



### About INM

The first organization in a German-speaking university with a focus on teaching and researching emergency medicine and medicine management was founded at the turn of the year 2001/2002 when the Institut für Notfallmedizin und Medizinmanagement (INM, Institute for Emergency Medicine and Medicine Management) was established as an interdisciplinary clinical organization at the Munich University Hospital by the Bavarian Ministry for Science, Research and Art. The research activities take up the core role in addition to teaching and furnishing reports – including some for the Bavarian state government. This research work involves the analysis and assessment of high volumes of patients' data, so protecting this is a matter of the utmost priority. This can only be guaranteed by a security solution that meets the highest standards.



### Barracuda NG Firewall Cost Efficiency at a glance

- Extendable Barracuda NG systems offer companies sustainable investment protection.
- Unique management functions allow for quick and efficient roll-outs.
- Central management lets you save significant time and effort.
- Unique license and appliances/server hardware combination lets you achieve a maximum of flexibility and cost optimization.



## Institute for Emergency Medicine and Medicine Management

Sensitive information protected by Barracuda NG Firewall

### Sensitive data must be protected

An essential element of the scientific work at the INM is storage and processing of person and patient-related information. Very tight legal stipulations defined by the Bavarian and Federal Data Protection Acts have to be adhered to when dealing with this sensitive data. All data protective measures must therefore stand up to an intensive discussion and examination with the controller for data protection at the University Hospital in Munich. It soon became clear to those responsible for IT at the Institute that the existing firewall solution - a pure packet filter solution - could no longer satisfy the current technical security requirements under the existing conditions. The four-man IT department at INM managed by Dr. med. Lazarovici began searching for a suitable alternative.

### Core requirements: More security, higher availability, greater efficiency

The IT Team initially defined the core requirements for a new solution at the beginning of the evaluation phase. The following criteria had to be fulfilled:

1. Increasing security standards: In addition to meeting the strict data protection law stipulations, an effective solution was required to counter the diverse attack attempts and malicious code activities. It was clear at this point that the route which the Institute for Emergency Medicine had to follow was to move away from a pure packet solution and onto an application level firewall.
2. Secured access to the Institute's network via VPN: The 30 full-time employees and their external colleagues should have easy access from outside onto the Institute's network, without compromising the security.
3. Increasing failsafe security: The new system should have a redundant concept. Several physical computers in distributed premises should be used here.
4. The new solution should be managed efficiently and centrally and also be easy to extend.

### One university – two networks

A further challenge was posed by a network topological feature of the overall system and embedding the INM network respectively into the overall University Hospital network. The hospital has two networks: The network for Science and Research and the network for Medical Care Provision. Hospital patients' data is stored and processed using the latter, i.e. this is where laboratory results can be accessed for example. This network is protected by its own firewall run by the hospital's computing centre. However, for a long time the Science and Research network protection was insufficient, apart from blocking the file sharing port.

### Reliable partner at hand

Following an intensive evaluation phase, Dr. med Lazarovici's IT department decided in favour of using a Barracuda solution. The Institute required a solution that would reliably guarantee that communications could continue running, even under difficult circumstances. The requirements also covered administrative efficiency increases with adapted management concepts. The Barracuda NG Firewalls were clearly the best solutions in all areas.

## About Barracuda NG Firewall Network Security

As the most successful attacks mounted today are within the network, a single remote access link with an unsecured external PC or laptop is often sufficient to allow hackers and malicious codes to open a back door into the company. There are also additional hazards that arise as a result of intentional or unintentional misconduct by some employees. This threat cannot be mastered with perimeter protection alone, because attackers are already behind the network limits. Crucial business processes run smoothly thanks to multi-gigabit firewall performance and integrated bandwidth management. By combining a Stateful Inspection Firewall with Intrusion Prevention, Denial of Service Protection, intelligent application-selective bandwidth and multipath management plus VPN technology, guarantee constant availability and protection. This is exactly what Barracuda is delivering with NG. Protection is no longer limited only to the perimeter and branches, but extends to all sensitive network areas. Flexible deployment and support for virtualized environments is crucial for successful realization of clean bit structures in your LAN.

## Smooth roll-out under extreme conditions

The implementation of the Barracuda NG Firewall ran smoothly, despite some specific special issues which were inherent to the project. The transition to Barracuda NG Firewall took place simultaneously with a move to new premises by both the Institute and the computing centre. And yet, the entire system had to remain constantly accessible and available throughout the entire transition phase.

It was inconceivable that the system be down for a period of several hours, because on the one hand, employees and students work continuously with the Internet and on the other, a high number of web servers was hosted in the Institute's computing centre, including the main server for teaching at the faculty of medicine.

The old solution was still in operation while the new system was initially activated for selected parts of the network. Some VPN clients were also assigned to some testers. Since no problems worthy of note arose during this test phase, the new system was transferred to the entire system in one major conversion process. This took place with a downtime of just a few minutes. The entire process, from the conception to the final transition, took three weeks.

## Positive résumé after two years

The Institute for Emergency Medicine and Medicine Management at the University Hospital in Munich today guarantees the secure availability of critical data and applications with redundantly designed Barracuda NG Firewalls, which are managed centrally via a Barracuda NG Control Center. Worthy of particular mention is that in comparison to the former gateways there are more individual customization options for the VPN access, a performance in gigabyte range as well as easy options for adding additional interfaces.

## About Barracuda Networks Inc.

Barracuda Networks Inc. built its reputation as the worldwide leader in content security appliances by offering easy to use and affordable products that protect organizations from email, Web and IM threats. Barracuda Networks has leveraged its success in the security market to offer networking products that improve application delivery and network access as well as world-class solutions for message archiving, backup and data protection. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are amongst the 100,000 organizations protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, Calif. Barracuda Networks has offices in 10 international locations and distributors in more than 80 countries worldwide. For more information, please visit [www.barracudanetworks.com](http://www.barracudanetworks.com).

**“The solution runs stably. Both the firewall and the VPN ran reliably from the outset. We would definitely decide in Barracuda's favour again.”**

**-Dr. med. Lazarovici,**  
Head of IT department at INM