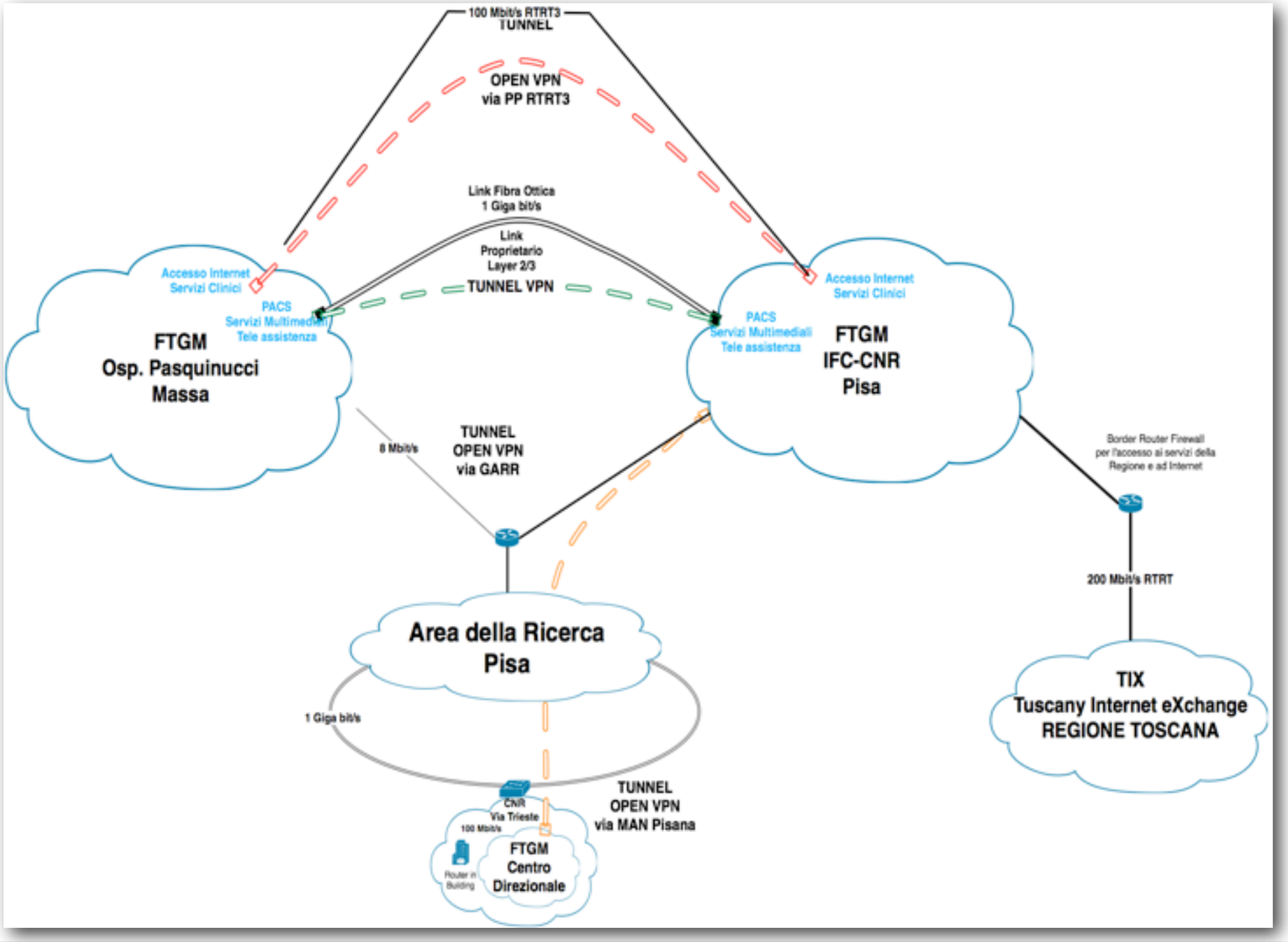
- L’obiettivo aziendale di passare da Ente accademico a Pubblica Amministrazione poteva essere raggiunto dal punto di vista tecnologico utilizzando O.S.

