

# Case Study



**IronPort Ensures Safe Email Travel for one of the World's Largest Airport Authorities**

## THE SITUATION

Like many organizations, French airport group Aéroports de Paris is facing a massive amount of incoming spam. For some employees, spam accounts for 75-95 percent of incoming mail. Though all users are not equally affected by this plague, it results in loss of time and frustration for all of them. Therefore, in early 2005, Aéroports de Paris IT department started looking for a solution to control unwanted mail flows. More than just an anti-spam tool, the solution had to act as a true, reliable and robust SMTP email gateway – integrating several technologies to provide network security, both upstream and downstream. And, of course, false positives had to be avoided.



With IronPort's products, we found a global security solution for protecting our email systems against various threats. ”

### AÉROPORTS DE PARIS AT A GLANCE

Turnover: 1.821 billion euros in 2004

Services: Europe's second largest airport group; first in Europe and second worldwide for international services

Locations: 14 airport hubs in the greater Paris area, including Paris-Charles-de-Gaulle, Paris-Orly and Paris-Le Bourget, totaling 75 million passengers per year

Staff: 9,597, including 8,238 Aéroports de Paris' employees

### THE IRONPORT ADVANTAGE

- Strong technological innovation, including the AsyncOS operating system, an MTA (mail transfer agent) specifically designed for SMTP, the SenderBase global Internet traffic monitoring network and proactive filters
- Employee productivity increased by eliminating spam
- Up to 75 percent reduction in administrative costs
- Enhanced network security



### THE IRONPORT SOLUTION

Out of 740,000 incoming messages each day, an average 11.5 percent contain spam and 3.5 percent carry viruses. These statistics have been issued since Aéroports de Paris deployed two IronPort C60™ email security appliances, which protect over 8,000 mailboxes against spam and viruses. All SMTP traffic now flows through IronPort's MTA platforms. This high-performance, secure equipment is 10-20 times faster than conventional systems. Aéroports de Paris has purchased all available modules. IronPort's appliances include threat prevention with IronPort Reputation Filters™ and IronPort Virus Outbreak Filters™, as well as further technologies such as IronPort's content scanning engine, Brightmail Anti-Spam and Sophos Anti-Virus.

"We were looking for a solution which would not require any change to our existing architecture. We selected IronPort's appliances for their efficiency and great manageability. Several anti-spam technologies are provided in a single, optimized appliance to address the spam challenge," explained Fabrice Lormant, System and Security Project Manager at Aéroports de Paris IT and Telecommunications Department.

#### Standalone, Scalable Equipment

IronPort® appliances ensure that Aéroports de Paris' email infrastructure is never overwhelmed. "IronPort C-Series™ appliances allow the multi-threading of SMTP queues, ensuring uninterrupted email delivery during attacks. We have never had any overload problems, as the system usage is only five percent," said Lormant.

IronPort's solution can be very easily and quickly deployed. The appliances include all necessary native features, such as the central management of all device configurations. Aéroports de Paris' IT staff performed the initial setup, based on a strategy suited to the company's needs, and classified mail senders based on their reputation using IronPort's SenderBase® – the world's largest Internet traffic monitoring network (leveraging data from over 100,000 contributing organizations). "Once the equipment has been set up, the solution is completely standalone, which saves time both for administrators and users," Lormant added.



The IronPort C-Series email security appliance is easy to set-up and manage.



### A Global Email Security Solution

IronPort appliances help to enhance Aéroports de Paris' network security by eliminating spam and other email-based threats. Reputation filtering processes messages at the IP address level and blocks any incoming malicious traffic upstream of the network. Suspicious mail is quarantined until the first virus signatures are made available. Attachments which contain executables are rejected based on a binary check.

IronPort's robust solution can also be used to prevent DoS (denial-of-service) attacks. Different security policies are defined for various user groups by looking up the LDAP directory. A powerful, yet easy-to-use, content scanning system enables administrators to set up filters operating on ADP – specific keywords or phrases. In addition, the mail gateway automatically appends a disclaimer (specific to each group of senders) to outgoing messages.

Lormant sums up, "Thanks to IronPort, 3,500 connections are rejected daily and 90 percent of spam is now blocked. No false positives have been reported since we implemented the solution."



#### IronPort Systems, Inc.

950 Elm Avenue, San Bruno, California 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL [info@ironport.com](mailto:info@ironport.com) WEB [www.ironport.com](http://www.ironport.com)

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

Copyright © 2000-2007 Cisco Systems, Inc. All rights reserved. IronPort, the IronPort logo and SenderBase are registered trademarks of Cisco Systems, Inc. All other trademarks are the property of Cisco Systems, Inc. or their respective owners. While every effort is made to ensure the information given is accurate, Cisco does not accept liability for any errors or mistakes which may arise. Specifications and other information in this document may be subject to change without notice. P/N 451-0118-1 10/07

IronPort is now  
part of Cisco.

