UNI•C

DANMARKS IT-CENTER FOR UDDANNELSE OG FORSKNING

Networking outside your own network - The Danish showcase

NHS-HE Forum, 9th November 2006

Martin Bech,
Deputy Director, UNI•C
martin.bech@uni-c.dk

Briefly about UNI•C

- **UNI•C** is a government corporation
- **UNI•C** has approx. 310 employees and has offices in Copenhagen, Lyngby, Aarhus and Odense
- In 2005 **UNI•C's** turnover was approx. € 42 million

UNI•C Areas of Business: A full NREN + Services

- The Danish Research Network (like GARR or RedIRIS)
- The Danish Internet Exchange (DIX)
- The Danish CERT (Computer Emergency Response Team)
- Network to schools in Denmark (96%)
- Network for others…
- Content services for schools
- Administrative systems for schools
- Statistical analysis
- Consultancy work

UNI•Cs organisation
Maj 2005

Direktionssekretariatet
Sekretariatschef
Lise Dalgaard

Direktion
Administrerende direktør
Dorte Olesen

Administrationsafdelingen
Administrationschef
Jakob Klingert

Uddannelsesdivisionen
Divisionsdirektør
Per Thorbøll

Stedfortræder
Systemchef
Henrik Mikkelsen

Forskning og Samfund
Divisionsdirektør
Martin Bech

Statistik og Analyse
Underdirektør
Karsten Vest Nielsen

Intern IT og Systemdrift
Teknisk direktør
Hans Ole Aagaard

Stedfortræder
Datakommunikationschef
Ole Kjærgaard

Special facilities for special user groups

- Network for everyone

But on top of that, many of us are involved in serving the needs of special user groups:

- Supercomputing facilities
- GRID clusters
- Facilities for radio astronomy
- Video and telephony
- Content portals, databases etc.

But what about facilities for health research and health care?

NRENs provide a lot of services…

	Universities and research institutions	Hospitals
Basic Internet connectivity	Yes	Yes
Video conferencing	Yes	
Collaboration tools	Yes	
Lambda networking	Yes	
IPv6	Yes (but no use)	
Roaming services	Yes	
CERT and security	Yes	
GRID and Scientific Computing	Yes	
Media Libraries	Yes	

For the health care sector, plain old internet is just not enough

The standard services of an NREN (or any telco) are not usable because of security constraints:

- Privacy and integrity of the data transmitted
- Connecting with everyone else means that firewalls have to have a lot of openings into the internal networks

If we want to serve the health care sector, we need to do something special because

The health sector is not like other sectors of modern society:

- in most sectors (finance, transport), organizations exchange data via a few well-known applications
- in the educational and research sectors, there are not as strict barriers between parties
- in public administration everyone keep to themselves, exchange messages and use a few common applications
- but in the health sector there is a rising need for exchanging both data and connections between a large number of applications (many of which are not pre-defined),
- and at the same time, privacy and security has to be respected.

Communication across organizations in healthcare

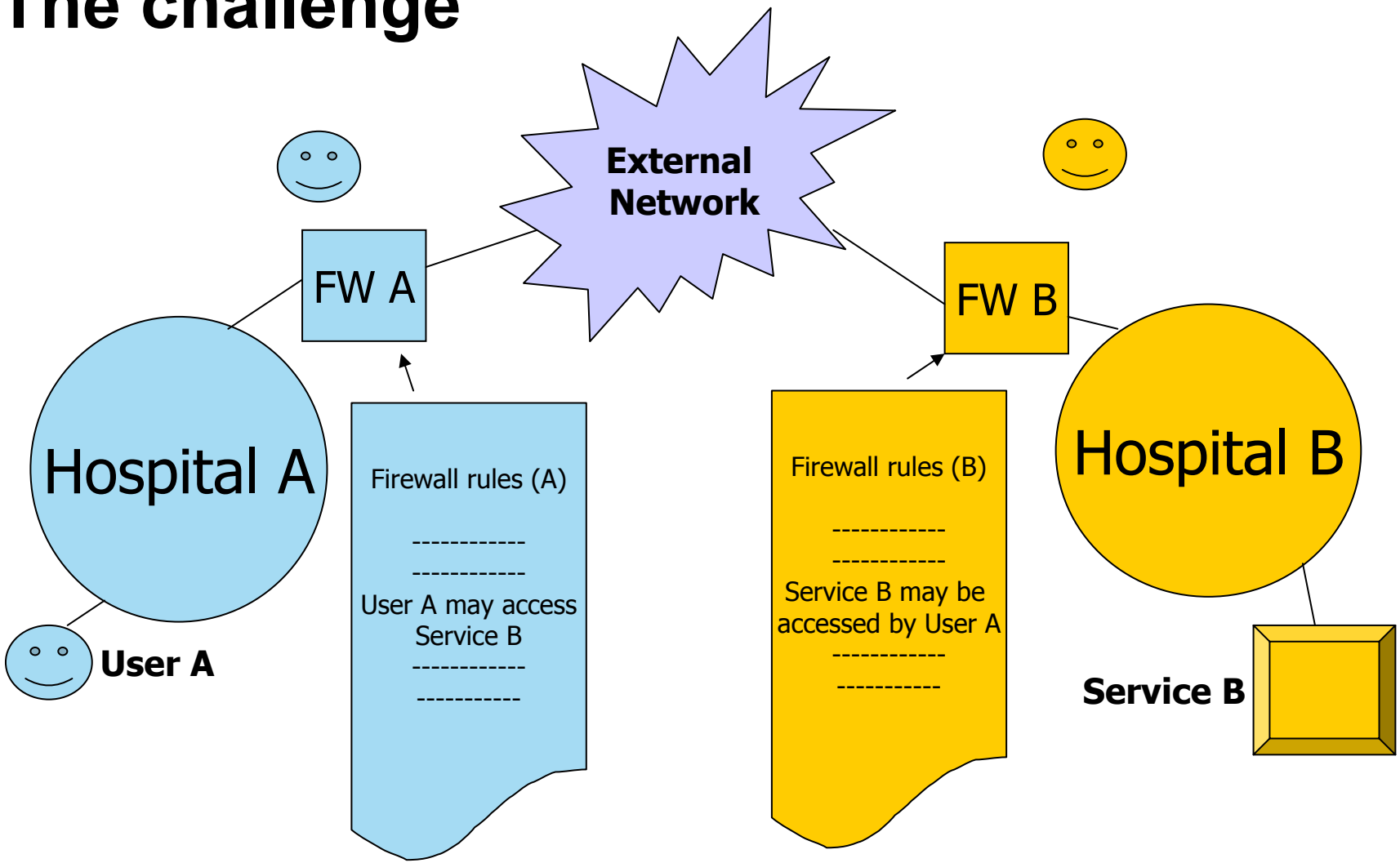
- Everybody wants to exchange data (at least ideally!)
- Every small part of the health system has its own firewall, security administration, access control mechanisms etc
- Every connection to or from such an entity requires approval, configuration, documentation and subsequently auditing

HealthGrids – in practice

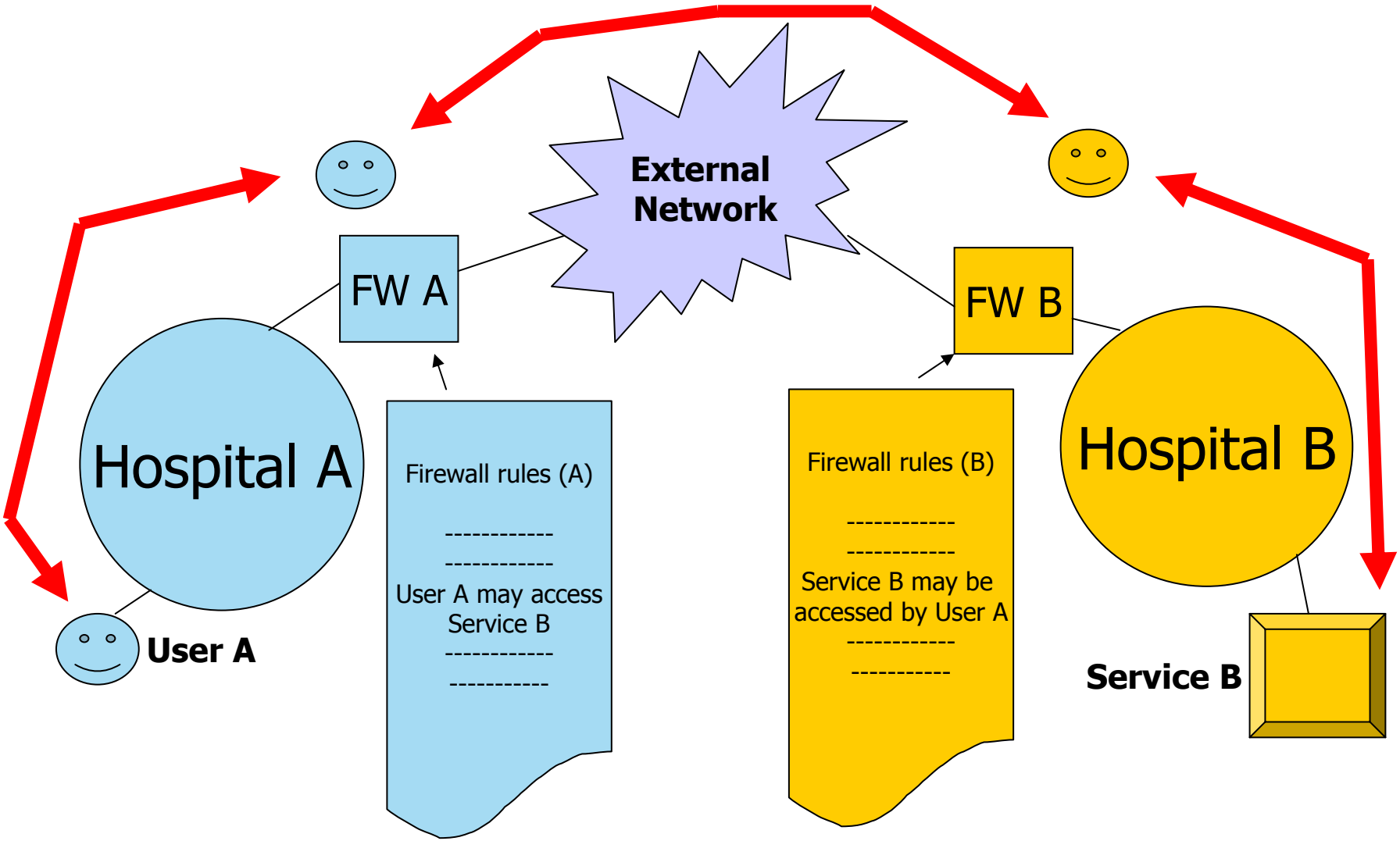
- Not just one grid node inside your network, communicating with ”the grid” – not even close!
- Some grid applications are accessed with clients to a remote facility (typically on TCP port 21XX)
- Some grids are operated by logging in with ssh (TCP port 22) to a remote node
- Some use a resource broker that is contacted first (TCP port 8443)
- Other use Web/SOAP/XML interfaces