- L'ipotesi sostenuta dal management
  - "la trasformazione delle infrastrutture ICT da ente accademico a ente sanitario inserito in un’organizzazione complessa, già in corsa da anni, doveva essere fatta per passi, con strumenti flessibili"

- Obiettivo finale
  - "il consolidamento della struttura ICT basata sulle regole dalla nuova organizzazione di appartenenza”.

Le nostre esigenze

- Realizzare una infrastruttura di trasporto su rete geografica pubblica, adeguata per il transito di informazioni cliniche e dati sensibili, mediante Reti Virtuali Private.
- Realizzare una rete integrata tra le aree di ricerca (IFC-CNR) e di servizio (FTGM-RTRT) comunicante in modo trasparente all'interno dei singoli presidi, rispettando le peculiarità reciproche delle due organizzazioni, rispettando i vincoli di sicurezza imposti dal sistema pubblico di connettività.
- Offrire un servizio di altissimo livello e qualità.
- Architettura scalabile, riutilizzabile in ambito pubblico e di ricerca con costi iniziali estremamente contenuti.



Rete Geografica
Fondazione G. Monasterio

Fondazione
Toscana
Gabriele Monasterio
PER LA RICERCA MEDICA E DI SANITÀ PUBBLICA

Switch Off Tecnologico

- Per la realizzazione della nuova infrastruttura sarebbe stato più semplice partire da zero.
- Dovevamo, invece, lavorare su quanto già attivo e in essere.
- Non era possibile creare disservizi, interrompendo l'attività clinica.
- Alcuni protocolli "clinici" come ad esempio il DICOM non permettevano una migrazione parziale e/o diluita nel tempo.
- Tutto doveva già essere testato e verificato attraverso un testbed che rappresentasse, in scala, la nostra infrastruttura.

- Vent’anni fa i padri di Internet progettarono una architettura semplice e generale.
- Le tecnologie legate al mondo di Internet sono state sviluppate in maniera aperta.
- I protocolli e le architetture sono descritti pubblicamente.
- Chiunque può facilmente sviluppare una soluzione hardware e software da utilizzare in rete o adatta a estendere le funzionalità di rete.
- *“Quando ho dovuto sviluppare il web non ho dovuto chiedere il permesso a nessuno”* (**Tom Berners Lee**).

Il punto di partenza

Scelte implementative

- Nella veste di comunità scientifica, l'esigenza di ricerca e sperimentazione ci richiedeva la necessità di adoperare modelli e percorsi non standard che sono offerti dal mondo dell'Open Source.

- L'Open Source, secondo la nostra visione, ci offriva soluzioni flessibili e con maggiore duttilità.

- Le competenze specifiche all'interno della Fondazione avrebbero fatto da catalizzatore per la realizzazione dell'infrastruttura di rete.

Hardware

- Abbiamo deciso di adottare “server standard” per implementare il nostro progetto.
- L’architettura di un pc general purpose, normalmente, non è particolarmente ottimizzata per le operazioni di rete.
- A prima vista non potrebbe raggiungere le stesse prestazioni di una soluzione di apparati di rete che contengono hw ad hoc soprattutto dal punto di vista del data plane.
- La potenza di computazione di un normale pc è nettamente superiore rispetto a quella di un prodotto di rete.

- Durante le operazioni di rete, il percorso interno dei dati utilizza massicciamente la struttura I/O del PC.

- La larghezza di banda del bus e la capacità computazionale del server rappresentano i due elementi hardware più critici coinvolti nella determinazione delle massime prestazioni.

- Questi due elementi influenzano il valore di picco della larghezza di banda e il massimo numero di pacchetti trasmessi al secondo.

