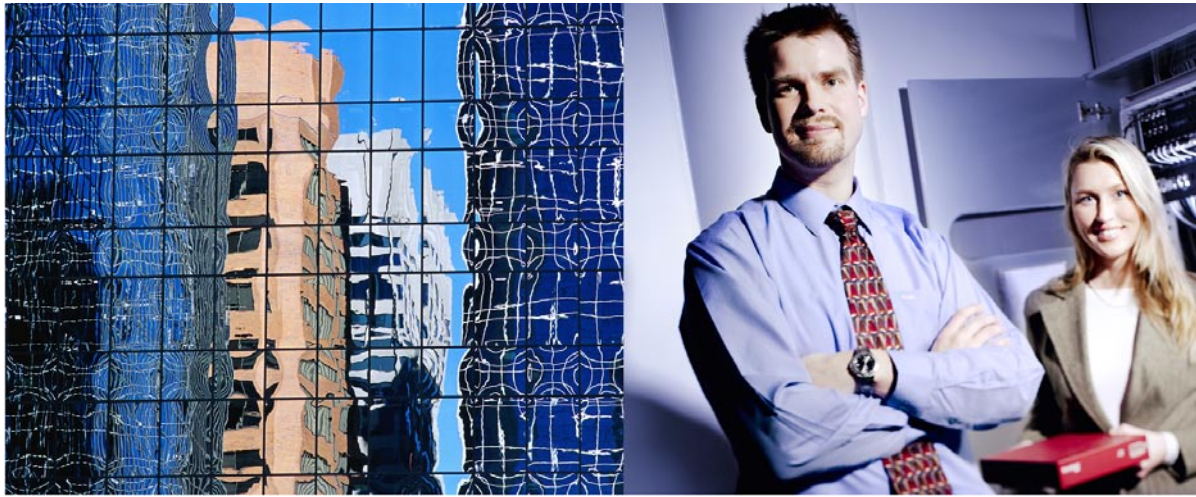


**STONESOFT**



**Case Study- RWTH Aachen**

---

## **Security as far as the eye can see**

---

# Security as far as the eye can see

## StoneGate Firewall Deployed at RWTH Aachen Computing and Communication Centre

The computing and communication centre at RWTH Aachen is the central hub and pivotal point for the university's IT services. It is responsible for providing services, user support and most important, for ensuring security. As the first fortress against attack, RWTH has particularly rigorous demands when it comes to issues of security and performance.

Sceptics only need to take a glance at their firewall log file. Barely a minute passes without an external hacker trying to find an open port or starting point to break into the network over the internet. Assaults are automated, with small company or private networks not requiring further attention by the attackers. With large, publicly known networks, however, things look very different. Universities and research establishments in particular are the victims of large-scale assaults and denial of service (DoS) attacks.

The Rhine-Westphalia Technical University (RWTH) Aachen knows a thing or two about this, and Andreas Schreiber, head of network operations at the RWTH data centre, has a wealth of experience: "Often the connection to the internet and German research network (DFN) would go down due to a denial of service attack. Under high load, our previous firewall – a system based on a high-end server – would grind to a halt, despite adequate hardware."

### Huge responsibility of the data centre

This was unacceptable for the RWTH computing and communication centre, which acts as the central facility of RWTH Aachen, providing resources and services to institutions as well as to the university's staff and students. The staff, consisting of 5,000 people, relies on the availability of services and security in the network, while almost 30,000 students are end-users. The data centre's tasks are extremely diversified, ranging from planning and operating the infrastructure, to providing centralised data and processing facilities and the services which run on them. Virtualisation is used to contribute actively to the development of new, spatial visualisation techniques, while high speed processing is accelerated through parallelisation. "We naturally also plan and operate the university network and develop concepts for pan-institutional solutions wherever IT is concerned," explains Andreas Schreiber.

Collaboration with similar establishments – such as those found in the framework of the NRW

Resource Association – is also important, both at a regional and supra-regional level. The aim is to build up a statewide competence network, with resources and know-how being provided and shared beyond the boundaries of individual universities. A firewall solution plays a crucial role, especially in this kind of networked environment. Consequently, not only is performance a central criterion, but so are other factors such as user-friendly management of rules and objects. Also, it must be possible to scale the system in order to meet new requirements. Andreas Schreiber and his team were convinced that the former system would not have met requirements in the near future.

### Clear selection criteria

By the end of 2004, it was clear to RWTH that the existing firewall solution could no longer be upgraded effectively. The problems which had plagued Schreiber beforehand together with his detailed knowledge of the old firewall, meant that he knew precisely what he was looking for: "On one hand, we wanted a high performance system which was capable of maintaining connections, even under heavy loading. The complex structures at RWTH further meant that it had to be as simple and straightforward as possible to administrate the firewall and its rules and objects. Naturally, as we plan over the medium to long term, scalability was also an important aspect for us." Schreiber's team began to evaluate vendors and solutions as preparation for the 'real' tests.