In any event: The state of the art today is that most projects and applications are using separate infrastructures

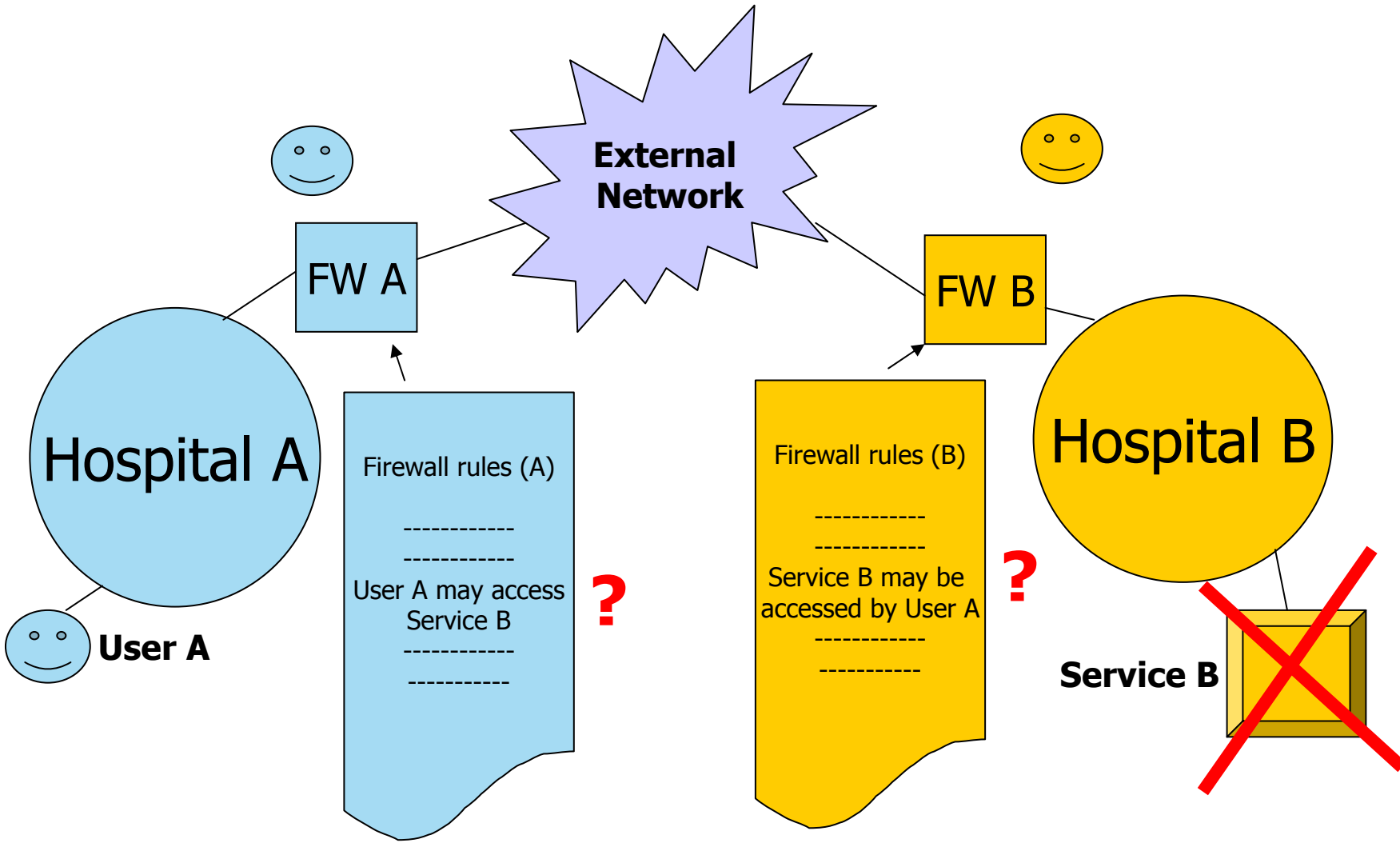
The challenge



Setup of a new connection



Expiry of a connection



Manual administration

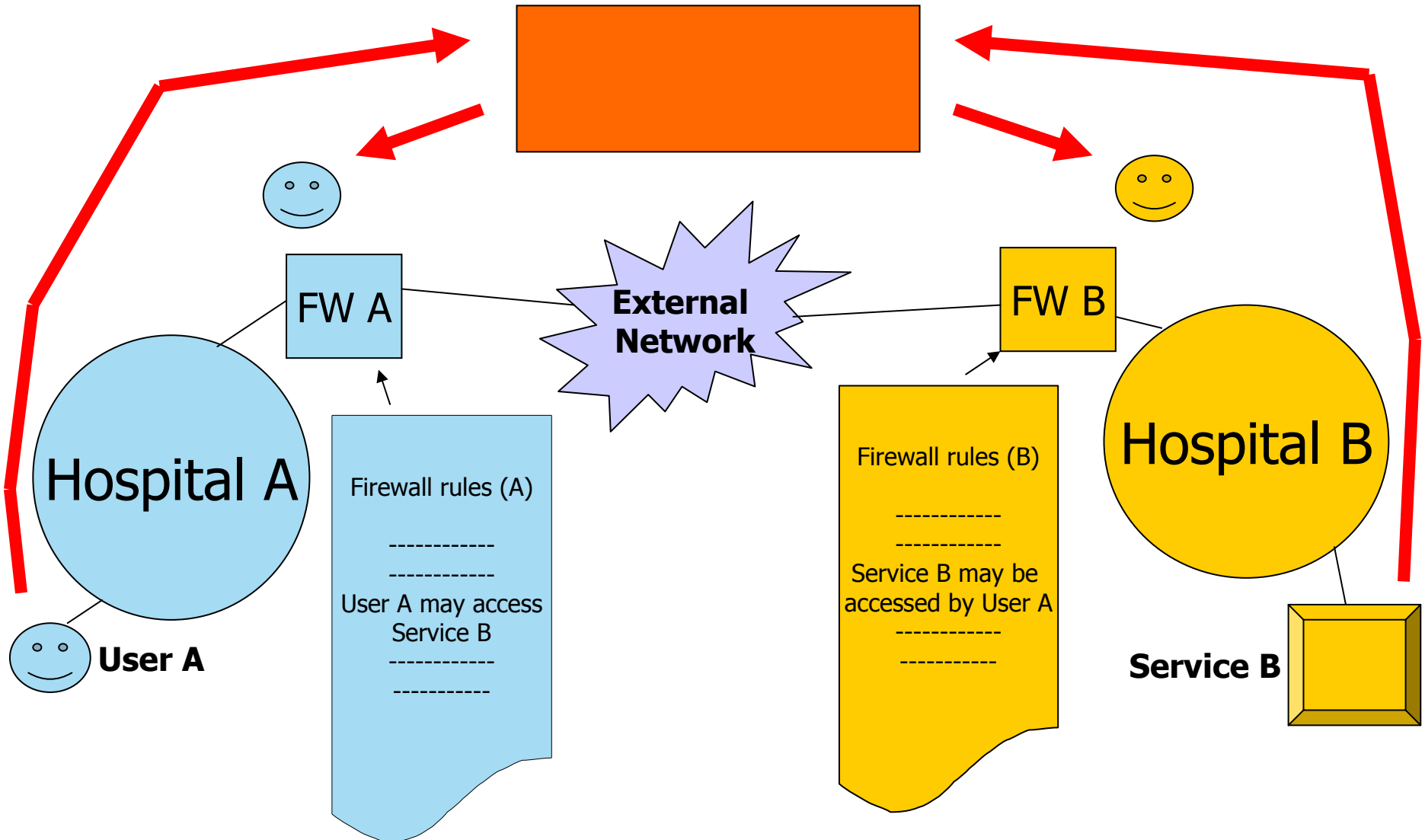
- No problem for a single example such as this
- But, if a national network contains 50 firewalls and just 10 common services are to be used across every unit, the total number of rules is 12.250
- Most firewall administrators can't say who is responsible for every rule