Gestire al meglio le risorse

Interfacce di rete

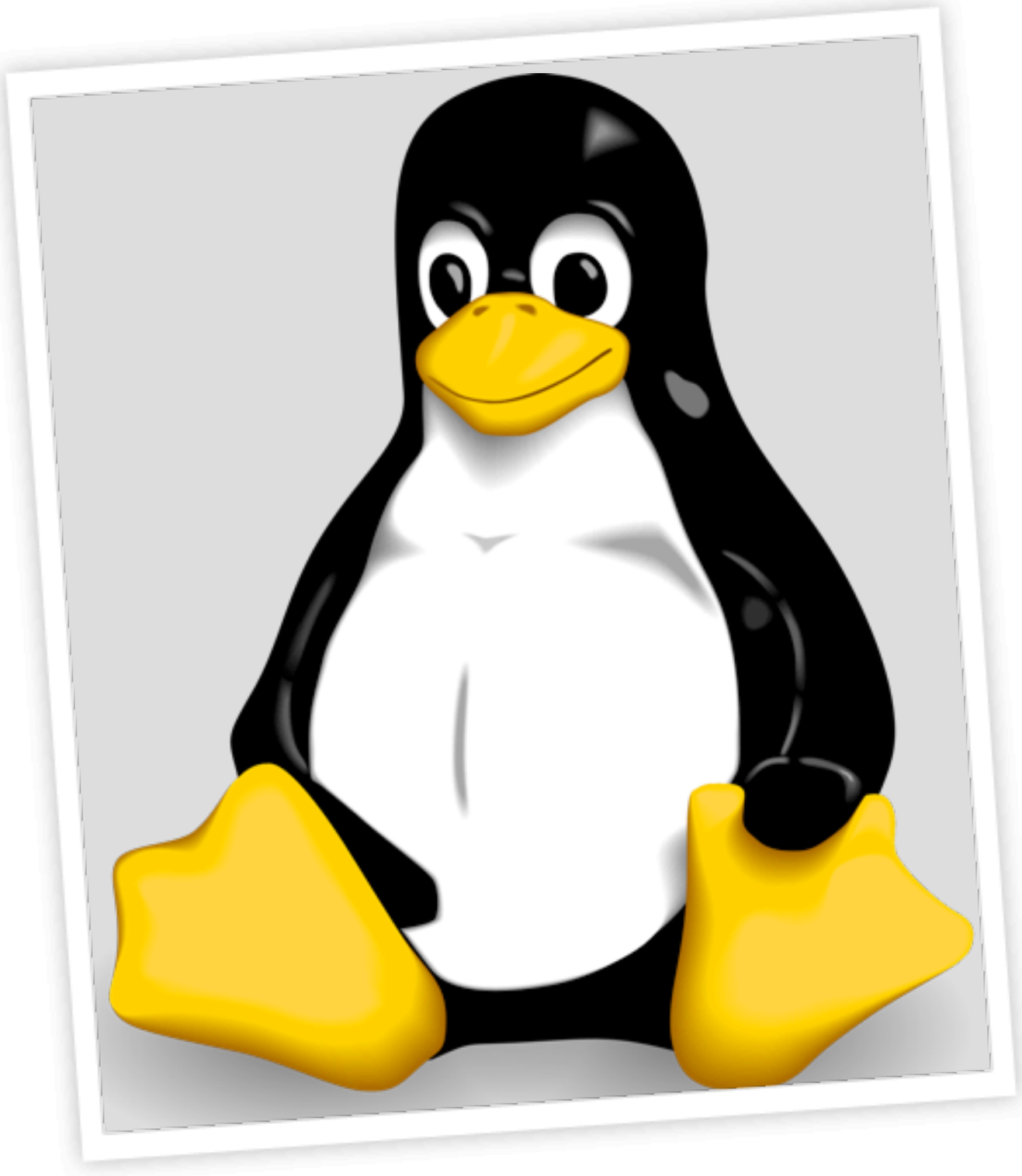
- Altro elemento cruciale sono le interfacce di rete in quanto possono condizionare le performance del sistema.

- Sul mercato esistono diverse nic con diversi gradi di prestazioni e configurabilità.

- La bontà in termini di velocità tra una scheda e l'altra si nota quando il collegamento di rete utilizzato cresce sino ad arrivare a velocità pari a 1 Gigabit o 10 Gigabit.

