

DOCUMENT* PRESENTED
BY WICK HILL

access
access
management
management
performance
performance
security
security

* © Wick Hill and the Wick Hill logo are trademarks of Wick Hill Group Plc. Registered in the UK and other countries. Other logo, brand and product names are trademarks of their respective owners. All 3rd party information contained within this document is copyright of the originator. Errors and omissions excluded.



Barracuda Networks Insures CSMA Club Web Sites Against Overload

About the Civil Service Motoring Association

Since its foundation in 1923, CSMA Club (Civil Service Motoring Association) has become the UK's largest private home, motoring and leisure association. Providing benefits to those working in the Civil Service, CSMA Club is a Brighton-based organisation that is owned and run on behalf of its members. CSMA Club offers special benefits on a wide range of services from home, travel and motor insurance to discounts on travel and leisure activities, as well as its own hotels and self-catering complexes.

CSMA Club promotes its member services and hotels through five main Web sites: www.csmaclub.co.uk, www.whitemead.co.uk, www.ghyllmanor.co.uk, www.wheelfarmcottages.co.uk and www.cotswold-motor-museum.co.uk. The traffic for all five sites, totalling between 4,000 and 10,000 static page requests per day, is balanced across two servers, both containing a copy of all five sites. The traffic also consists of a certain amount of interaction from members including updating personal details online as well as looking up information about CSMA Club partners, suppliers and services.

Anytime one of the CSMA Club Web sites went down the servers would have to be manually swapped, which led to inefficient use of already-limited hardware resources. CSMA Club determined that a load balancing solution was crucial, to ensure that the daily Web traffic was appropriately distributed, ensuring that no single server was overloaded, thus decreasing the chances of Web site downtime.

Shopping around

While researching load balancing solutions, CSMA Club discovered that some appliances on the market can be difficult to use, costly and complex.

"The products that we first looked at were just too expensive – they were packed with all sorts of unnecessary features," said Rob Manktelow, CSMA Club technical services manager.

Manktelow contacted a Surrey-based Barracuda Networks partner who informed him that the Barracuda Load Balancer was easy to use and well within his budget.

"Our contact listened to our needs and requirements," said Manktelow. "They gave us login details to the Web GUI of a Barracuda Load Balancer demo unit and talked us through the key features. Within minutes we were able to see how easy it was going to be to set up."

Trial without tribulation

CSMA Club arranged for a free trial of the Barracuda Load Balancer 340.

"The appliance arrived the next day and the initial deployment was an absolute breeze," said Manktelow. "We were balancing traffic across our Web servers within a couple of hours."

"The Barracuda Load Balancer has been very cost effective and provided us with clear, easy to read statistics enabling us to get a clear view of traffic patterns and alerting us to failed servers."

-Rob Manktelow
 CSMA Club technical services manager



Barracuda Load Balancer 340 Fast Facts:

- Achieves high availability & scalability objectives
- Integrated load balancing & intrusion prevention
- No per port, per server or per feature license fees
- Advanced load balancing features including direct server return and Layer 7 cookie persistence
- Includes SSL offloading

Manktelow was particularly impressed with the Barracuda Load Balancer's ability to easily take servers offline to perform routine maintenance without disrupting access to Web sites. He liked the ability to drop a server from a cluster to allow for updates without taking down sites.

"We can test software releases before the server is reintroduced into the cluster," said Manktelow. "Another really useful feature is the unit's flexibility. You can run the Barracuda Load Balancer in three different operating modes making it one of the most flexible load balancers on the market."

The three modes are Route-path, which offers the most flexibility, while Bridge-path allows the unit to be deployed without changes to existing IP infrastructure. Finally there is Direct Server Return which allows up to 10GB throughput and is ideal for content delivery networks.

The Barracuda Load Balancer's built-in Intrusion Prevention System (IPS) adds another layer of protection against attacks. Before CSMA Club installed the Barracuda Load Balancer they used two layers of firewalls in front of their Web servers.

"The Barracuda Load Balancer is complementary to our firewalls," said Manktelow. "The IPS has helped us to block HTTP attacks such as oversized request-url directory, double decoding and bare byte Unicode encoding that were destined for the Web sites."

The right fit

The Barracuda Load Balancer is priced to suit smaller businesses that have heavy traffic across multiple Web servers. With no per port or per server license fees, the Barracuda Load Balancer is less expensive than many competing solutions, making the Barracuda Load Balancer the right fit for nearly any IT budget.

The Barracuda Load Balancer automatically receives the latest intrusion prevention and security updates from Barracuda Central, an advanced technology operations centre where engineers continuously monitor and mitigate the latest Internet threats. The Barracuda Load Balancer is easy to deploy, featuring an auto-discovery module and complete configuration via an intuitive Web interface.