Therefore: We need a system to keep track of all these connections

The Connection agreement system

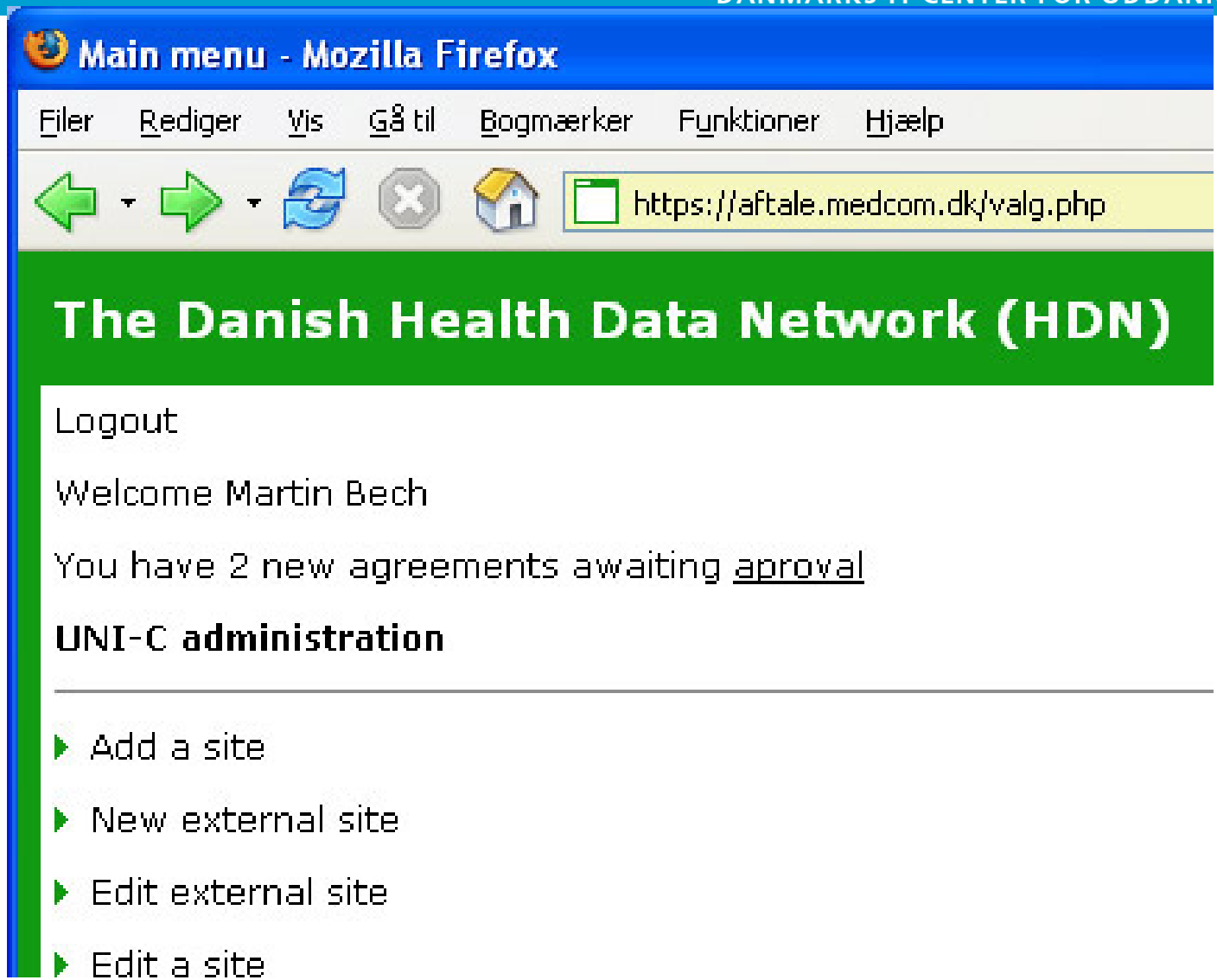
- All groups of users and all services are put into the system by the users
- User A finds Service B in a large directory
- User A enters a request for a connection to system B
- Both User A and the administrator of Service B accepts the connection in the system
- The system generates rules which the fírewall administrators put into their firewalls

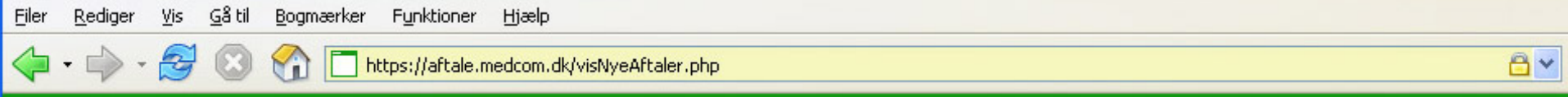
Using the connection agreement system



The connection agreement system

- Everybody can find the services they need – and each other
- Eliminates the need for administering a huge number of VPN tunnels
- Establishes documentation of who ordered what connection and how long it is supposed to exist
- Simplifies security administration
- A simple and inexpensive solution to a problem that is common to all nation-wide health care systems


Main menu - Mozilla Firefox
Filer Rediger Vis Gå til Bogmærker Funktioner Hjælp
https://aftale.medcom.dk/valg.php
The Danish Health Data Network (HDN)
Logout
Welcome Martin Bech
You have 2 new agreements awaiting aproval
UNI-C administration
Add a site
New external site
Edit external site
Edit a site



The Danish Health Data Network (HDN)

Logout | Menu

TESTLOKATION-aarhus new agreements

agreement no: 20050906085541-590

TESTLOKATION-Lyngby-video	TESTLOKATION-aarhus
Server: videostander.uni-c.medcom, 195.80.243.114, Alle-høje-porte	Client: videotest, 195.80.243.70
Contact: TESTLOKATION-3 administrator	Contact: Lennart Sorth, tlf.: 35878889
Comment: UNI-C test regel - til videokonference test (H.323 mv)	

TESTLOKATION-Lyngby-video has deleted the agreement

○ Delete agreement

Kommentar:

GO

15-03-2006 12:58:28:	Lennart Sorth	Godkendt okidokey
2-11-2005 14:18:35:	Anders Mundt Due	Godkendt Nogen i Århus må godt lige sige ok ;-)
21-11-2005 14:08:06:	Martin Bech	Godkendt
22-03-2006 10:13:29:	Lennart Sorth	Fortrudt
22-03-2006 15:26:47:	Lennart Sorth	Fortrudt
31-10-2005 14:11:31:	Anders Mundt Due	Godkendt
6-09-2005 08:55:53:	Lennart Sorth	Aftale oprettet
6-09-2005 08:56:42:	Lennart Sorth	Godkendt Lad os nu teste H.323 ml Lgb og Aarhus
6-09-2005 08:59:43:	Lennart Sorth	Godkendt helt fint, den er jeg også med på :)

agreement no: 20051007135219-639

TESTLOKATION-Lyngby-video	TESTLOKATION-aarhus
Server: videostander.uni-c.medcom, 195.80.243.114, Polycom-VDO-KONF	Client: videotest, 195.80.243.70
Contact: TESTLOKATION-3 administrator	Contact: Lennart Sorth, tlf.: 35878889

TESTLOKATION-Lyngby-video has deleted the agreement

○ Delete agreement

Kommentar:

15-03-2006 12:58:20:	Lennart Sorth	Godkendt okidokey
22-03-2006 10:13:44:	Lennart Sorth	Fortrudt
7-10-2005 13:52:29:	Dan Mønster	Aftale oprettet

The Danish Health Data Network (HDN)

