

DATAQUEST

A DATAQUEST Partner Special

The Business of Infotech

IT CASE BOOK 2009



SECURITY

In Association With

FORTINET
UNIFIED THREAT MANAGEMENT SOLUTIONS

- **Securing the Campus Network**
SIBM
- **Unified Security Solution**
eClerx
- **Securing the Airport Network**
GMR Group
- **Integrated Security Solution**
TAFE
- **Delivering Security**
Cambridge Solutions

Securing the Campus Network

FORTINET
UNIFIED THREAT MANAGEMENT SOLUTIONS



RAJESH B BAGEWADI

SENIOR NETWORK ADMINISTRATOR,
SYMBIOSIS INSTITUTE OF BUSINESS
MANAGEMENT

The Fortigate 800 solution has fulfilled our requirement in terms of user authentication, Internet load balancing, antivirus, Web filtering, firewall, and so on

Results

- Better management of Internet bandwidth through policies
- Network can be segmented into zones and unique policies for each zone created. User authentication with Active Directory
- Easier management of the system through Web console
- Security from multiple threats through antivirus, Web filtering, firewall, IDS/IPS, etc.

Fortinet's solution has helped Symbiosis Institute of Business Management to manage internet bandwidth and create security policies for its gigabit network

Symbiosis Institute of Business Management (SIBM), Pune is counted among the best business schools in India. Established in 1978, it received permanent affiliation from the Pune University in 1996. In 2006, the UGC recognized it as a full-fledged university, and SIBM became part of Symbiosis International University (SIU). Apart from two-year MBA programs for residential students, SIBM offers one-year MBA programs for working professionals and customized MBA programs for corporates.

Need for security

SIBM has a gigabit network with multiple virtual LANs spread across the campus. For securing this network, SIBM decided to deploy an appliance based UTM (unified threat management) product.

"The product had to support the following features: firewall, IDS/IPS, anti-virus, web filtering, spam control, user authentications for Internet, Internet load balancing and failover lease line connections," states Rajesh B Bagewadi, senior network administrator.

A project consultant for the network project listed the criteria for selection of vendor. As a result of this process, Fortinet's products were selected.

Implementation

SIBM decided to deploy Fortigate 800 and FortiAnalyzer. While Fortigate 800 is a UTM appliance, FortiAnalyzer is a dedicated hardware solution that securely aggregates and analyzes log data from the FortiGate appliance.

The FortiAnalyzer appliance accepts and processes a range of log records provided

by FortiGate, including traffic, event, virus, attack, content filtering, and email filtering data. It also provides advanced security management functions such as quarantine archiving, event correlation, vulnerability assessments, traffic analysis, and content archiving. It also provides more than 300 customizable reports, whether scheduled or on-demand. Network administrators thus get a comprehensive and detailed view of network usage and security information, which helps them to discover and address vulnerabilities faster.

With the help of a system implementer, the project consultant and the Fortinet team, the installation and implementation took about a week and did not involve any downtime.

However, challenges came up during installation in Internet network load balancing, failover of Internet and web content filtering, as well as in Active Directory integration.

Managing Network Security

The FortiGate-800 network security system features four 10/100/1000 tri-speed Ethernet ports for networks running at gigabit speeds and four user-definable 10/100 ports that provide granular security through multi-zone capabilities.

The platform has allowed administrators at SIBM to segment the gigabit network into zones and create unique security policies between zones. This helps to manage the Internet bandwidth and user authentication with Active Directory. The system is easy to manage through a Web console and has enabled SIBM to manage Internet usage in a better way through policies. ◀



Unified Security Solution

The deployment of a unified threat management solution from Fortinet helped eClerx completely secure its network and data-center

eClerx provides data analytics and customized process solutions to global clients from its offshore centers in India. Its portfolio of services comprises data analytics, operations management, data audits, metrics management and reporting services

Need for Security in a Rapid-Growth Scenario

eClerx began considering various vendors for security solutions, when its existing UTM (unified threat management) solution exhibited limitations. The organization, and thereby, the network and users were growing rapidly and the security solution seemed unable to take the load.

eClerx evaluated solutions from a number of vendors and finally decided on Fortinet's solutions. "We didn't find any other solution as holistic as Fortinet's," says Ritesh Pothan, CIO, eClerx. He states that the extensive set of features and policies also promised that the solution would be able to take care of any future requirements at eClerx.

eClerx used the solution for a month on trial basis, before heading for a full-scale deployment.

Complete Security Solution

Both for its offices and data-centers, eClerx has used Fortinet's solution. The products and services comprise FG1000Ax4, FG400A, FG310B, FL100B, FL800Bx2, FM400, and FC 450 for three years.

Migration from the earlier UTM solution and deployment of the enterprise-wide Fortinet solution took about six months. A team of five people, including

from Fortinet, the vendor and eClerx's in-house team, were involved.

