



Flyers get worldwide connections with LAN2LAN

“LAN2LAN’s security expertise has allowed us to turn a commercial necessity into a genuine competitive advantage...”

Jason Bamforth,
IT Director,
London City Airport

Background

London City Airport is unique. It is, perhaps, the only true London airport, since it is situated in the heart of the city. It has one terminal and a separate management centre, but it operates more than 90,000 aircraft movements a year, serving more than three million passengers. It is a key international hub for the capital, whose customers have high expectations of the facilities it offers. Among the most important is the provision of Wi-Fi Internet access in the terminal building. The airport’s IT team turned to LAN2LAN for a solution that would give all users quick and easy connection, without compromising the security of the airport’s network infrastructure.

The Challenge

Seasoned business travellers are learning to take wireless Internet access for granted. Most major terminuses, whether they are airports, railway stations, or even bus stations, provide some means of wireless connection. Often, however, it involves some means of purchasing a short-term licence, or at least the use of a passcode, which is not always readily available.

These barriers to connection may be appropriate for a hotel lobby or coffee shop, where users may be inclined to linger for an hour or more. However, the nature of travel via London City Airport means that users will only want access to the network for a short time; by the time they have jumped through the security hoops, their flight may be called.

“London City Airport is a brand shaped by leading-edge technologies,” says Jason Bamforth, IT Director for the airport. “Its viability was determined from the outset by the arrival of quiet, short-take-off-and-landing aircraft, such as the BA146.

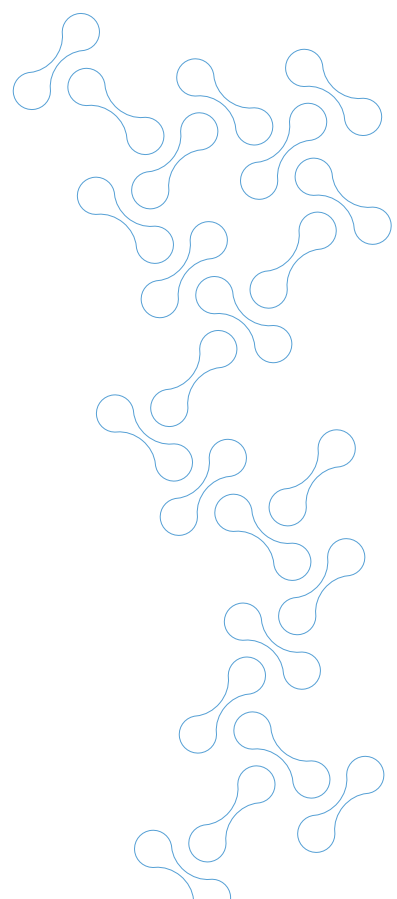
“The continued use of advanced technologies is integral to the development of our business. To compete with other hubs, we have to provide wireless Internet access and we were determined it was going to be the best possible solution.

“Above all, we wanted to give our customers quick and easy connection, with as few security obstacles as possible.”

The task given to LAN2LAN was to add a public wireless network to the airport’s existing infrastructure. This meant providing strong security to keep the public and internal networks separate, while still allowing free and easy access to public users. In a scenario where the IT team has no control over the random connections made to the network, any one of millions of machines could prove to be a damaging vulnerability.

Says Jason Bamforth: “We had no concerns about the security of the actual wireless infrastructure, since the idea from the start was to allow anyone within the terminal to connect. The security issues we wanted to address are common to all forms of Internet connection, wired and wireless. In particular, our concern was with content filtering, so that users could not download harmful or illegal material, either accidentally or deliberately.

“We also needed strong Firewall protection, to keep out unauthorised or malicious connections, as well as defence against viruses and malware. These could infect the infrastructure either through an Internet connection, or through a user connecting with an infected machine.”



The Solution

LAN2LAN's recommendations gave London City Airport three discrete wireless infrastructures, with three separate Service Set Identifiers (SSIDs). The first of these is used by the airport's staff, the second by passengers and the third by Restair, the company operating the catering franchise within the terminal.

"Restair were among the prime movers for the deployment of wireless," says Jason Bamforth. "They are using the Wi-Fi network for their wireless ordering system, which has helped speed up their service to customers."

The wireless network is built with Trapeze switches and access points. The public traffic and the internal infrastructure are both routed through Bloxx content filtering appliances, using Tru-View third generation filtering to give day-zero protection against unclassified sites that contain potentially harmful content.

A pair of Fortinet FortiGate 800 firewalls, deployed in an active cluster, are used to split traffic between the two data-bearers, using policy-based routing. This configuration helps to ensure high availability for the network. The public and internal networks are kept separate by the Firewalls, locking out any potential for cross-infection.

Says Jason Bamforth: "Although the biggest threat must come from the public connections, we have to be scrupulously vigilant to ensure that one of our passengers does not acquire some damaging malware from our own infrastructure. They must have absolute confidence in the integrity of the network they are connecting to."

Trapeze SmartPass guest access provisioning is used to initiate the first user connection. When passengers use the network for the first time, they are presented with a welcome screen sponsored by the Financial Times newspaper. This prompts them to agree to the terms and conditions of use.

The SmartPass system generates a user name and password and a cookie is placed on their machine. The next time they connect, they have immediate access.

"LAN2LAN specified and designed the entire solution, including the cabling between the wireless access points and the network switches," says Jason Bamforth. "It was a straightforward and quick deployment which has been an immediate success with our customers and our franchise partners."

The Benefits

With the approach of the London Olympics in 2012, London City Airport is gearing up for a new peak in activity. "We are going to be a crucial part of the Olympic infrastructure," says Jason Bamforth, "and we must be able to deliver a world-class service.

"Provisioning quick and easy Wi-Fi for all passengers in the terminal building was an important step. LAN2LAN's security expertise has allowed us to turn a commercial necessity into a genuine competitive advantage, because other Wi-Fi hotspot deployments are not so easy to use. The smart access we can provide enhances the message of innovation and great service that are the cornerstones of our brand."

LAN2LAN has also provided a fully redundant deployment of the solution, to allow for business continuity in the event of any disruption to the service. This aspect is particularly important for the airport's own infrastructure, and for the franchise partners whose service depends on sustained availability of the network.

"We now have a wireless infrastructure that is secure and robust enough to scale with our evolving needs," says Jason Bamforth. "It has applications in baggage handling, ticketing and many other areas, all of which will contribute to the delivery of continuously improving service. We're gearing up to be a vital hub for the Olympics and beyond, and LAN2LAN have given us a flying start."

FORTINET™

TRAPEZE
GOLD PARTNER

BLOXX
NO NONSENSE.

5 Genesis Business Park,
Woking, Surrey
GU21 5RW

T: 0870 787 4001

F: 0870 787 4002

E: info@LAN2LAN.com

W: www.LAN2LAN.com



LAN2LAN
Clever Networks. No Limits.