



Australian Education Department Turns To F5 So That Over A Million Students, Teachers and Staff Have Secure and Highly Available Access To Intranet Services

Executive Summary

One of Australia's largest organisations -- a government department responsible for educating more than a million children and adults -- has a network with 2,500 WAN end-points spread over a wide geographical area. Over the years, the department has developed a range of corporate applications hosted at two main city locations. In the past, the department only provided limited access to the corporate network with the remote locations, unable to benefit from the wealth of available applications. This was partly because of security concerns but also because the legacy applications were not accessible over the Internet. By introducing F5's FirePass® devices to interface with an Oracle portal, the department has not only provided secure access but has saved time and the expense of rewriting the corporate applications. FirePass allows students, teachers and administrative staff to log onto the portal with a web browser for all the corporate services and applications they need.

The additional and unique benefit of partnering with F5 is the extension of the department's application delivery objectives of scalable, secure universal access. But they're also using F5's BIG-IP application networking systems for managing user application sessions and ensuring the integrity and availability of all their applications.

The department is a forerunner in their approach to solving application delivery challenges. Instead of attempting to deploy a number of point products and non-integrated solutions, they have deployed the majority of the components that make up the integrated F5 Application Delivery Network.

Challenge

The main drivers of the project were the need to bring a number of disparate applications into a unified service so that students and staff could have easy, secure access to enterprise applications.

However, the core IT applications that are used in a large government department take many years and millions of dollars to develop. They provide many complex and powerful functions that are central to the efficient management of the organisation. Unfortunately, these legacy applications were often developed for local LAN access and not for the web. Therefore, their functionality and availability was restricted to only those who were hard-wired to the network.

Making legacy applications suitable for web access can be an extremely expensive and time consuming task. Many organisations are forced to make the choice of either doing a major overhaul of their systems or building new 'webified' applications from the ground-up. Considering a number of vendors, BIG-IP was technically far superior and F5 Networks had both a proven track record with similar types of web sites. They also looked like they were going to be here for the long haul and not just a here-today and gone tomorrow startup.

And once the applications are in a form suitable for sharing with users in remote locations, another factor comes into play – security.

By creating a web version of applications, organisations are potentially making their core applications vulnerable to HTTP attacks.

The technical solutions to all of these issues are complex and multi-faceted but end-users need to be shielded from this complexity or they won't use the services available to them. This is especially important in an area like education, where many of the end-users are children. So the



solution has to include a means of making the applications and services available through a common, easy-to-use interface that belies the complexity of the network.

These were among the challenges faced by the network team at this education department in Australia.

Solution

The department's preferred architecture for the network was a corporate portal accessible via an intranet from any of the 2500 end-points, with a web browser as the standard operating environment.

However, the key to making the applications and services available through the portal was based on a secure, flexible and scaleable web interface that could easily integrate the legacy systems with the corporate intranet.

"When we went looking for a product with all of the functionality we needed, we found only one company that could provide it – F5," explained the department's networking team leader. "Nothing else came close."

"The F5 FirePass provides integration with the Oracle portal and gives us a secure means of delivering our legacy applications and other third party web applications by offering a secure transport using HTTPS," the team leader added. "It was an easy and cost-effective way of being able to provide complete solutions without having to write custom scripts."

The portal allows students, teachers and administrative staff to access the different systems and services they require using a variety of desktops, yet they all experience the same front-end interface.

"The standard operating environment is a web browser," the team leader explained. "There is a single sign-on and when you log in, your profile is pulled out of a LDAP database that authenticates the applications you have access to as a student, teacher or staff member. From a user perspective it is transparent because it has a common look and feel."

Students can gain access to email, forums and chat rooms; teachers can perform classroom bookings, roll marking and fill in forms through the corporate network.

"Schools were never able to access departmental servers to access files via the Internet because it was too much of a security risk," the team leader said. "They are now able to do that and they are blown away about it."

"Also, if staff want to work from home, they can now access the corporate servers securely via the portal because of the security features built into FirePass."

The department relies on the ICAP (Internet Content Adaptation Protocol) API feature within FirePass to pass virus scanning off to the corporate infrastructure that checks for malicious attacks. FirePass can scan web and file uploads via ICAP. Infected files are blocked at the gateway and not allowed onto network servers.

The scalability and flexibility of FirePass also means that the department can continue to expand the number of applications and services accessible through the portal.

"We can integrate new applications into the environment with a minimum of fuss because users will be familiar with the interface," said the team leader. "For existing applications, they don't have to be re-written. So we can move them into an area that is secure, and allow FirePass to provide access. That has prolonged the life of our legacy applications."

The ease of implementation was also a key benefit of FirePass.



“Getting FirePass up and running is so easy,” said the team leader. “It’s fantastic. FirePass allows functionality to be available out of the box. It also saves the time and effort of writing custom applications. We had a plethora of corporate applications we needed to webify. Because of FirePass, it required no real development. We just borrowed the functions from F5 and wrapped them up in the Oracle portal.”

The department has installed a number of other F5 products to ensure maximum availability and performance of the network. It has standardised on F5’s BIG-IP application networking systems, with about 20 of the devices installed at critical points within the network for optimizing application performance while providing redundancy and scalability.

The department is in the process of deploying F5’s BIG-IP® Global Traffic Manager product (formerly 3-DNS) to provide a full redundancy and fail-over function, so traffic can be transferred between sites in the event of a system failure. BIG-IP Global Traffic Manager provides wide-area application networking and high availability of IP applications and services running across multiple data centres.

In addition, the department uses F5’s iRules, customisable commands technology that integrates with the various components to ensure a scalable and secure network that offers ready access to disparate applications, all in a unified service. The department uses iRules to manipulate cookies and allow secure integration between the Oracle portal and FirePass. It also uses iRules with other applications in its corporate IT infrastructure.

“We are becoming increasingly dependant on the flexibility and features that iRules provide,” the team leader said.

In short, the department is building a true F5 application delivery network, a uniquely integrated architecture where the department can ensure that their applications are secure, highly available, and fast, end-to-end. F5 is the only vendor who offers this complete end-to-end portfolio designed as key architectural building blocks. The result for the department is tremendous cost-savings and the ability to meet strategic objectives with extreme flexibility.

About F5

F5 Networks is the global leader in Application Delivery Networking. F5 provides solutions that make applications secure, fast and available for everyone, helping organizations get the most out of their investment. By adding intelligence and manageability into the network to offload applications, F5 optimizes applications and allows them to work faster and consume fewer resources. F5’s extensible architecture intelligently integrates application optimization, protection for the application and the network, and delivers application reliability - all on one universal platform. The company is headquartered in Seattle, Washington with offices worldwide. For more information go to <http://www.f5.com>.