

Amadeus Hospitality

The hotel IT arm of Amadeus sleeps easy thanks to Fortinet

Case Study

Situation

Trust, reliability and quality of service play a vital role in the hotel industry. Amadeus Hospitality, the hotel IT business unit of Amadeus, a worldwide leading technology partner for the entire travel and tourism industry, expects the same qualities from their IT infrastructure. Following a series of security breaches and data corruption at a number of hotels, Amadeus Hospitality in Germany made the decision to completely re-work their security infrastructure. The result is the deployment of a wide range of unified threat management appliances from Fortinet to provide complete security at the German main office and VPN connections to the branch offices and to date 150 hotels.



Amadeus Hospitality provides thousands of international hotel and catering industry customers with applications for profitable hotel management, worldwide distribution and IT hosting. Due to the multitude of personal data held in hotel IT systems ranging from guest addresses, staff payrolls to customer credit card and bank details, it is vital that Amadeus Hospitality guarantees the hotels and their guests 100% security for this data. Security breaches cannot be tolerated. As the hotels often have no IT staff on site to deal with any issues that arise, they are reliant on Amadeus to be alert to any breaches and take action as necessary.

Deployment:

2x FortiGate-1000A
2x FortiGate-400A
FortiGate-50Bs & 60Bs
FortiAnalyzer
FortiManager

Industry:

Tourism

The need for a complete overhaul of the security infrastructure was first recognized in 2005 following complaints from hotels about virus attacks resulting in server crashes and data loss. The IT staff at the German Amadeus Hospitality realized that their existing firewall – which had been in use for over five years and was limited in terms of performance and features – was no longer able to cope with the increasingly cunning cyber threats and the speed and depth of attacks. In addition, the remote monitoring and maintenance to the hotels via 1300 ISDN call up lines was increasingly slow and cumbersome.

“At Amadeus Hospitality, we make long-term decisions relating to our IT infrastructure. When we came to assessing new security solutions, we had to consider how the security provider was positioned on the market and be sure that the technology would provide us with a fully secured environment and would not only meet the current stringent requirements but also be able to adapt to new security challenges and demands,” said Marcus Schmid, director IT Projects and Services at Amadeus Hospitality.

Solution

Amadeus Hospitality ran a comparative test with three vendors – NetScreen, SonicWall and Fortinet – looking for the solution that would allow a simple and secure network environment. To do so, there were two main issues that had to be solved. First of all, the new firewall platform should offer high performance and add on security features such as virus scanning and intrusion prevention internally and for the hotels and branch offices. Secondly, to replace the ISDN lines, the platform should offer two-way security using VPN functionality. Finally, with the main task of hotels being to concentrate on their guests and not IT issues, ease of deployment and management was also a key criterion. After a detailed analysis of all three solutions, Amadeus chose an infrastructure based on FortiGate™ integrated multi-threat appliances from Fortinet.

“We were impressed by the range of features that Fortinet offers,” says Marcus Schmid. “None of the other firewalls we looked at were able to offer us integrated IPS or anti-virus functionality. Fortinet offered us a complete package. Also, the performance of the Fortinet firewall was second to none.”

Amadeus Hospitality has deployed two FortiGate-400A and two FortiGate-1000A appliances in their headquarters in Vaterstetten near Munich. The FortiGate-1000A appliances are clustered for high availability and provide all the critical security functions – including firewall, anti-virus, anti-spam, web content filtering and IPS - to the core network on which the 130 employees of the German Amadeus Hospitality are connected. The load balancing functionality helps maintain high performance levels and the flexible zoning feature means that Amadeus Hospitality can create separate security policies for internal departments and applications. The two FortiGate-400A appliances serve as the VPN hubs for the remote connections to the hotels served by Amadeus Hospitality. Due to strict SLAs with their customers, these appliances are installed in a clustered configuration. The

hotel business works 24/7 and has the same expectations of the security solution. Also, Amadeus Hospitality in Vaterstetten is not just serving hotels in Germany or Central Europe but 6.700 hotels around the world – in a range of different time zones.

And to date 150 hotels around the world have a FortiGate-50B or FortiGate-60B security appliance installed, which serve as VPN tunnels connecting to the FortiGate-400A appliances in Vaterstetten. Each appliance is equipped with full UTM functionality including IPS, anti-virus, firewall and antispam. Thanks to the VPN connections, the IT staff at Amadeus Hospitality can monitor the hotel appliances and trouble shoot remotely if necessary.

Due to the simplicity of the FortiGate appliances, the installation could be carried out by Amadeus Hospitality IT staff. In spite of the relatively large and widespread installed base, the initial infrastructure was up and running within two weeks. Adding new VPN tunnels with hotels is a matter of an hour or less.

Success

Amadeus Hospitality in Germany is completely satisfied with their solution. The administration efforts for the IT department have been considerably reduced and maintenance is easy, even though the remote security appliances have to be managed centrally by the IT team in Vaterstetten. To improve the transparency, Amadeus recently extended their Fortinet solution by adding FortiAnalyzer™, Fortinet's real-time network logging, analyzing, and reporting tool. This system enables the team to collate and analyse log data from all the Fortinet appliances, giving them a comprehensive view of network usage and security information. As a result, they can create tailored reports on the activity of the appliances for internal purposes or to report connectivity and performance levels back to the hotels.

As Marcus Schmid reports, the hotels have also noticed an improvement and a significant drop in security breaches as a result of the new security infrastructure: "In the past, a lot of our customers had little or no security solution in place. Now they have a complete package and can rest assured that they are safe from hackers and viruses, which may corrupt the integrity of their assets. We in turn appreciate the simplicity and manageability of the infrastructure – and our ability not only to meet our internal SLAs but also guarantee our customers a high quality of service so that they are free to concentrate on their own customer services."

Thanks to the FortiGuard™ subscription services, Amadeus Hospitality can guarantee their customers real time automatic security updates, no matter where they are in the world. This ensures that the hotels can be sure of the highest level of protection around the clock – particularly important in view of the increasing variety and sophistication of internet attacks.

Amadeus Hospitality also appreciates the pricing structure. Fortinet offers a licensing structure per appliance, not per user. Thanks to the scalability of the FortiGate systems, Amadeus can grow their infrastructure without stretching the budget.

To further improve and simplify management, Amadeus Hospitality is evaluating FortiManager™ – a tool to monitor and manage the complete environment at a glance via a web browser.

Marcus Schmid summarizes: "We were looking to create an environment with minimal maintenance and maximum security. We have found Fortinet to have met and gone beyond our needs."

About Fortinet

Fortinet is the pioneer and leading provider of ASIC-accelerated unified threat management, or UTM, security systems, which are used by enterprises and service providers to increase their security while reducing total operating costs. Fortinet solutions were built from the ground up to integrate multiple levels of security protection--including firewall, antivirus, intrusion prevention, VPN, spyware prevention and anti-spam -- designed to help customers protect against network and content level threats. Leveraging a custom ASIC and unified interface, Fortinet solutions offer advanced security functionality that scales from remote office to chassis-based solutions with integrated management and reporting. Fortinet solutions have won multiple awards around the world and are the only security products that are certified in seven programs by ICSA Labs (Firewall, Antivirus, IPSec, SSL, Network IPS, Anti-Spam, and Anti-Spyware). Fortinet is privately held and based in Sunnyvale, California.

CAS179-0508