Deployment threw up several challenges, including some downtime, as the system did not work as expected. "It was a complex installation. We had a set of rules on the earlier system, and we were looking from additional features from the new system. The upgrade caused some instability. A lot of challenges came up during setting policies, Active Directory authentication, and so on," says Ritesh.

Protecting the Network

eClerx has used the system for over a year now and Ritesh describes the experience as "Very decent, We are expecting it to get better."

Apart from securing the network, data-center, and email, Fortinet's solution has enabled eClerx to deploy security, even when an employee is outside the network. Through security clients for laptops, users can keep them secure and continue to be as productive as within company premises.

"Another good feature is SSL based proxy capabilities, which have simplified proxy management," states Ritesh. He also finds Active Directory integration useful in creating protection profiles, though this feature is not working too smoothly as of now. Through FortiAnalyzer, it is easier to generate and manage logs.

"Fortinet has the most comprehensive set of policies, which will be of use to us today and tomorrow. We haven't used all the features and policies yet, because we have opted for a systematic, slow transition," Ritesh concludes. ◀



RITESH POTHAN
CTO, eCLERX

It is a holistic solution with a comprehensive set of features. Its future promise is very high

Results

- Performance and business productivity have increased
- eClerx has been able to move from an IP based to a user-based configuration
- Apart from the data-center, network, and email, security can also be deployed on laptops moving outside the network.

Securing the Airport Network



M RAJESH
AGM, IT, GMR

Without this solution, we may not be able to run the show. It has fulfilled our business requirements almost 100%

Results

- Logical separation of the airport network has been achieved
- There is no compromise on network performance or security

Fortinet’s solution at Hyderabad’s airport helped GMR to logically separate the network, without affecting performance

GMR Group is a rapidly growing infrastructure organization, with interests in airports, highways, energy and urban infrastructure.

Among the airports that the group is responsible for is the Rajiv Gandhi International Airport, Hyderabad.

Special Security Requirements

To design the network and security at the Hyderabad airport, GMR required a device that would help them logically separate the networks of the customers—airlines, ground handlers, concessionaire, and so on—and at the same time, provide them connectivity to the common network.

“We chose Fortinet’s device because it has the capability of Virtual Domains (VDMs) with good performance, which is very useful for airport environments,” says M Rajesh, AGM, IT, GMR.

Effective Security Solution

Fortinet provides Unified Threat Management (UTM) security systems. Its range of security solutions are flexible enough to help businesses of all sizes meet their security challenges. Fortinet’s security platform has been built from the ground up, and provides multiple layers of protection and easy management. This also helps to increase flexibility in deployment, better security through integration, and scalability with changing business requirements.

GMR has deployed FG3600A at the Rajiv Gandhi International Airport, Hyderabad.

FortiGate platforms provide essential network defenses by integrating enterprise

firewall, Virtual Private Network (VPN), intrusion prevention, antivirus/antimalware, Web filtering, anti spam and application control features.

The FG-3000 series, which includes FG 3600A, integrates multiple security services into a modular appliance-based platform. It offers flexible network interface options, including hardware-accelerated Gigabit and 10-Gigabit Ethernet support. FG-3600A has one AMC expansion slot, eight 10/100/1000 interfaces and two SFP (SX/LX/TX) interfaces.

“The deployment took about a week and there was no downtime,” states Rajesh. A team of two people was involved onsite. A system integrator was involved as well.

The challenge, says Rajesh, was to ensure high availability (active/passive) implementation without network downtime.

The solution has been in use for the past eight months at the airport. Rajesh informs that all pending activities have been completed successfully.

Meeting Requirements

The Airport’s network has been designed as a common infrastructure platform, so that every customer of the Airport connects to the common network for their operations. At the same time, each customer’s network is logically separated from the other networks, to ensure protection. Fortinet’s device is indispensable for achieving this complex connectivity. Rajesh states that it gives good performance as well.

“We have really benefited with the box for logical separation of the network,” says Rajesh. ◀



Integrated Security Solution

Scalability, reliability, and easier management are some of the advantages that TAFE has seen after deploying a unified threat management solution from Fortinet

TAFE (Tractors and Farm Equipment) is a US \$750 tractor major based in Chennai, Tamil Nadu. It is among the top five tractor manufacturers in the world. Through its other divisions and wholly owned subsidiaries, TAFE also makes diesel engines, gears, panel instruments, hydraulic pumps, engineering plastics, plantations and passenger car distribution.

Need for Security

TAFE used a firewall and other security measures, but the growing number of threats in an Internet-enabled world prompted the organization to invest in a standardized security product that would provide protection from the entire range of security threats.

TAFE decided to deploy unified threat management (UTM) technology, which would encompass antivirus, Web filtering, content filtering, spam filtering, IDS, IPS, and VPNs.

