



## VALENCIENNES HOSPITAL COMPLEX : AT THE HEART OF INFORMATION SECURITY

To ensure that its information system opens up successfully to general medicine, the hospital complex deploys NETASQ solutions. On a typical day, the IT team has to manage around 2000 nodes, 60 networks and 20 sites.

- STAKES SPECIFIC TO HOSPITALS
- A NETWORK THAT EVOLVES THROUGH ADAPTED SECURITY SOLUTIONS
- CUTTING COSTS BY SIMPLIFYING ADMINISTRATION
- VISIBLE CLIENT BENEFITS

### Interview with Frédéric André IT Department Manager at the Valenciennes Hospital Complex

#### STAKES SPECIFIC TO HOSPITALS

Like any large hospital, the Valenciennes hospital complex encounters the same frequently-occurring sets of problems in managing its network, and must in addition to that, take into account new demands for the openness of its information system to general medical practice.

*“The basic issue at hand is the opening of the hospital network to the general public, and the political stakes and French government regulations have worked towards pushing this new deal,”* stated Frédéric André.

General practitioners need to access their patients' health files and the first step is to send them reports on radiology or operations. The Valenciennes hospital complex has followed the national trend in applying the concept of shared medical files. French government regulations will soon expect healthcare networks to contribute to DMP, or shared medical file scheme.

#### CUTTING COSTS BY SIMPLIFYING ADMINISTRATION

Electronic Document Interchanges (EDIs) between general practitioners involve the setup of a global and comprehensive security policy.

This security plan not only takes into account the hospital's internal security but later changes as well.

*“On top of mere intrusion prevention technology, NETASQ also possesses the right know-how that allows us to optimize the use of our security solution.”*

*“A cluster configuration on a NETASQ F2000 firewall has been implemented with a large number of network adapters in order to partition the different types of remote access or different departments,”* said Frédéric André. This security policy enables a fully secure interconnection with the network of the SIIH (Inter-hospital information technology syndicate), which federalizes the 37 hospitals in the Nord Pas de Calais region.

*“The hospital comprises a campus and remote units, therefore we had to partition them with DMZs. As for the usual problem of internal security, we cannot be satisfied with just a “fortified castle” policy. The policy today is based on different points: mail servers, web servers, file servers, application servers and mobile workstations. We have tools which are not necessarily the same for each type of technology, thus enabling us to distribute risks,”* explained the IT department manager.

As for NETASQ solutions, the hospital complex has been deploying them for more than three years now, and has activated several features. The firewall and intrusion prevention functions were of course among the first few, as well as IPSec VPN for interconnecting external networks in total confidence. Features such as URL filtering and antispam came along to complete the solutions.

For the administration of its UTM appliances, the IT team uses NETASQ's administration tools. *“The daily use of these tools is made even easier with the push technology applied to its alarms. These alarms, raised at regular intervals, do not interrupt the normal work rhythm. Furthermore, the centralization of information and control panels enables the second type of analysis – assessing the events that take place.”*

Frédéric André estimates that the hospital has saved considerably on administration costs since *“the concepts of push technology and centralized control panels precisely reverse the need for someone to constantly monitor the firewall and other security tools. The simplicity of the user interface means there are no tasks to subcontract and only three employees are needed to carry out administrative tasks.”* Mr André also confided that the hospital has indeed seen substantial savings from the fact that basic administrative tasks are no longer subcontracted.



## A NETWORK THAT EVOLVES THROUGH ADAPTED SECURITY SOLUTIONS

The Valenciennes hospital complex boasts one of the most powerful networks in the international hospital community.

The best solutions have been sought to provide users with the highest satisfaction – a 10-gigabit framework, quality of service and VLANs.

IP telephony has also been integrated in the hospital's communications system, which will be deploying Wi-Fi networks in 2006 in order to meet the needs for mobility with the emergence of new software for hospitals.

Despite the impressive security configuration, Frédéric André remains aware of the effort that goes toward maintaining an optimal level of security. *“The security policy regarding external connections consists of making regular vulnerability checks and working on neutralizing the risks. Secondly, internal users need to be instructed on computer, the definition of a computer account, and the rights and responsibilities of a hospital employee.”*

## VISIBLE CLIENT BENEFITS

- ! UTM solutions provide a wealth of features
- ! A stable platform reduces the number of administrative tasks and the expenses incurred.
- ! Time is saved with the openness and user-friendliness of the administration software
- ! The frequent use of the administration tools is made easy with the intuitive user interface which enables easy distribution of resources without additional cost.

## VALENCIENNES HOSPITAL COMPLEX

- 1 884 beds and observation wards
- 26 hemodialysis stations
- 325 doctors
- 3 251 employees
- 150 000 patients in consultation
- 60 000 A&E admissions
- 3 700 emergency and resuscitation cases

With a budget of almost 250 millions euros, the Valenciennes Hospital Complex is the center of healthcare development in the southern half of France's Nord region (800 000 inhabitants) after Lille's University Hospital complex.

- Configuration :
- 2 NETASQ F2000 appliances in a cluster

*“For more than three years now, we have valued NETASQ's proactivity both on updates and on after-sales service,”*

**Frédéric André**  
IT Department Manager

Such a solution goes perfectly in line with the security policy already in place and does not require any radical change.

## About NETASQ

NETASQ, the leading European manufacturer of professional internet security appliances was founded in Villeneuve D'Ascq (France) in 1998. The company designs and markets UTM (Unified Threat Management) solutions which combine application and network firewall functions, VPN and content filtering with a unique real-time intrusion prevention technology – ASQ (Active Security Qualification). NETASQ has full control of its proprietary ASQ technology.



**NETASQ**  
3 rue Archimède 59650 VILLENEUVE D'ASCQ  
Tel : 03 20 61 96 30 – Fax : 03 20 61 96 39

[www.netasq.com](http://www.netasq.com)