



CASE STUDY

Instituto de Salud Carlos III

Spanish National Organization Chooses FortiWeb™

Situation

[Instituto de Salud Carlos III](#), a national public research and scientific support organization for the promotion of biomedical and health science research in Spain, is focused on developing and providing high-quality techno-scientific services for the Spanish National Healthcare System and society as a whole. Its mission is to develop and provide the highest quality scientific-technical services to the National Healthcare System and society in general.

Solution

In 2010, Instituto de Salud Carlos III (ISCIII) decided to optimize its IT infrastructure in order to eliminate server duplication and further increase information security. Since the public organization had been relying on FortiGate® multi-threat security appliances for its network security for the past three years and had been very satisfied with Fortinet's technology, it decided to replace its demilitarized zone (DMZ) configuration, which involved multiple servers.

When it came time to look at a Web application firewall (WAF), ISCIII had a few requirements that needed to be met. The first one was that the WAF functionality was compatible with the ISCIII infrastructure which is completely virtualized and the number of access points is extremely high. The agency's Webmail needed protection against brute-force attacks and SQL injection types of attacks. They also wanted to look at outgoing traffic to ensure that no proprietary/sensitive data leaves the enterprise. In essence, the ISCIII was looking for a solution which could protect its web application infrastructure against OWASP top 10 attacks.

After reviewing multiple Web application firewalls, ISCIII decided to deploy Fortinet's [FortiWeb™](#) appliance. FortiWeb was selected by ISCIII because it provides a uniform and umbrella solution for web application security and reduces complexities while representing a cost-effective investment. The FortiWeb family of web application and XML firewalls protect, balance and accelerate web applications and Internet-facing data from attack and data loss.

Working with [Fujitsu España](#), ISCIII deployed two FortiWeb-400B appliances to secure the sensitive information accessible from its web applications, leveraging the following key features:

- The institution protected its webmail against user identity theft by implementing a "Brute Force Login" security policy,
- An "SQL Injection" policy was configured in order to prevent web application hacking. In fact, several of the ISCIII's applications were hacked in the past with links to malicious websites incorporated in the applications,
- The institution has applied the "Information Disclosure" policy to help prevent attacks on servers, which store the applications containing sensitive information.

Challenges

- Deploy a Web application firewall in a completely virtualized environment

Objectives

- Protect against OWASP top 10
- Protection against information disclosure

Deployment

2 x FortiWeb-400B
2 x FortiGate-1000A
FortiGate-800
FortiGate-60C
FortiAnalyzer-800B
FortiManager-400B

Industry

Government

The number of users and the variety of access points used to enter our network means that we need a fast, reliable and secure communications network, which includes the protection of our web applications from Internet threats.

- *Antonio José Arenas*
Systems Coordination
and Information
Technologies Unit

Instituto de Salud
Carlos III

Configured to redirect web application requests to internal servers, FortiWeb became the sole point of access for all web-based applications from any of ISCIII's internal and external networks. FortiWeb has also been configured to perform SSL application processing, which frees up valuable resources (CPU & RAM) that can then be used by other servers as the environment is fully virtualized.

Success

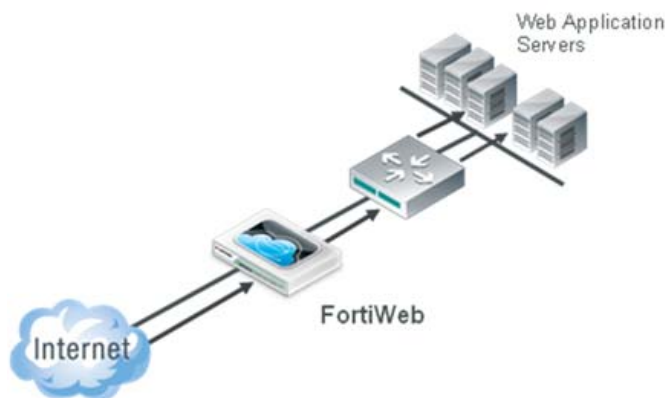
The number of users and the variety of access points used to enter the network provided ISCIII with a fast, reliable and secure communications network, which includes the protection of web applications from Internet threats.

Another benefit since deploying the FortiWeb appliance is the base protection filters deployed by the FortiWeb Attack Signature

Database. These provide the ISCIII with protection against "typical OWASP top 10 type of attacks.

Finally, working with Fujitsu España proved to be invaluable to ISCIII. Fujitsu España has the knowledge and know how to test and integrate the Fortinet solution and in doing so were able to design and deploy the Fortinet solution throughout ISCIII's virtualized infrastructure. Their experienced consultants understand what the government agency needed and answered with features available in FortiWeb.

CAS230-0411



FORTINET®

GLOBAL HEADQUARTERS

Fortinet Incorporated
1090 Kifer Road, Sunnyvale, CA 94086 USA
Tel +1.408.235.7700
Fax +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE – FRANCE

Fortinet Incorporated
120 rue Albert Caquot
06560, Sophia Antipolis, France
Tel +33.4.8987.0510
Fax +33.4.8987.0501

APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated
300 Beach Road #20-01, The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784