As RWTH does not maintain regular working hours with breaks or without productive operations, the new system was subjected to full loading as early as the test phase. Also, because a firewall is exposed to attacks the moment it is connected to the Internet, it must fulfil its protective function entirely from day one. Andreas Schreiber's team knew that the selection process would have to be extremely meticulous because the acid test for the chosen system would begin immediately after its integration into the university environment.

**“The outstanding thing about the StoneGate firewall is that, even under the most adverse conditions it always remains online, even if things are slightly slower than normal.”**

**Andreas Schreiber, head of network operations at the RWTH data centre**

### **Four trials, one solution**

In the end, the number of potential products was whittled down to four prospective solutions. The data centre staff started off by simulating various loading scenarios to get a feel for the performance of the individual products. In doing so, it soon became clear to them that, out of the three commercial and one open source firewall products, only one fulfilled their demands: the StoneGate solution from the Finnish vendor, Stonesoft.

StoneGate contains integrated functions supporting high availability and load balancing – features either not supported by other products or only available optionally at additional cost. Users enjoy a number of direct benefits from load balancing: firstly, the incoming data is automatically distributed over a number of linked firewalls, thereby reducing individual system load to a manageable level; and secondly, redundant firewalls can be entirely removed from the system, with the remaining firewalls taking up the traffic of the disabled system without any down time – an indispensable function for maintenance and upgrades.

### **Critical aspects wanting**

The three other tested firewalls were unable to compete with Stonesoft’s solution. Andreas Schreiber says: “One of the products was too instable, resulting in a number of unexpected crashes, especially when subjected to unusually high load. Another device offered a wide range of functions, which were so complex to install and manage that our administrators simply shook their heads in disbelief. The open source solution just didn’t measure up to our demands in terms of high availability and scalability.” Following intensive testing, Schreiber and his team were convinced: StoneGate from Stonesoft offered the best cost-performance ratio and would be able to fulfil RWTH Aachen’s needs, both present and future. What impressed them particularly was the management of the solution.

A graphical user interface simplified enormously the handling of thousands of rules and objects – something that was even praised by command line enthusiasts. Although the administration tools had been specifically developed for StoneGate, the vendor had integrated open software interfaces, which allowed Andreas Schreiber to migrate his existing, firewall data quickly and without difficulties. A self-written script imports – with the help of Stonesoft staff – policy settings, IP addresses and other security-relevant data into the StoneGate rules engine. “Because we didn’t have to enter the data again, we were not only able to save a lot of time, but also avoid an extremely error-susceptible process. Errors in input data can

never be ruled out with such a large volume of information,” Schreiber continues.

Despite the complex system environment with around 200,000 IP addresses to be protected, the installation was completed in an unexpectedly short time. Schreiber estimates a total of around three ‘man-days’ from start to finish – including preparations for the hardware platform.

### **Installed and good**

StoneGate firewalls handling incoming and outgoing data traffic are now running in the RWTH Aachen data centre. The system has meanwhile proven itself under real-life conditions and already had to master a few thorny situations.

“The outstanding thing about the StoneGate firewall is that, even under the most adverse conditions, such as a denial of service attack, it always remains online, even if things are slightly slower than normal,” says Andreas Schreiber. “Under similar conditions, where other products capped the link very early on, our Stonesoft system simply kept on going,” he continues. Even if the current load capacity has almost reached its limit, Schreiber is not concerned. This is because StoneGate not only offers horizontal scalability through parallel systems, but also potential for vertical improvements. Hardware upgrades can be carried out easily and without interrupting the firewall service, with migrations being completed in the shortest possible time.

### **Minimum effort, maximum performance**

Schreiber’s staff is also enthusiastic about the new firewall, with the uncomplicated administration receiving praise in particular. With the exception of a short briefing in StoneGate-specific functions, firewall experts were able to start working with the solution.

Consequently, little time was lost on training, thereby leading to lower overall costs than for a solution that can only be administrated after extensive training and subsequent certification. Administration costs have meanwhile fallen further because the Stonesoft management software supports a wide range of options for automating tasks. As a result, the staff is no longer burdened with routine tasks, leaving them more time to focus on security-relevant issues. The firewall, for example, now adapts the anti-spoofing functionality automatically to the routing rules, so that administrators no longer have to spend time on this.