Logout | Menu

All agreements for H:S

Show agreements for a single site: H:S Show New timestamp: Set

			Not approved	Approved	Expired		
Agreement No.	20030611154041-29	Expiration date: 0000-00-00	○	◉	○	HTTP	Update
Server:	Århus Amt	NIP - Nationale Indikator Projekt		Lone Kærsvang	195.80.243.98		☐ Delete
Client:	H:S	HSKlient		Johan Kjærgaard	195.80.242.33		
Agreement No.	20030925153731-69	Expiration date: 2008-09-25	○	◉	○	SSH	Update
Server:	Sundheds Portalen, sundhed.dk	Sundhedsportalen TeamSite1		Ole Widriksen	195.80.245.1		☐ Delete
Client:	H:S	H:S redaktion til (teamsite) sundhedsportalen		Gorm Mandsberg	195.80.242.34		
Agreement No.	20030925160840-70	Expiration date: 2008-09-25	○	◉	○	HTTP	Update
Server:	Sundheds Portalen, sundhed.dk	Sundhedsportalen TeamSite1		Ole Widriksen	195.80.245.1		☐ Delete
Client:	H:S	H:S redaktion til (teamsite) sundhedsportalen		Gorm Mandsberg	195.80.242.34		
Agreement No.	20030925160913-71	Expiration date: 2008-09-25	○	◉	○	HTTP	Update
Server:	Sundheds Portalen, sundhed.dk	Sundhedsportalen TeamSite2		Ole Widriksen	195.80.245.2		☐ Delete
Client:	H:S	H:S redaktion til (teamsite) sundhedsportalen		Gorm Mandsberg	195.80.242.34		
Agreement No.	20030925161031-72	Expiration date: 2008-09-25	○	◉	○	SSH	Update
Server:	Sundheds Portalen, sundhed.dk	Sundhedsportalen TeamSite2		Ole Widriksen	195.80.245.2		☐ Delete
Client:	H:S	H:S redaktion til (teamsite) sundhedsportalen		Gorm Mandsberg	195.80.242.34		
Agreement No.	20030925161315-73	Expiration date: 2008-09-25	○	◉	○	HTTPS	Update
Server:	Københavns Praktiserende Lægers Laboratorium	KPLL		Niels Hornum	195.80.243.75		☐ Delete
Client:	H:S	HSKlient		Johan Kjærgaard	195.80.242.33		
Agreement No.	20031118092724-144	Expiration date: 2008-11-18	○	◉	○	HTTP	Update
Server:	Sundheds Portalen, sundhed.dk	Sundhedsportalen WXC		Ole Widriksen	195.80.245.6		☐ Delete

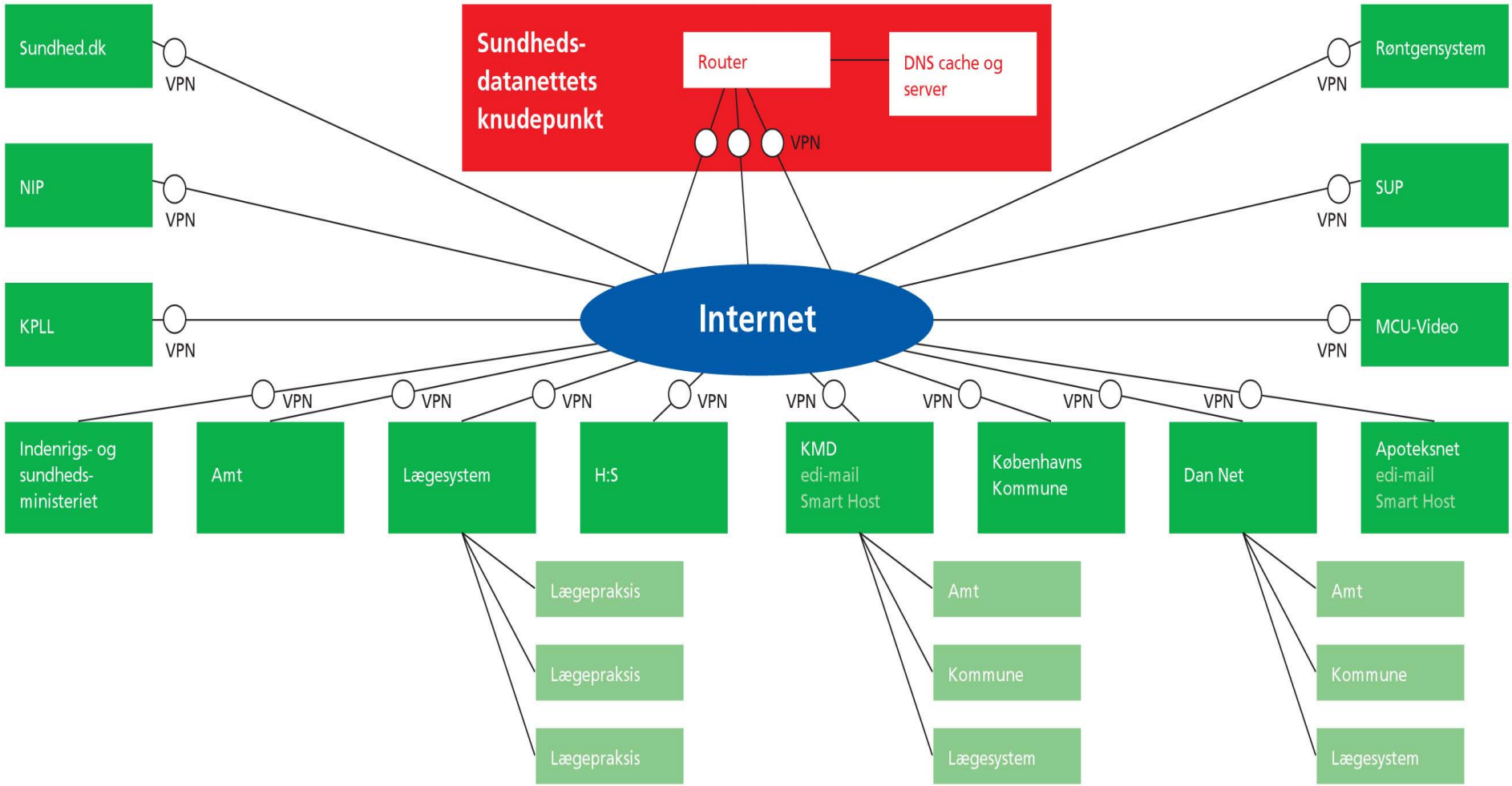
The process in Denmark towards a unified network

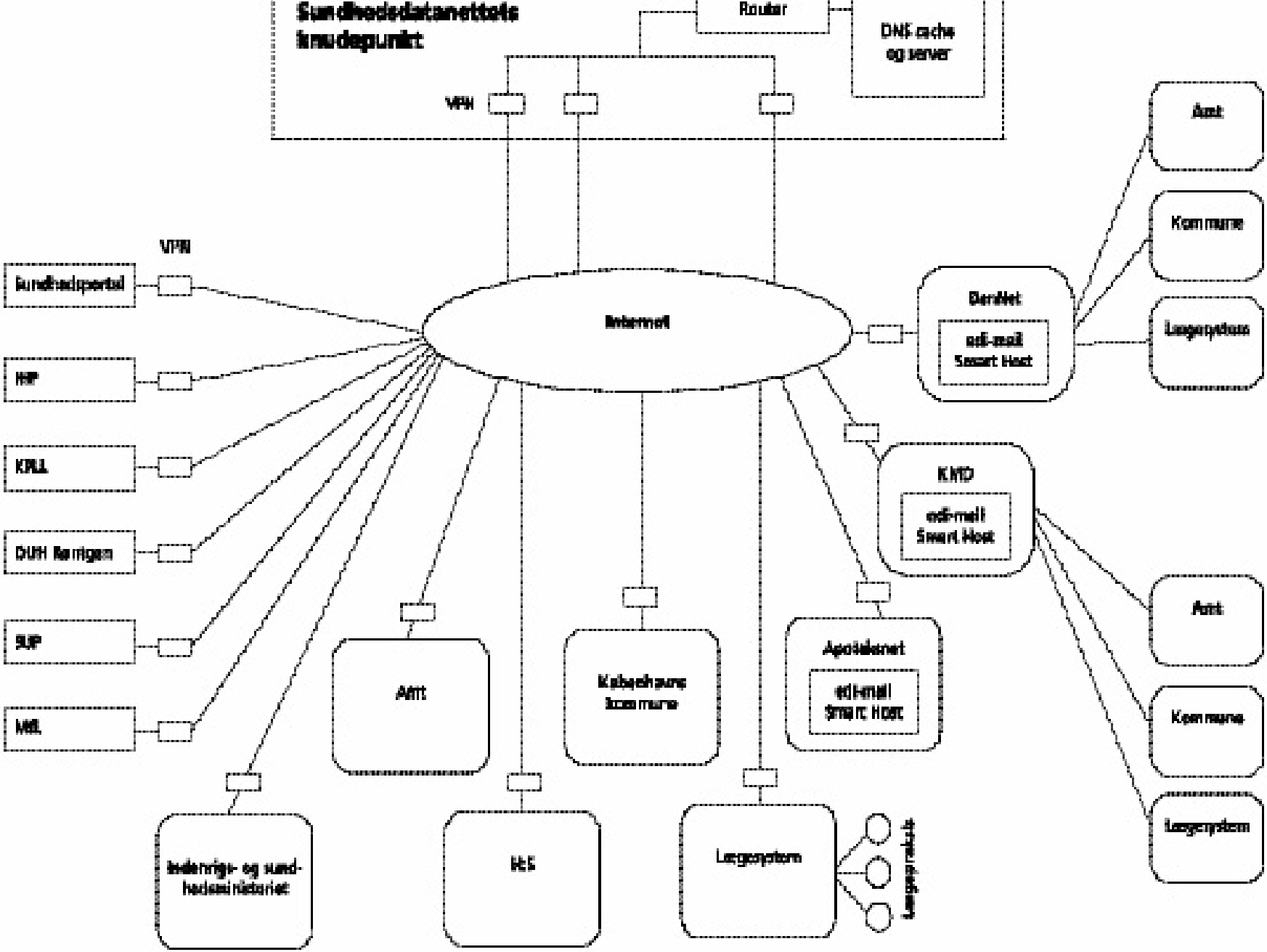
- Clever guys in MedCom wanted ”some kind of interconnect”
- They came to us in 2001, and we proposed a series of interviews with the regional networks
- An infrastructure working group was formed
- The democratic process lead to the design
- A prototype network was formed, and tests carried out
- By january 2003, first ”real” traffic in the network
- Tender process for most of 2004
- Regular operation by May 2005
- Today: All hospitals, all pharmacies, all local authorities, 1/3 of GPs, ½ of specialized doctors and vendors, laboratories etc…

