Organization
Customer: FILIADATA GmbH
Site: https://www.dm.de
Industry: Retail (analytics)
Headquarters: Karlsruhe, Germany
Employees: 500

Challenges
FILIADATA was faced with SSL traffic that had increased almost sixfold within a few years – from 10 to almost 60 percent. This encrypted web traffic was impacting performance on the secure web gateways, which was hurting IT operations at its 3,300 retail stores.

Solution

- Symantec Advanced Secure Gateway
- Symantec ProxySG S series
- Symantec Content Analysis System

Benefits

- Filters and protects web traffic better
- Reliably intercepts malware and potentially dangerous files and URLs
- Reduces operating costs by 30 to 40 percent by consolidating from four to two appliances

Symantec Strategic Partner
LEITWERK AG

Next Generation Web Security

Symantec Advanced Secure Gateway in dm-drogerie market

When the Secure Web Gateways at FILIADATA GmbH reached their performance limits, the IT team decided to replace the systems with the new, seamlessly integrated, Advanced Secure Gateway from Blue Coat (now part of Symantec). The platforms, deployed in spring 2016, have proved to be a winning choice, not only due to their high performance, but because they also provide the team with an array of innovative new security features.

FILIADATA is a fully owned subsidiary of dm-drogerie markt GmbH, responsible for IT infrastructure operation and security within the group. In two redundant data centers, more than 500 employees develop, operate, and manage critical IT services (including 4,300 PC workstations) for 3,300 dm stores in 12 countries. The scope of activities includes IT consultancy and project management, architecture design and development, and system administration and support.

Given the growing number of business-critical applications – and the increasingly close integration of IT with business processes – the topic of network security is becoming increasingly important at FILIADATA. As a result, the IT service provider maintains a powerful security infrastructure that protects both corporate resources, as well as remote dm stores, from all angles.

Secure Web Gateway as a key component

The topic of web security plays a key role in FILIADATA's security strategy. After all, each day several thousand users go online via the dm network. These users range from headquarters employees and branch managers on their notebooks through to area managers, distribution center staff and back office employees. "In 2013 we installed two Blue Coat ProxySG 900-20 appliances to prevent colleagues from unknowingly infecting the network with malware while surfing. These allowed us to check web access on a group-wide basis, and enforce our policy in all dm stores", explains Christian Stäblein, Area Manager at FILIADATA. "The ProxySG platforms support highly granular URL categorization, which is updated with the latest threat information in real-time. This has made it easy for us to achieve the high security level we set as our target."

Using category-based content filtering, the Secure Web Gateway enabled the team to thoroughly analyze web traffic for potentially malicious content, and intercept web-based malware reliably. The appliances, installed as a cluster in "active mode", were each designed for up to 9,000 concurrent connections. This initially appeared to be sufficient capacity for long-term operation, despite the constant global increase in web traffic.

> The ProxySG platforms support highly granular URL categorization, which is updated with the latest threat information in real-time. This has made it easy for us to achieve the high security level we set as our target.
>
> —Christian Stäblein,
> Area Manager, FILIADATA

Increases in SSL traffic impair performance

However, the gateways already reached their performance limits after about two years. Initially this was only during peak loads, but shortly afterwards it also happened during everyday operation. The team first suspected that the performance issues were due to the increased volume of group internet traffic, not least as dm had recently adopted a number of new web-based applications. This seemed to be the likely cause the congestion in the ProxySGs, but the suspicion remained unconfirmed. However, traffic analysis carried out in collaboration with Symantec and Leitwerk AG, a system integrator, pointed in another direction. They showed that the percentage of SSL traffic in the dm network had increased almost six fold within a few years – from 10 to almost 60 percent – and it was encrypted web traffic handling that had overburdened the gateways.

"In recent years, increasing numbers of major web service providers – especially Google – have begun to encrypt their online communication," explains Stefan Kratzer, Leitwerk Branch Manager. "This of course led to a huge increase in SSL traffic, which also became noticeable on the Secure Web Gateways. This is because the ProxySGs must first decrypt encrypted traffic, and then analyze, re-encrypt, and forward it. This is an enormously laborious process for the appliances, which went beyond the performance levels for which they were originally scoped."

FILIADATA was thus faced with a decision. "We could have stuck with the two ProxySGs. However, to do this, we would have had to disable SSL inspection, and simply forward encrypted traffic," explains Stäblein. "Given the countless viruses and threats concealed in SSL and TLS traffic these days, this was simply not an option for us. So we decided to collaborate with Symantec and Leitwerk to find a reliable solution."

Advanced Security Gateway makes a good impression

At first, Symantec provided FILIADATA with a larger ProxySG S400 as an emergency solution and for use in an initial trial. This system coped very well with the increased traffic volumes. However, before they could proceed with the project, a second alternative presented itself in the shape of the new Symantec Advanced Secure Gateway.

Advanced Secure Gateway, introduced in autumn 2015, combines the classic ProxySG appliance performance capabilities with the Symantec Content Analysis System's advanced inspection and anti-malware functionality. In this way, they not only filter and protect web traffic, but also reliably intercept malware and potentially dangerous files and URLs. For optimal detection accuracy, they support two dedicated malware engines, white- and blacklisting, static code analysis, and tight integration with malware sandboxing solutions.

> In Advanced Secure Gateway, we found a solution that meets our requirements in scope, scalability, and security. … For us, security is becoming ever more important.
>
> —Christian Stäblein, Area Manager, FILIADATA

Consolidation from four to two appliances

"The new ASGs proved to be a very good solution – not only as high-performance successors to the existing ProxySGs, but also because they could be very easily integrated into the data center due to their common architecture," explains the Large Account Manager at Symantec. "The integrated malware protection also allowed FILIADATA to replace their ProxyAV platforms, which were due to end their life cycle. It therefore became apparent that they could consolidate from four to two appliances, and reduce operating costs by 30 to 40 percent."

After the trial confirmed their initial assessment, the systems went live in Karlsruhe in spring 2016, and have proven their worth since day one. Christian Stäblein therefore draws a positive conclusion from the project. "Although our system performance issues caught us out at the start, the project itself worked out very well. In Advanced Secure Gateway, we found a solution that meets our requirements in scope, scalability, and security. We are still a way off from achieving the full potential of the systems, but will thoroughly test the new features. For us, as everywhere, security is becoming ever more important".

Advanced Secure Gateway overview

The Advanced Secure Gateway is a Secure Web Gateway, based on the ProxySG S series hardware, and combines ProxySG and Content Analysis System functionality in a single appliance. The combined solution thus allows companies to check and protect their web traffic, and reliably intercepts all types of known and unknown malware and advanced threats. The integrated, cost-effective security platform is suitable for business locations of all sizes, including data centers, branch offices, and locations where rack space is limited.

LEITWERK AG profile

The LEITWERK Group consists of LEITWERK AG and its subsidiaries. It is today one of the leading partners of the regional economy for comprehensive IT and communications solutions in Baden and Alsace. At its headquarters in Appenweier and at four other locations in Freiburg, Achern, Karlsruhe and Strasbourg, more than 330 employees support small and medium-sized companies, as well as major international companies, community facilities and freelance professionals.

Symantec™

350 Ellis St., Mountain View, CA 94043 USA | +1 (650) 527 8000 | 1 (800) 721 3934 | www.symantec.com