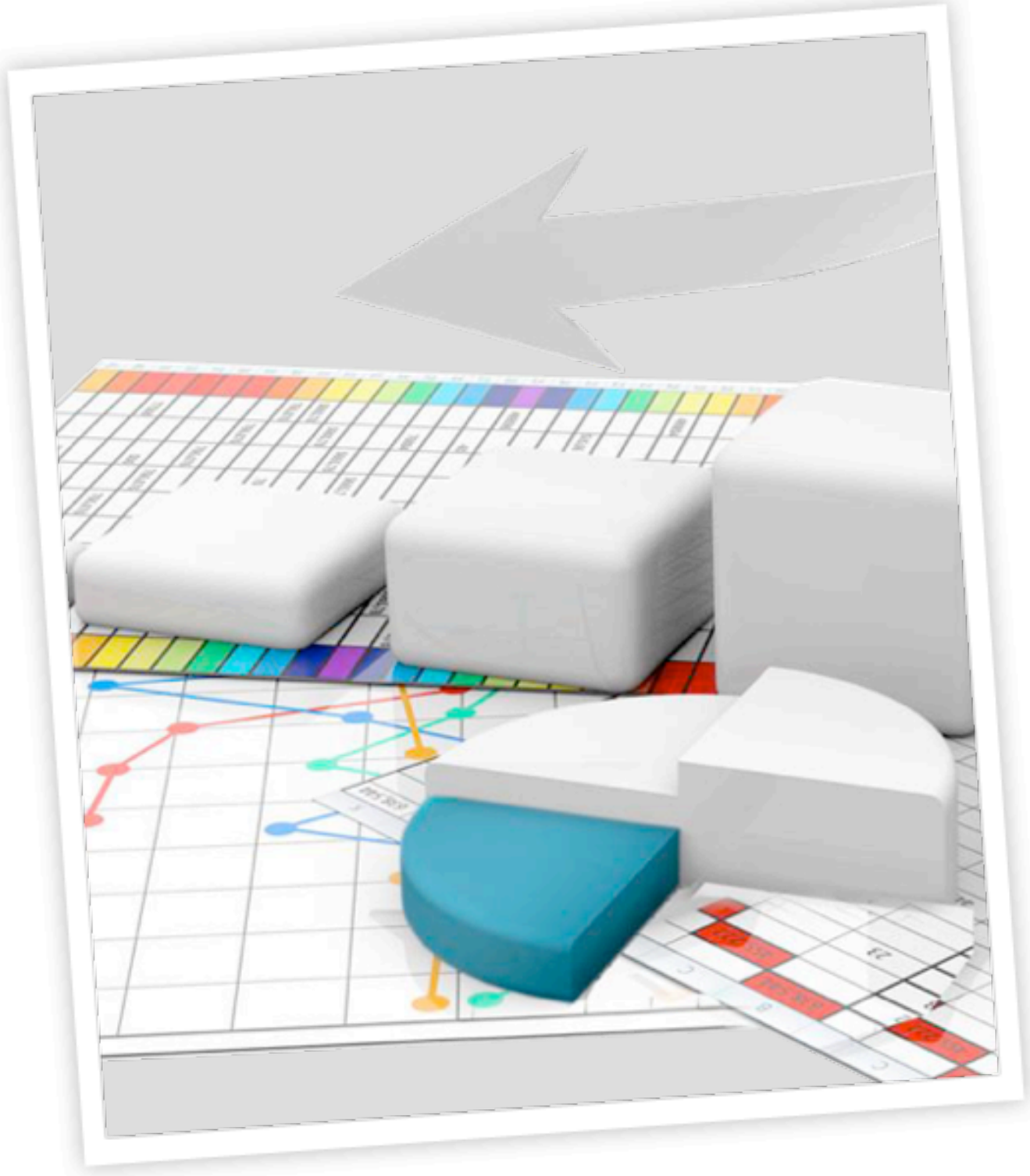
Hardware robusto

- L’hardware adoperato non può rappresentare un punto di fallimento.
- La robustezza dei server incide sui costi ma garantisce una maggiore continuità del servizio offerto.
- Requisiti necessari sono:
  - Alimentatore doppio hot swap.
  - Controller raid che supporti almeno il mirror.
  - Doppio processore.
  - Bus PCI-X
  - Schede di rete con processore a bordo.



Sistema operativo

- Abbiamo scelto Gnu/Linux come sistema operativo per la realizzazione della nostra infrastruttura.
- Installati solo i pacchetti strettamente necessari.
- Nessuna interfaccia grafica o applicazione non necessaria per il nostro scopo.
- Versione “Stable” della distribuzione.



Architettura Software

- L'architettura software deve provvedere a gestire le due attività principali:
  - Il processo di inoltro dei pacchetti (data plane).
  - La gestione delle comunicazioni per la parte di control plane.
- Linux integra tutte le funzioni di forwarding direttamente nel kernel.
- Le attività di control plane sono gestite da demoni che girano in user space.
- I processi di data e control plane, a differenza dei prodotti commerciali, condividono la Cpu del sistema.