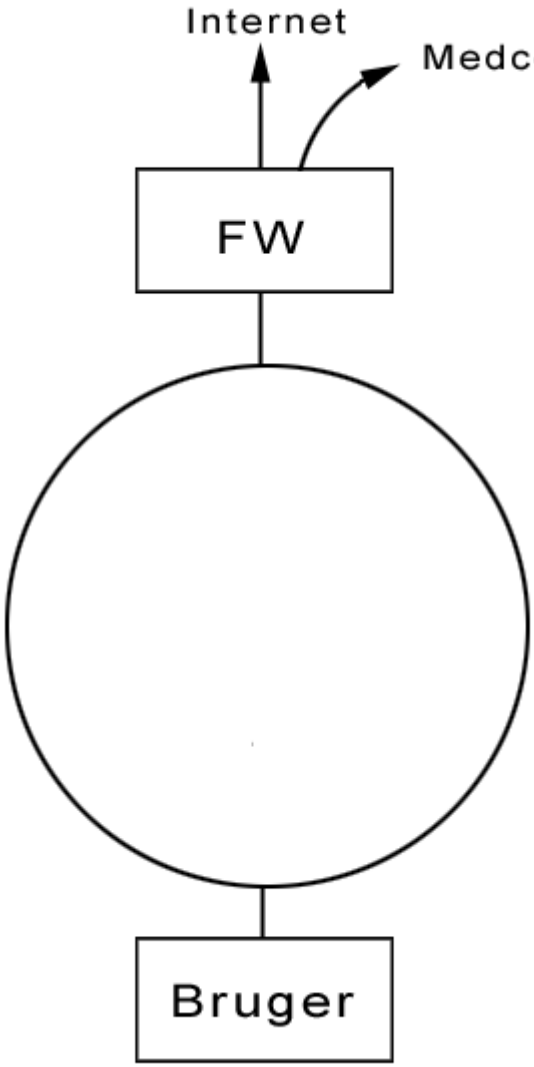
UNI•C

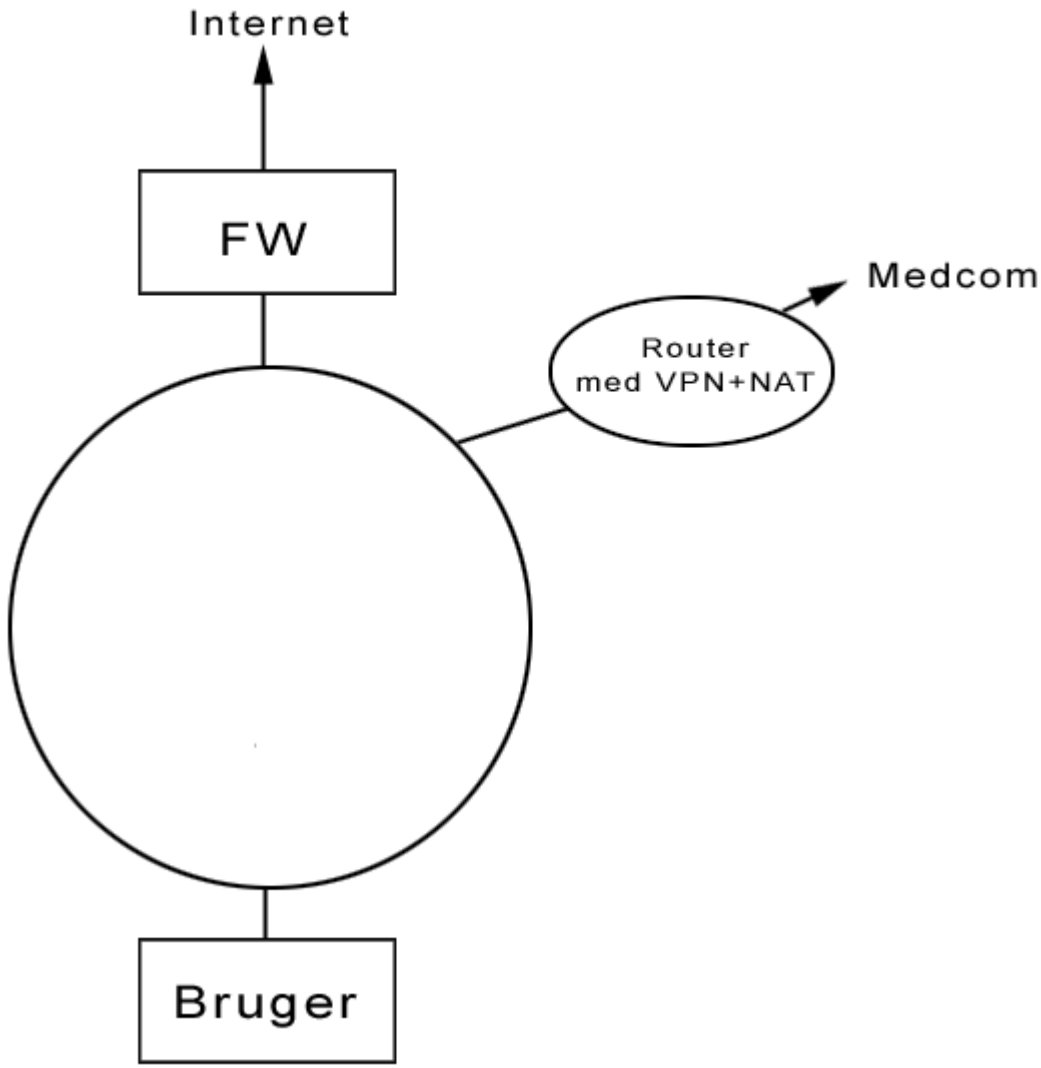
The Danish Research Network: Forskningsnettet

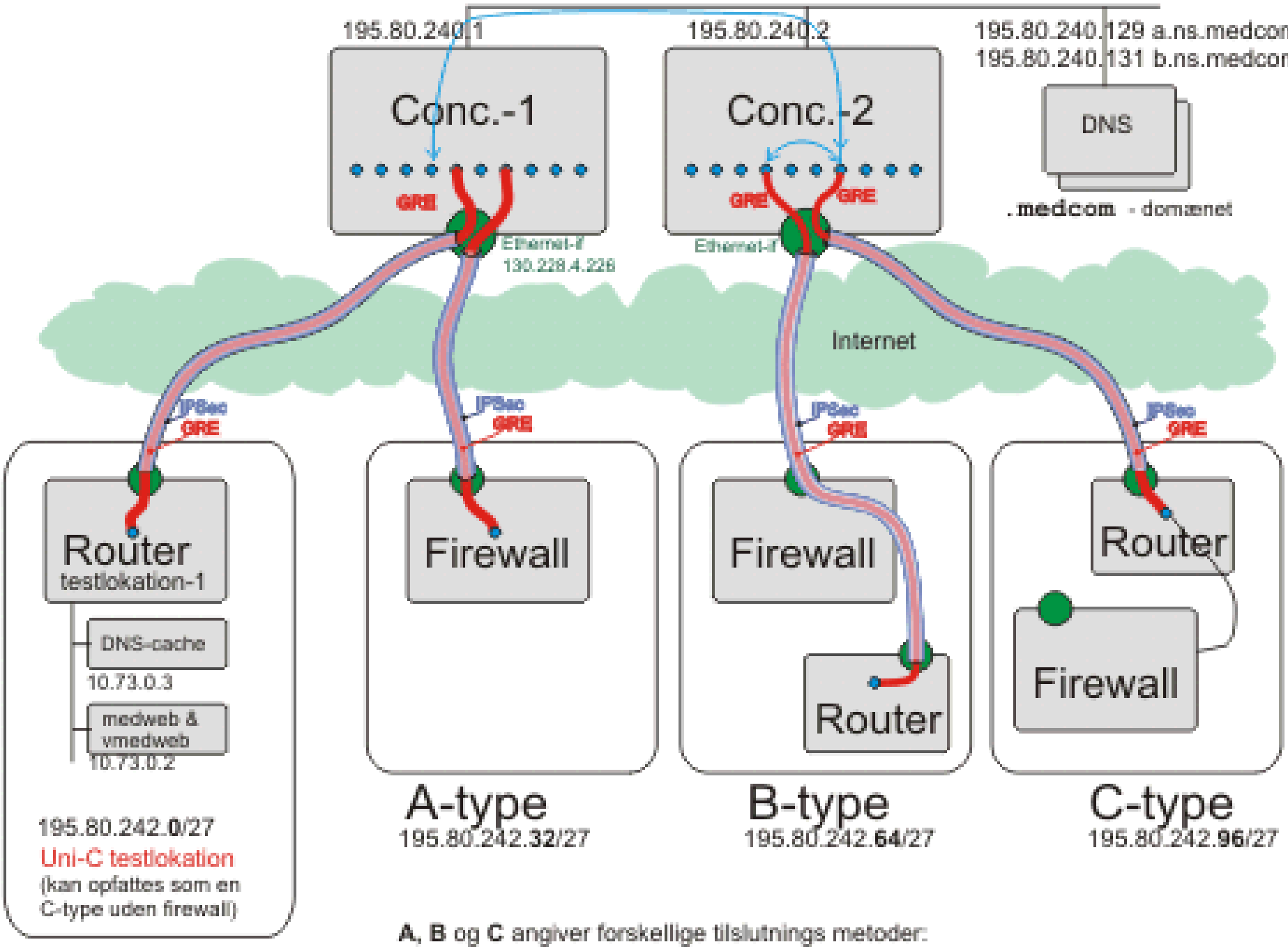
Example: Before the Danish Health Data Network, exchange of big scanner images between the university hospitals in Aarhus and Odense had be done using a separate, leased line