Administrators were also pleasantly surprised by StoneGate’s ability to change the rule base and even software versions during productive operations. In doing so, the rule base benefits from

**“What impressed them particularly was the management of the solution.”**

**Andreas Schreiber, head of network operations at the RWTH data centre**



seamless integration into the operating system, which means that a reboot is not required in order to load rules or update lists. Because changes become effective instantaneously, this is an enormous advantage for security in an environment where updates may have to be made immediately – for example if a new virus has been discovered exploiting specific ports. Also, the ability to install software and operating system updates without taking the firewall cluster offline has long been an item on Andreas Schreiber’s list of wishes. “It’s really convenient to be free of the constraints of service slots when maintaining or optimising the firewall. This remote update functionality saves us a lot of time and naturally also boosts user satisfaction. Ever since installation of the StoneGate firewalls, we haven’t had to disable a single port.”

Without a doubt, the long and meticulous firewall selection process was worthwhile for RWTH. If Andreas Schreiber and his team have their way, future extensions of the RWTH security infrastructure will also be based on the StoneGate system. The next phase will involve improvements to the filtering functionality, a move that will help protect the university network from new, and potential threats. Preserving the openness of the system for research and education is a challenge, which Andreas Schreiber has well in hand, thanks to StoneGate’s finely tuneable policies and rule engine.

### **About RWTH Aachen**

With almost 30,000 students in nine faculties, RWTH Aachen, the technical university of the Rhineland-Westphalian city of Aachen, north-west Germany, is widely recognised as one of Europe’s most distinguished technological seats of learning and also counts as the region’s principal employer. While RWTH Aachen has a strong bias towards science and engineering, it also offers an extensive range of curricula in the fields of economics, humanities and medicine. As one of the central facilities of RWTH Aachen, the Center for Computing and Communication offers resources and services for institutions, staff and students of the university.

[www.rwth-aachen.de](http://www.rwth-aachen.de)

**“This remote update functionality saves us a lot of time and naturally also boosts user satisfaction.”**

**Andreas Schreiber, head of network operations at the RWTH data centre**



## Stonesoft Experience

Stonesoft Corporation (HEX: SFT1V) is an innovative provider of integrated network security and business continuity. Stonesoft is a global company focused on enterprise level customers requiring advanced network security and always-on business connectivity with low TCO, best price-to-performance ratio, and highest ROI.

StoneGate™ Platform unifies firewall, VPN and IPS, blending network security, end-to-end availability and award-winning load balancing into a unified and centrally managed system for distributed enterprises. Founded in 1990, Stonesoft Corporation has corporate headquarters in Helsinki, Finland; Americas headquarters in Atlanta, Georgia; and Asia Pacific headquarters in Singapore.

## The StoneGate Platform

The StoneGate Platform lowers the risks of doing business in a digitalized world. StoneGate appliances and software provide secured, optimized, and resilient connectivity for converged services, while preventing damage from attacks. With the help of unified management you can cost-efficiently manage and monitor the security and connectivity in your network.

### Secured, Optimized, and Resilient Connectivity

With StoneGate Firewall/VPN, you can connect your offices with each other reliably and fault-tolerantly using Site-to-Site VPN, ISP Multi-homing with Multi-Link VPN Technology, Firewall/VPN and IPS Sensor Clustering and Load Balancing, Server Load Balancing, and Quality of Service and Bandwidth Management

### Preventing the Damage from Attacks

StoneGate guards your network with StoneGate Firewall and with StoneGate IPS. StoneGate Firewall enforces your security policy, prevents denial-of-service attacks, and drops malicious http traffic. StoneGate IPS stops attacks and non-authorized traffic as well as protects unpatched servers before they are updated.

### Unified Management

The StoneGate Management Center delivers an innovative and holistic approach for role-based administration through a single, centralized management system. Forming the heart of the StoneGate Platform, the Management enter provides unified tools for Security Enforcement, for Security Surveillance, and for Systems and Data management.

# STONESOFT

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

#### Stonesoft Corp.

Itälahdenkatu 22 A  
00210 Helsinki  
Finland  
tel. +358 9 4767 11  
fax. +358 9 4767 1234

#### Stonesoft Inc.

1050 Crown Pointe Parkway  
Suite 900  
Atlanta, GA 30338, USA  
tel. +1 770 6681 125  
fax. +1 770 6681 131

#### Stonesoft Corp.

90 Cecil Street  
#13-01 Carlton Building  
Singapore 069531  
tel. +65 6325 1390  
fax. +65 6325 1399

Copyright 2006 Stonesoft Corporation. All rights reserved. All specifications are subject to change. The products described herein are protected by one or more of the following US and European patents: US Patent Nos. 6,912,200, 6,650,621 and 6,856,621. European Patent Nos. 1,065,844, 1,289,183, 1,289,202, 1,326,393 and 1,259,028; and may be protected by other US patents, foreign patents, or pending applications. Stonesoft, theStonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. All other trademarks or registered trademarks are property of their respective owners.