Routing dinamico

- Il protocollo di routing adottato è Ospf.
- Il demone utilizzato per gestire il routing dinamico è Quagga.
- L'architettura multi-daemon di Quagga permette modularità, scalabilità e facile manutenzione del sistema.
- Pro:
  - Command line interface Cisco like.
  - Supporta vari protocolli di routing.
  - Supporta Ipv6.
- Contro:
  - Set di funzionalità limitate.
  - Molti file di configurazione da gestire.

Sicurezza

- Per implementare le politiche di sicurezza abbiamo utilizzato Netfilter.
- Netfilter è un componente nativo del kernel di Linux che permette l'intercettazione e la manipolazione dei pacchetti di rete.
- Il firewall di Linux offre funzionalità di filtraggio statefull dei pacchetti e di gestione del Nat.
- Pro:
  - Facilmente estendibile attraverso moduli aggiuntivi.
  - Possibilità di gestire configurazioni complesse di Nat.
- Contro:
  - Manca una vera interfaccia grafica di gestione.

Vpn

- Per la interoperabilità extraziendale verso altre aziende ospedaliere o fornitori abbiamo adottato Racoon in modo da poter instaurare con il nostro interlocutore tunnel Ipsec.

- Per i tunnel interni alla nostra infrastruttura di rete utilizziamo Openvpn che ci permette di creare tunnel cifrati in tecnologia TLS, snelli e performanti,

- Attualmente non esiste alcun apparato commerciale che supporti Openvpn.

- Le tecniche di traffic engineering hanno lo scopo di ottimizzare le prestazioni della rete.

- Il nostro obiettivo “prestazionale” è utilizzare tutte le risorse di rete (collegamenti) tra le nostre tre sedi, trasportare il traffico di rete sul link appropriato a seconda della sua tipologia.

- Inoltre vogliamo garantirci di minimizzare la perdita di pacchetti, il ritardo, la congestione, e massimizzare il throughput.

Traffic Engineering

Quality of Service

- Il trasporto del traffico clinico deve avere precedenza rispetto al trasporto di altre tipologie di traffico.

- Abbiamo la necessità di caratterizzare la qualità del servizio offerto dalla nostra rete in modo da dare priorità al traffico clinico.

- Per implementare la qualità del servizio sulla nostra rete abbiamo adottato le politiche di shaping offerte da Traffic Control (**TC**).

Alta affidabilità

- I servizi di rete devono rimanere sempre attivi e disponibili.
- I nostri router non possono rappresentare un punto di fallimento.
- La disponibilità del servizio viene garantita attraverso vari metodi:
  - Duplicazione dei sistemi.
  - Doppia Alimentazione.
  - Doppi link di rete.
  - Percorsi multipli.

- Dal punto di vista software per gestire l'alta affidabilità dei sistemi utilizziamo il protocollo VRRP e il demone KeepAlive.
- Ogni router e' composto da due server, i quali sono connessi attraverso un collegamento di rete dedicato che permette lo scambio di messaggi di stato.

Intrusion Prevention System

- Snort e’ risultato la scelta vincente per identificare traffico anomalo e accessi non autorizzati verso computer della nostra rete.
- Numero basso di falsi positivi.
- Non e’ possibile analizzare traffico cifrato.
- Attualmente usiamo Snort solo in modalità “Alert” (ids passivo).
- Pro:
  - Possibilità di utilizzo di più preprocessori (es. antivirus).
  - Set di regole disponibili su Internet.
  - Interfaccia web di gestione.
- Contro:
  - Esoso di risorse.

Autenticazione

- Per l’implementazione del supporto 802.1x offerto per l’accesso alla rete wireless (e in futuro alla rete wired) abbiamo attivato un server FreeRadius.

- Il server Radius non possiede direttamente i dati di autenticazione degli utenti.

- Le informazioni vengono richieste “in real time” al nostro server Ldap (OpenLdap).

Servizi di rete

- I servizi di rete offerti all'interno della nostra infrastruttura sono realizzati con soluzioni Open Source, altri sono scritti direttamente da noi utilizzando prodotti del mondo open.

- Ecco alcuni esempi:
  - Dhcp.
  - Dns (bind e powerdns).
  - Nagios.
  - Cacti.
  - Arpwatch.
  - FengOffice (documentazione).
  - Grisu (python e mysql).
  - Rvpn (python e mysql).