Sundhed.dk
NIP
KPLL
VPN
Sundheds-datanettets knudepunkt
Router
DNS cache og server
Internet
Røntgensystem
SUP
MCU-Video
Indenrigs- og sundheds-ministeriet
Amt
Lægesystem
H:S
KMD edi-mail Smart Host
Københavns Kommune
Dan Net
Apoteksnet edi-mail Smart Host
Lægepraksis
Lægepraksis
Lægepraksis
Amt
Kommune
Lægesystem
Amt
Kommune
Lægesystem


Sundhedsdatanettets
knudepunkt
Router
DNS cache
og server
VPN
Amt
Kommune
Lægesystem
VPN
Sundhedsportal
Internet
Dansk Net
edi-mail
Smart Host
HIP
KMD
KMD
edi-mail
Smart Host
DUH Farmigen
Amt
Kobenhavns
kommune
Apotekernet
edi-mail
Smart Host
SUP
MEL
Amt
Kommune
Lægesystem
Indenrigs- og sund-
hedsministeriet
MES
Lægesystem
Lægepraksis


Internet
Medcom
FW
Bruger


Internet
FW
Medcom
Router
med VPN+NAT
Bruger


195.80.240.1
195.80.240.2
195.80.240.129 a.ns.medcom
195.80.240.131 b.ns.medcom
Conc.-1
Conc.-2
DNS
.medcom - domænet
GRE
GRE
GRE
Ethernet-if
130.228.4.226
Ethernet-if
Internet
IPSec
GRE
IPSec
GRE
IPSec
GRE
IPSec
GRE
Router
testlokation-1
DNS-cache
10.73.0.3
medweb &
vmedweb
10.73.0.2
Firewall
Firewall
Router
Router
Firewall
195.80.242.0/27
Uni-C testlokation
(kan opfattes som en
C-type uden firewall)
A-type
195.80.242.32/27
B-type
195.80.242.64/27
C-type
195.80.242.96/27
A, B og C angiver forskellige tilslutnings metoder:

UNI•C

The Danish Research Network: Forskningsnettet

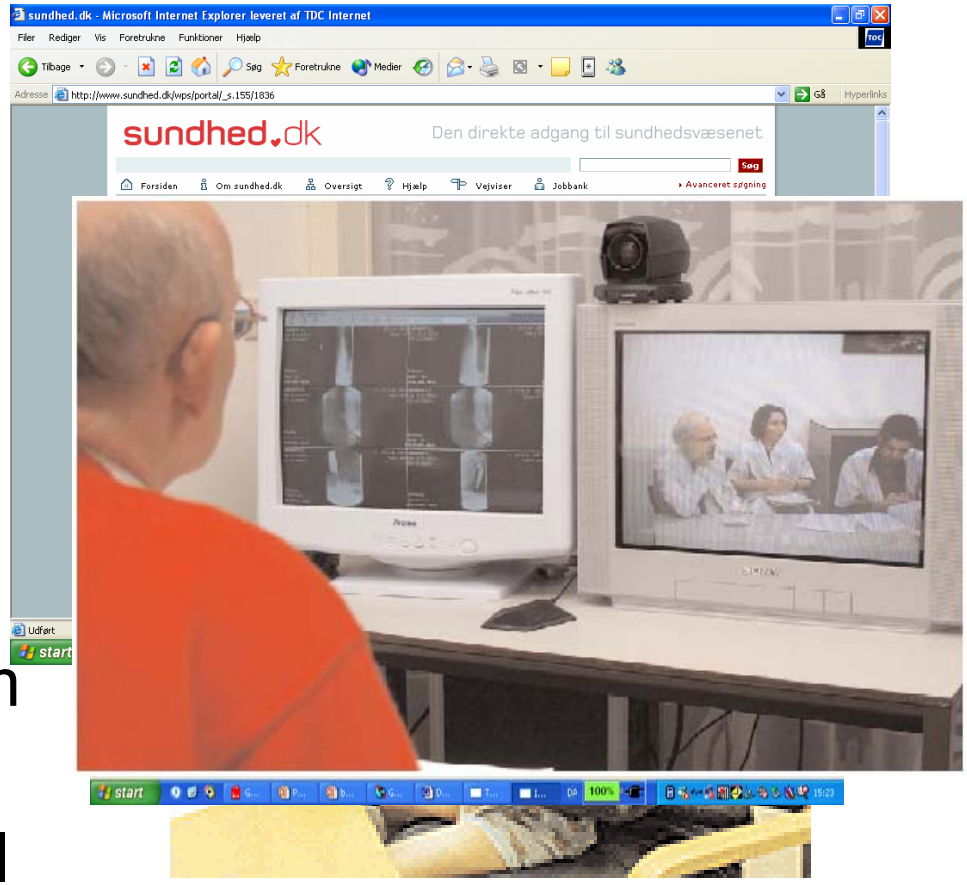
Is in business again!

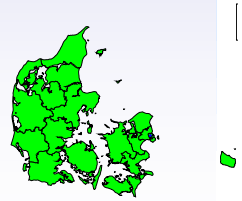
MedCom

Center for
Sundheds-telematik

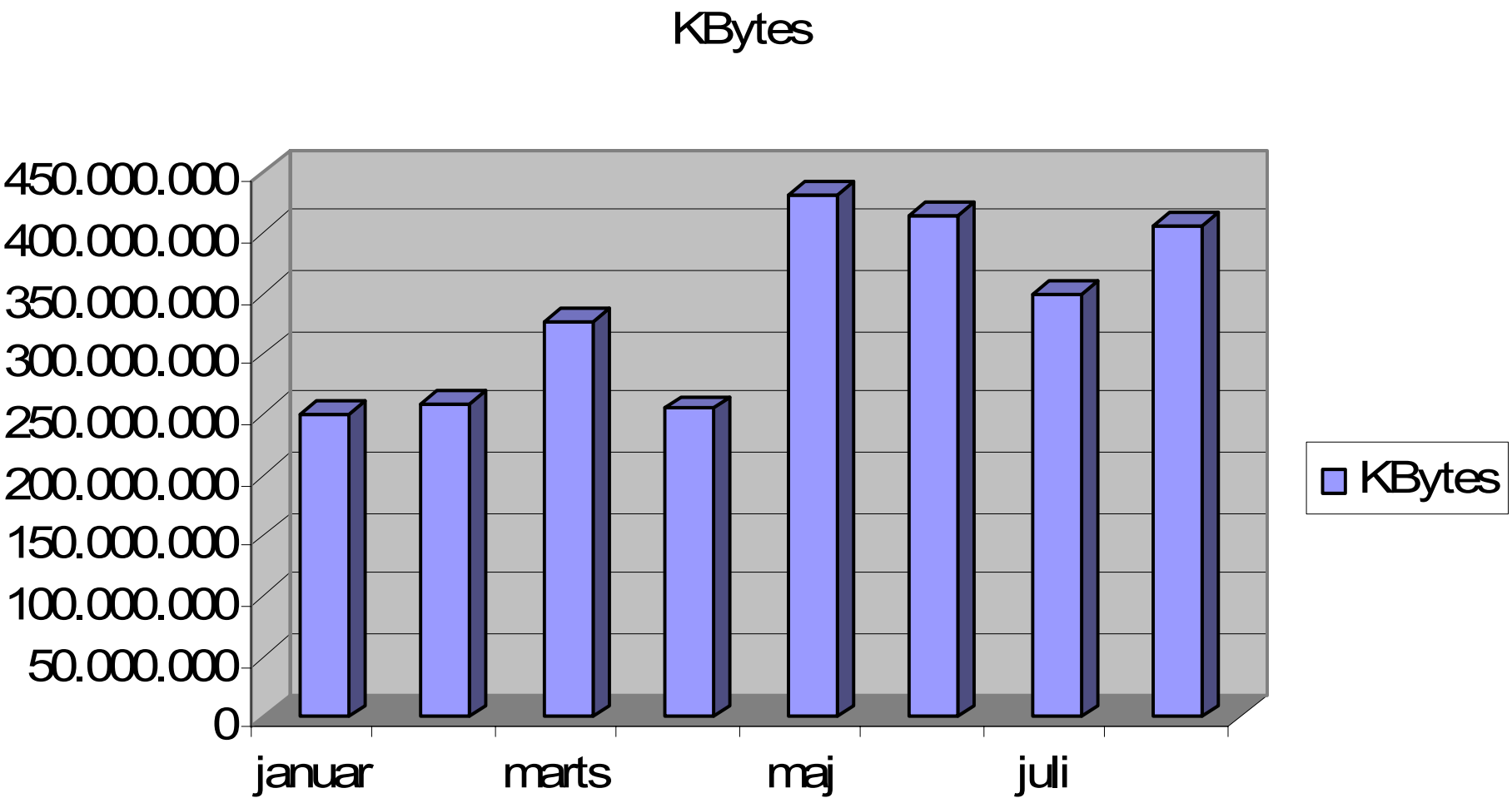
Internet project: Services

- Web accesss
- Teleconsultation
- Videoconference
- Collaboration Platform
- National Health Portal