To this end, TAFE explored the features of UTM products available in the market with various vendors. "We created a test environment for evaluating the UTM boxes and measured the UTM throughput, VPN configuration, firewall capability in blocking unwanted traffic, log management and reports, firewall rule management complexity and support feedback in forums," says Valavan of TAFE.

"Fortinet was selected based on firewall performance, bandwidth, support, VPN compatibility, license terms, pricing, and existing customers' feedback," he adds.

Going Live

TAFE has deployed two Fortigate 300A boxes, along with FortiAnalyzer.

A team of four people—three from TAFE and one from their partner—were involved in the implementation. A Fortinet representative also assisted in the process.

Implementation took about fifteen days. Most of the tasks, such as creation of rules and objects, were done in offline mode. TAFE took a day's downtime, in order to move the Fortigate boxes to the live environment.

Valavan recalls one challenge that came up during implementation. When Fortigate was implemented on the network, the mail service failed completely, because the IMSS server failed to communicate with TAFE's internal mail server. This was because of existing configurations on the IMSS server—when the firewall was implemented on this server, the server could not communicate with internal and external mail servers at the same time, because of these configurations. A change in configuration had the system working smoothly.

The system went live in March 2008.

Complete Security Solution

Valavan acknowledges it's early days yet, but says he's satisfied with the UTM features of the boxes, though TAFE is still figuring out the intricacies of licensing in the Fortigate system.

He says that reliability, scalability, and ease of management of the system have increased considerably, compared to their earlier firewall. ◀



A AMIRTHA VALAVAN
PRINCIPAL CONSULTANT,
NETWORK SECURITY, TAFE

We are satisfied on the implemented UTM features

Results

- Better scalability; able to monitor all network traffic based on bandwidth, as well as type of traffic
- Improved reliability; availability of accurate data about viruses, traffic, violations, and so on
- Easier management

Delivering Security



PRADEESH KARUNAKARAN
SENIOR TECHNICAL SUPPORT
ENGINEER, CAMBRIDGE
SOLUTIONS

We find the devices very useful in controlling Internet access, in order to optimize bandwidth usage for our operations

Results

- Controlled Internet access; better management of Internet bandwidth through policies
- The solution is easy to deploy and easy for new users or administrators to learn
- The solution is cost-effective

Cambridge Solutions uses Fortinet's appliances for total security and optimized bandwidth usage

Cambridge Solutions offers a range of IT and business process outsourcing services, including IT services, BPO services, and claims and risk management services. These services are combined with strong onshore presence in the client's home country and expertise in knowledge-based processing. Cambridge has presence in more than sixty locations worldwide. In India, Cambridge is present in five locations—Bengaluru, Chennai, Shimoga, Mumbai, and Pune.

Investing in Security

Cambridge began using Fortinet's solutions about four years ago, when the need for unified threat management (UTM) devices was felt to secure the company's networks. The appliances deployed at that time were FortiGate-500A, 300A and 100A.

For the Bengaluru office that has close to 1,300 employees, the company is planning to upgrade to FortiGate-1000A.

The FortiGate-500A platform features two 10/100/1000 tri-speed Ethernet ports providing flexibility for networks running at or upgrading to gigabit speeds, four user-definable 10/100 ports for redundant WAN links, high availability, and multi-zone capabilities. The platform enables administrators to segment their network into zones for granular control of network traffic, and an internal four-port switch for direct connectivity with the FortiGate-500A.

FortiGate-300A also has similar features as the 500A and is ideal for medium-sized enterprise networks. FortiGate-100A is suitable for small offices. It features dual WAN link support for redundant Internet connections, and an integrated four-port switch that can be used to provide networked devices a direct connection to the

security device. FortiGate-1000A is suitable for large networks. It features ten 10/100/1000 tri-speed interfaces.

All FortiGate platforms integrate enterprise firewall, virtual private network (VPN), intrusion prevention, antivirus/antimalware, Web filtering, antispam, and application control features to keep enterprise networks secure.

FortiGate units are designed to meet the most stringent requirements for performance and reliability, and include redundant, hot-swappable power supplies and fans to minimize single-point failures, and also support active/active redundant failover for uninterrupted service. Their high capacity, reliability, and easy management are factors that work in their favour, when it comes to enterprise's security infrastructure.

Speedy Implementation

"Implementation took hardly two days," says Pradeesh Karunakaran, senior technical support engineer, Cambridge Solutions. Initially, when Cambridge began using Fortinet's appliances, they were based on LDAP authentication. Later, however, a firmware upgrade by Fortinet added Active Directory authentication capabilities to these devices.

Effective Security

"Fortinet is really good in UTM," says Karunakaran. "We find the devices very useful in controlling Internet access, in order to optimize bandwidth usage for our operations," he explains. He adds that for their setup, content filtering and VPN are among the most useful features of the solution.

"It is an effective solution with respect to cost and working principles," says Karunakaran. "It is easy to deploy and new users can learn to use it easily," he concludes. ◀