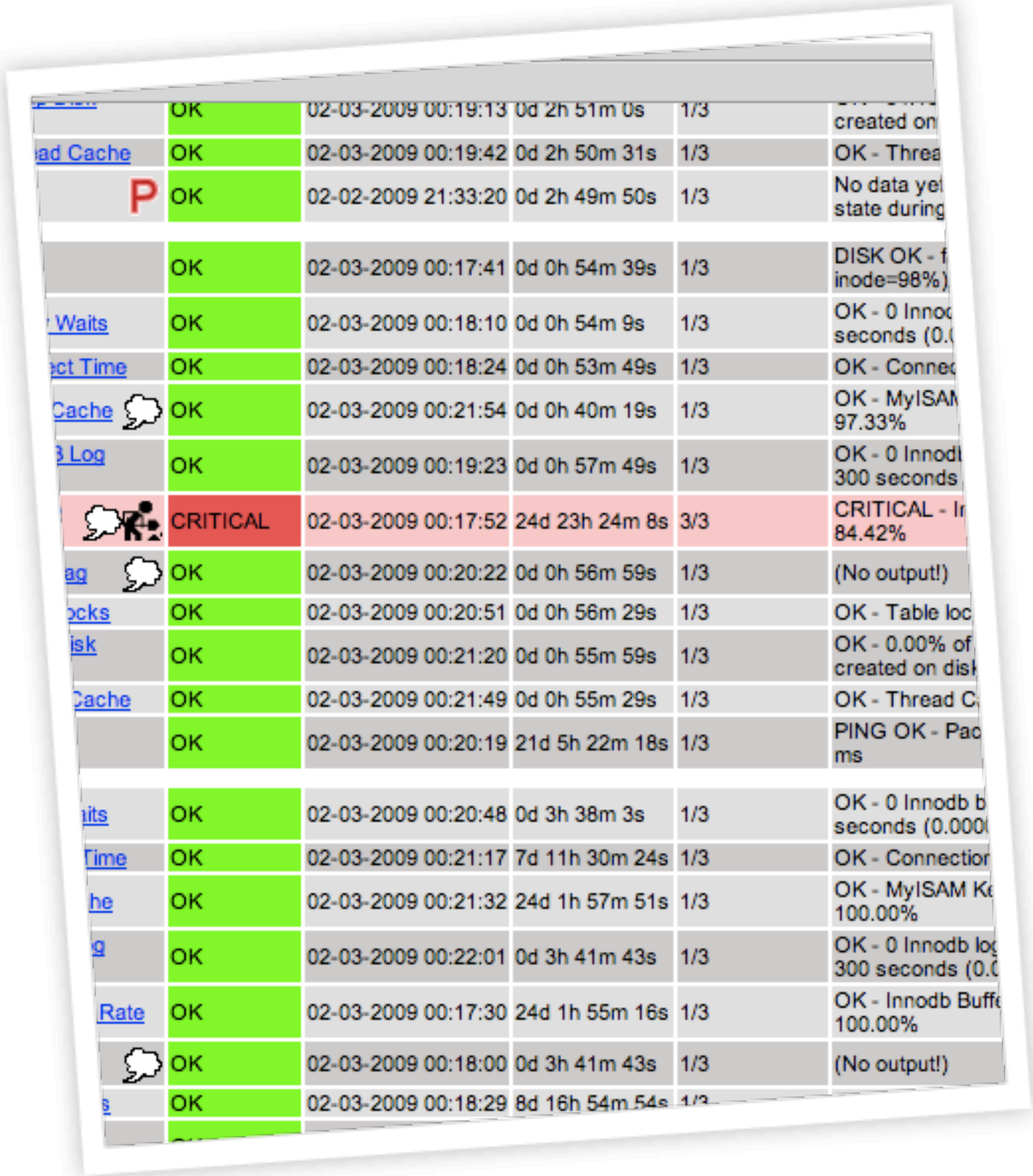
Proxy Web

- Per implementare il proxy web aziendale abbiamo adottato con grande soddisfazione Squid.

- Attraverso opportuni plug-in o content vector abbiamo esteso le funzionalità del proxy offrendo una soluzione di antivirus “in-line” per il traffico in entrata.