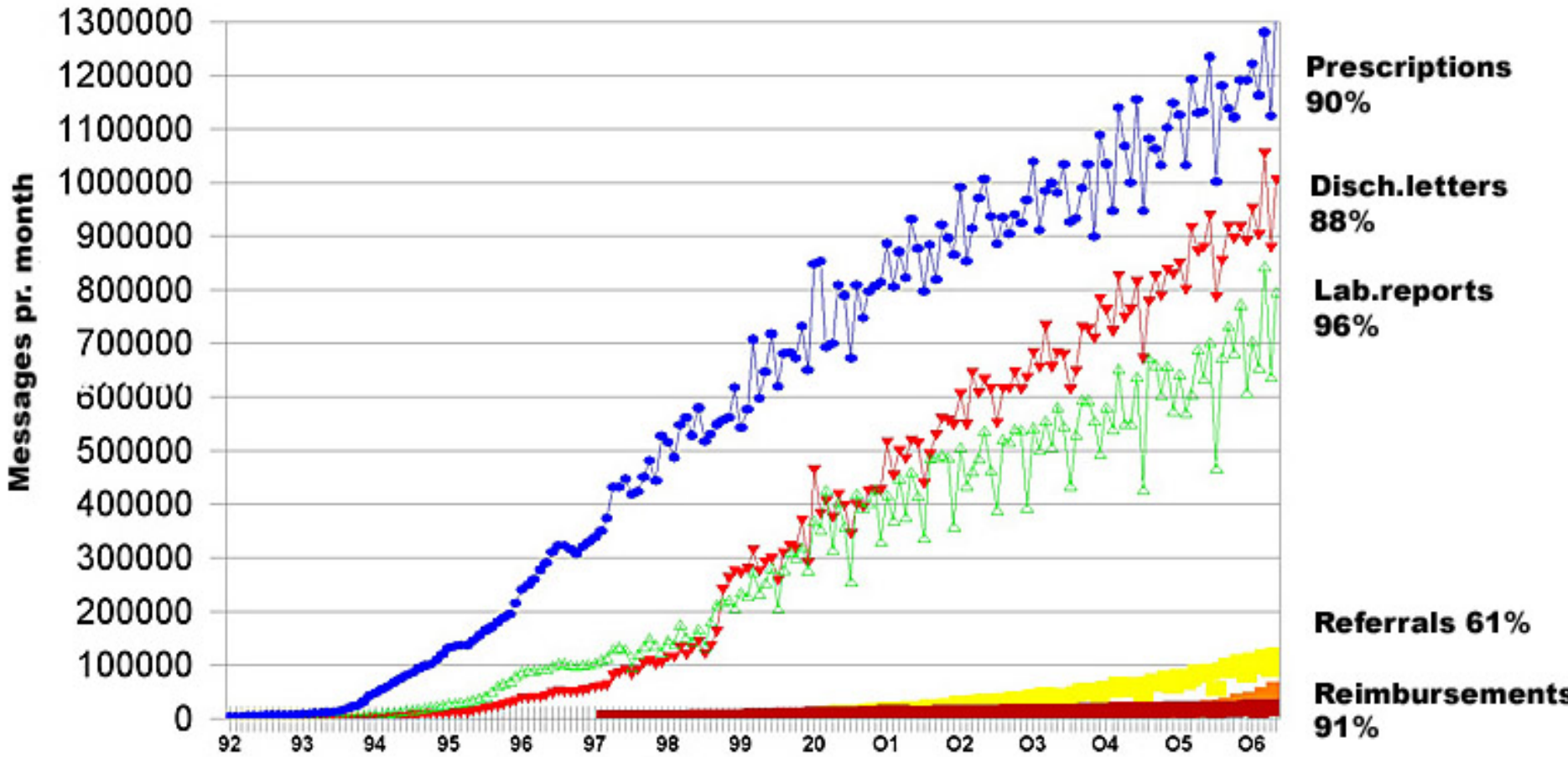




Traffic volumes in the Danish Health Data network



Message-based data exchange on the Danish National Network: >3 million pr. month



Direct benefits for the health sector

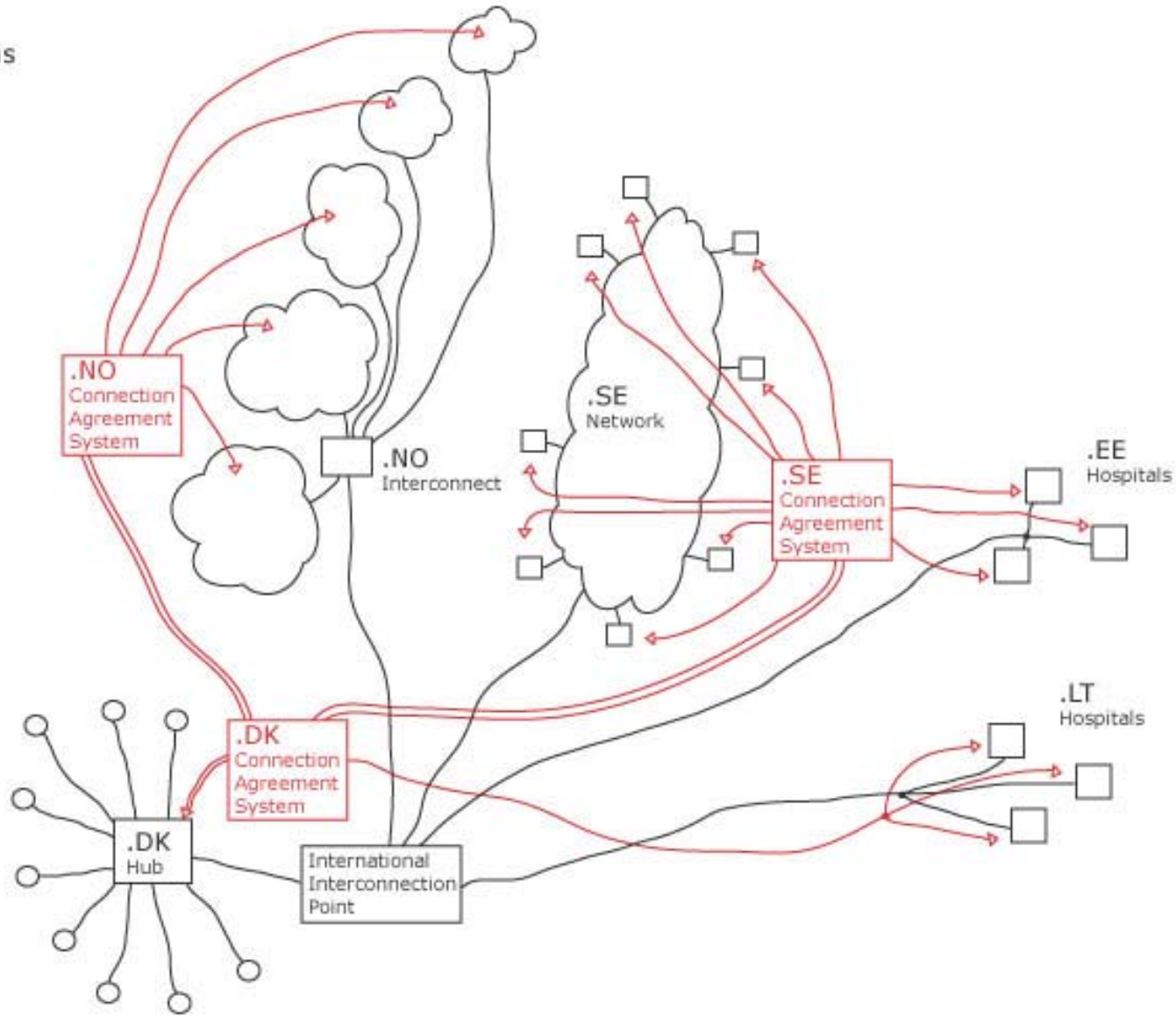
- The price of passing EDI and XML messages by VANS operators dropped from € 0,30 to € 0,03 within the first year
- The national health portal is based on this network
- A lot of the barriers inhibiting collaboration are gone
- Cheaper, safer, more secure and better documented network usage
- A more efficient market for service providers
- The network compensates for shortage of specialists

