STORMSHIELD

CUSTOMER CASE STUDY

# Enhancing internal network security: a priority for local authorities

**PUBLIC INFRASTRUCTURE**

In an increasingly digital world, local authorities have modernised to enable them to offer new connected services. But this connection entails two risks: exposing even more of the confidential information that local authorities have to process, and having these services compromised or disrupted by malicious parties.

This raises the issue of enhancing the security of their IT networks, to ensure continuity of service and protect citizens from cyberattacks. The above considerations underpinned a decision taken by a community of municipalities in Germany with a population of 200,000.

## Critical infrastructure and sensitive information requiring protection

To manage and administer all the community's network services (electricity, gas, drinking water, district heating, etc.) and its public infrastructure (public lighting, car parks, municipal swimming pools, transport, etc.), the community of municipalities set up a dedicated company in which it holds a 100% stake.

In addition to the day-to-day implementation and operation of the infrastructure and services provided, a web portal is available to the public, enabling them to find all the information they need and make certain requests using web forms.

Given the critical nature of its activities and the data that passes through and is stored on its Information System, it was becoming imperative for this company to enhance its level of security.

## Enhanced security levels

The customer therefore decided to add a second firewall, in addition to its current equipment, to provide dual protection for its internal IT network.

Because of its "critical" rating under the KRITIS regulation issued by the German Federal Office for Information Security (BSI), this customer has a legal obligation to adequately secure its information system, which is essential to the smooth running of public services. This dual protection is one of the enhanced security measures implemented to ensure business continuity.

In choosing this new equipment, the customer wanted to avoid using the same manufacturer, thus making the task more complex in the event of an intrusion attempt, as bypassing two different technologies would by definition be more difficult.

Advised by its integrator, Phalanx IT, it selected the Stormshield Network Security solution; or, more specifically, a cluster of SN6100 firewalls and the Stormshield Management Center centralised management console.

In addition to the quality and effectiveness of these two solutions, the decision to work with a European player whose solutions are recognised and certified at the highest level was also a determining factor.

# THE SOLUTIONS USED

→ SN6100
→ Stormshield Management Center

## Performance and functionality tailored to customer needs

Following deployment to the customer's complete satisfaction by Phalanx IT's certified teams, it now has a Next Generation firewall cluster that meets all its requirements in terms of performance and functionality.

Designed for large-scale critical infrastructures, the SN6100 offers a throughput of 170 Gbps and the highest port density on the market – essential in planning for future changes in network infrastructure security requirements.

The customer also enjoys high availability and enhanced security via network segmentation and the implementation of strict rules, enabling it to better control the flow of traffic to the most critical areas. The SN6100 also features redundant components (power supply and ventilation), to avoid any risk of failure.

In addition, the customer has implemented the Stormshield Management Center centralised management solution. This tool enables it to streamline its firewall supervision, configuration and maintenance tasks.

As well as saving time for administrators and minimising the risk of error, this tool – which is specially designed to meet the needs of multi-site networks – follows the same philosophy of anticipating a future need for network scalability.

STORMSHIELD