- Per filtrare i contenuti (p.es. la pornografia) usiamo, in simbiosi con Squid, il software open source Dansguardian.

- Il proxy web ci permette anche di “ottimizzare” il traffico in uscita verso Internet.



	OK	02-03-2009 00:19:13	0d 2h 51m 0s	1/3	created on
ad Cache	OK	02-03-2009 00:19:42	0d 2h 50m 31s	1/3	OK - Threa
P	OK	02-02-2009 21:33:20	0d 2h 49m 50s	1/3	No data yet state during
	OK	02-03-2009 00:17:41	0d 0h 54m 39s	1/3	DISK OK - f inode=98%)
Waits	OK	02-03-2009 00:18:10	0d 0h 54m 9s	1/3	OK - 0 Innoc seconds (0.(
ct Time	OK	02-03-2009 00:18:24	0d 0h 53m 49s	1/3	OK - Connec
Cache	OK	02-03-2009 00:21:54	0d 0h 40m 19s	1/3	OK - MyISAM 97.33%
3 Log	OK	02-03-2009 00:19:23	0d 0h 57m 49s	1/3	OK - 0 Innodl 300 seconds
	CRITICAL	02-03-2009 00:17:52	24d 23h 24m 8s	3/3	CRITICAL - I 84.42%
ag	OK	02-03-2009 00:20:22	0d 0h 56m 59s	1/3	(No output!)
ocks	OK	02-03-2009 00:20:51	0d 0h 56m 29s	1/3	OK - Table loc
isk	OK	02-03-2009 00:21:20	0d 0h 55m 59s	1/3	OK - 0.00% of created on disk
Cache	OK	02-03-2009 00:21:49	0d 0h 55m 29s	1/3	OK - Thread C
	OK	02-03-2009 00:20:19	21d 5h 22m 18s	1/3	PING OK - Pac ms
its	OK	02-03-2009 00:20:48	0d 3h 38m 3s	1/3	OK - 0 Innodb b seconds (0.000
Time	OK	02-03-2009 00:21:17	7d 11h 30m 24s	1/3	OK - Connectior
he	OK	02-03-2009 00:21:32	24d 1h 57m 51s	1/3	OK - MyISAM K 100.00%
g	OK	02-03-2009 00:22:01	0d 3h 41m 43s	1/3	OK - 0 Innodb log 300 seconds (0.(
Rate	OK	02-03-2009 00:17:30	24d 1h 55m 16s	1/3	OK - Innodb Buffe 100.00%
	OK	02-03-2009 00:18:00	0d 3h 41m 43s	1/3	(No output!)
s	OK	02-03-2009 00:18:29	8d 16h 54m 54s	1/3	

Monitoraggio dell’infrastruttura

- I nostri sistemi hanno bisogno di un monitoraggio continuo e puntuale.
- Il monitoring ci permette di conoscere le prestazioni dei sistemi di rete (Cacti) e di essere informati in tempo reale su eventuali malfunzionamenti degli apparati.
- Per effettuare il controllo utilizziamo Nagios con l’aggiunta di plug-in di terze parti o direttamente scritti da noi.
- Un evento anomalo o un malfunzionamento viene segnalato via Email, Sms e Dashboard.

IPv6

- La nostra infrastruttura di rete è pronta per supportare e trasportare flussi di dati in IPv6.
- La rete geografica lavora in "dual stack" per gestire a pieno il traffico di rete IPv4 e IPv6.
- Il processo di routing da noi adottato utilizza un demone ad hoc per poter veicolare in modo corretto il fusso di dati IPv6.

Conclusioni

- Abbiamo ancora molta strada da fare.
- Siamo consapevoli di non essere gli unici ad aver adottato soluzioni Open Source.
- Il nostro “non sentirci soli” ci permette di far affidamento su una comunità grande e variegata.
- La nostra attività vuole semplicemente dimostrare che le soluzioni Open Source possono essere adottate in contesti di business.
- Lavoriamo per rinforzare i consorzi di conoscenza.

Domande?????

Grazie!!!

Sito FTGM:
http://www.ftgm.it

Sito personale (slide):
http://www.augiero.it

Contatti:
giuseppe@ftgm.it
giuseppe@augiero.it

Una Rete Open Source in Sanità

Giuseppe Augiero - Alessandro Mazzarisi