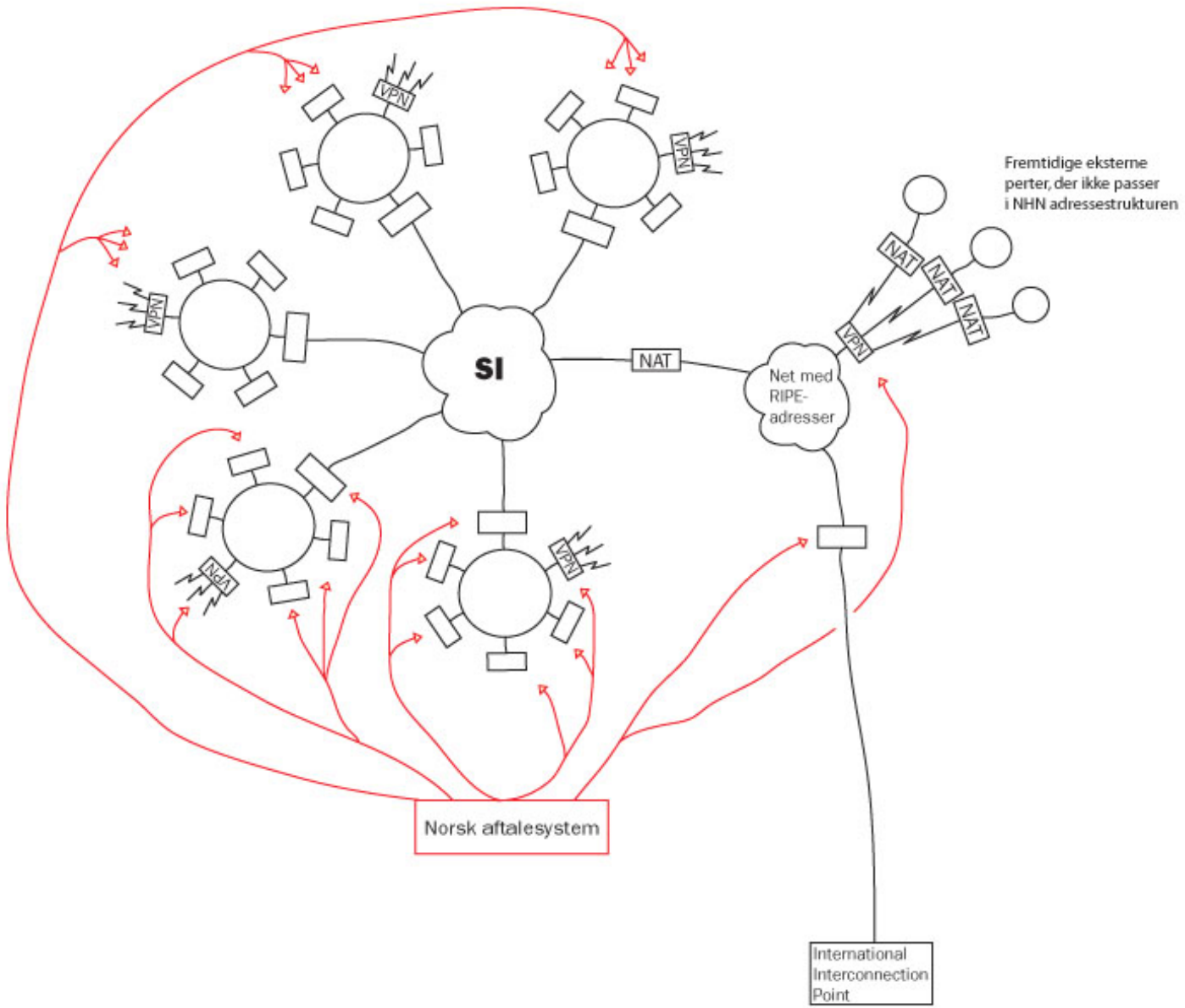
Works on top of different network architectures

- Where all traffic passes a central hub (Denmark)
- Where there is a separate network for the whole health sector (Sweden)
- Where the network is a cluster of clusters (Norway)
- It may also be applied when connecting remote hospitals (Lithuania, Estonia, Slesvig)

Networks and connections are shown in black

Access control is shown in red




VPN
VPN
VPN
VPN
NAT
SI
NAT
Net med
RIPE-
adresser
Fremtidige eksterne
perter, der ikke passer
i NHN adressestrukturen
NAT
NAT
NAT
VPN
VPN
Norsk aftalesystem
International
Interconnection
Point

The Health Care Network provides:

	Hospitals
Basic Internet connectivity	No
Video conferencing	Yes
Collaboration tools	Yes
Lambda networking	Not yet
IPv6	If needed
Roaming services	Yes
CERT and security	Yes
GRID and Scientific Computing	Yes
Media Libraries	Yes

Have we now solved all problems?

YES – National Health Care networks can now be created from regional ones in an easy and inexpensive way

YES – We can now manage the increased complexity of the explosion of many types of connections between organizations

YES – Trans-national networks can be established with preserved security

YES – Local security administrators can let their users do the administration and documentation of their security components

NO – Network interoperability does not guarantee working interoperability of services

NO – The present system does not offer any means for identity management of users (yet…)

Health Care Network Status November 2006

- In Denmark, regular operation since May 2005.
- Swedish Healthcare network connected
- Norway is starting pilot project
- Partners in Baltic eHealth (an E-Ten project) are connected now, using the Danish system – and then moved to the coming natíonal systems when they are in place
- Many countries have expressed interest
- An EU-project for the proliferation of Health Data Networks is being prepared

What will it take to do this in other countries?

- The national or regional health authority must sign an agreement with MedCom, in order to get the connection agreement system **for free**
- It is written using open source tools and documented in english
- Equipment for € 20.000 (some servers and routers)
- Adaptation to the local health care network architecture (in the order of € 100.000)
- A national team supporting and proliferating the network

What will it take to do this as part of a health-grid project?

- Include MedCom and UNI•C in the project and you will get the connection agreement system **for free** for the duration of the project
- It is written using open source tools and documented in english
- Equipment for € 20.000 (some servers and routers)
- Adaptation to project infrastructure (in the order of € 100.000 or less)
- Supporting and proliferating the network will be handled by the project

An opportunity for NRENs in Europe

- NRENs have the skills and the attitude
- Still a bit too complicated for a telco and too big for many system integrators
- This can be generalized to all handle all sorts of private connections through your network and other networks - ”***ultra-lightweight lambdas***”
- The main growth in network traffic will not happen on the open internet
- It we wait too long, someone else will do it!
- And they will not be using our network and our services

The Health Sector is fine, but could we generalize this?

- General internet traffic growth have decreased in the the last 2-3 years
- Almost all handling of data is potential network traffic
- For instance: Storing scanner images onto a centralized storage facility, using the network, is faster cheaper and more realiable.
- The Danish Health Data Network doubles every six months (for the last year)
- Data volumes (ie. potential network traffic) is growing rapidly (doubling every year or faster)
- Actual network traffic is not

Why?

…Because of lack of infrastructure

- Storage and computing facilities
- Network capacity
- **Security infrastructure that allows private network traffic to stay private**
- **Security infrastructure that allows the communicating organizations to preserve integrity**

If we provide the necessary infrastructure, we get the potential network traffic back on the network!

The connection agreement system can also be used by the user community in general as a precursor for lambdas

Defining a point-to-point closed connection

- Is not a lambda
- Only runs IP
- May not even have fixed QoS

But

- Helps users test and demonstrate a need for real lambdas
- It exists today, is simple to deploy and generates connections within the hour

As a future development, the connection agreement system can even be used as a user interface for users to define lambda connections themselves.

Strategy homework for next time:

- Will you provide a facility for user-managed closed circuits in your network?
- Or will you rather let someone else do it?
- Do you need the growth in traffic volume and extra funding that such a facility will cause?

If you need inspiration for this, call on us at UNI•C, and join the coming EU-project.

Despite my limited knowledge about your network, I dare speculate…

Why could the connection agreement system be relevant in an NHS context?

- **Even if your network is closed and covers all relevant parties, a network of your size must have some firewalls internally**
- **Management of internal firewalls within the network**
- **There are always some parties that are external, and yet they still need to be connected: Private hospitals, GPs, service providers, independent labs, home care, …**
- **Managing connections abroad**
- **Generating network and security documentation**
- **… ?**

The proposed EU-project: HDN.eu

- 10 countries or major regions in Europe
- Deploying the connection agreement system
- With co-funding from the EU under FP7
- Total budget 1.5M€
- Consortium final by new year
- Already expressed interest: Sweden, Norway, Iceland, Wales, Holland, Serbia (and Denmark).

Health Data Networks across Europe

Do you want want to join?

martin.bech@uni-c.dk