"The Barracuda Load Balancer has been very cost effective and provided us with clear, easy to read statistics enabling us to get a clear view of traffic patterns and alerting us to failed servers," said Manktelow.

About Barracuda Networks Inc.

Barracuda Networks Inc. is the worldwide leader in email and Web security appliances. Barracuda Networks also provides world-class IM protection, application server load balancing, Web application security, and message archiving appliances. Coca-Cola, FedEx, Harvard University, IBM, L'Oreal, and Europcar, are amongst the 70,000 organizations protecting their networks with Barracuda Networks' solutions. Barracuda Networks' success is due to its ability to deliver easy to use, comprehensive solutions that solve the most serious issues facing customer networks without unnecessary add-ons, maintenance, lengthy installations or per user license fees. Barracuda Networks is privately held with its headquarters in Campbell, Calif. Barracuda Networks has offices in eight international locations and distributors in more than 80 countries worldwide. For more information, please visit www.barracuda.com.



About the Barracuda Load Balancer

Available in four models, the Barracuda Load Balancer is an affordable, scalable and comprehensive solution for intelligently distributing network traffic across multiple servers. Barracuda Load Balancers support up to 250 servers with no per port or per server licensing fees for ultimate network efficiency.

The Barracuda Load Balancer offers network administrators reliability, speed and security with cookie-based session persistence, SSL acceleration and network intrusion prevention. Designed to achieve network flexibility and operational reliability, the Barracuda Load Balancer integrates powerful layer 4 or layer 7 load balancing. To minimize ongoing administration, Barracuda Load Balancers receive hourly Energize Updates delivered automatically by Barracuda Central to provide the most current intrusion prevention definition and security updates.



Barracuda Networks, Inc.

www.barracuda.com

info@barracuda.com



DEK Halts Spam with Barracuda Spam Firewall

Barracuda Networks Provides Complete Email Security Protection for Leading Provider of Screen Printing Technologies

About DEK

DEK is a leading provider of equipment and processes for the high accuracy mass imaging of electronic materials. The UK-based company has developed screen printing technologies for leading-edge electronic assemblers since 1969. Through the combined strength of machines, stencils and screens, consumables and process support products, DEK delivers total support for their customers' materials deposition processes.

To assure that its customers continue to receive this high-quality support and service, it is necessary for DEK employees to have solid, uninterrupted means of communication within the organisation as well as with customers. In the years preceding 2005, DEK struggled with keeping email, one of its most important communication channels, flowing due to increasing amounts of unsolicited email hitting employees' inboxes.

Spam wastes DEK time and resources

The legacy email filtering system DEK relied on was not efficient in stopping the massive amount of spam that was bombarding the company's more than 800 globally-based email users who were located both in the field and 18 satellite offices. According to Chris Bill, IT security analyst at DEK, an estimated 20 percent of spam was getting through to its email users.

When DEK's MIS department originally began filtering email it was to ensure compliance, however spam had become a primary issue. Illegitimate email was wasting employee time and resources. Previously, the MIS department would check its email filter periodically. However, this became nearly a full-time task, which included the risk that a genuine email, possibly an order from a long-standing customer, could be inadvertently deleted.

"Every working day, a member of the helpdesk team would spend at least three to four hours sifting through the received messages to both try to block spam messages and release any genuine messages that may have been blocked," said Bill. "I cannot begin to think how much time was wasted by employees."

Finding a new, reliable, email security solution

Plagued by complaints from frustrated users who had to wade through massive amounts of spam as well as those who had lost important emails, Bill was tasked with finding a more suitable and capable email security solution.

With the increase of spam also came an increase in the threat of email-borne viruses and malware. Bill and the MIS department knew that they needed to find a complete email security solution that could provide protection against these ever-present threats.

Along with putting a stop to spam and protecting users from viruses and malware, compliance with internal policies was still paramount to DEK. The MIS department and DEK management were keen to stop inappropriate content from entering the company and they also needed to ensure that employees did not send email that might include inappropriate language or content to customers.

"We needed a product that would be easy to use, stop spam and viruses, help us with compliance and that would stay within our budget," said Bill. "I thought we might be asking for too much."

"The Barracuda Spam Firewall does what is says on the tin: It stops spam, helps with compliance, protects our email users from viruses and needs very little maintenance."

-Chris Bill
IT Analyst
DEK



Barracuda Spam Firewall 400 Fast Facts:

- Services up to 5,000 active email users
- Compatible with all email servers
- Easy plug and play installation
- Per user settings and quarantine
- Clustering for redundancy and added capacity

Barracuda Spam Firewall stops spam and helps ensure compliance

After researching and evaluating several solutions, Bill spoke with a Hertfordshire-based IT company which has been recommending Internet security products to DEK since 2000. The IT company recommended a Barracuda Spam Firewall and Bill was pleased to learn that Barracuda Networks offers a 30-day free evaluation unit.

"It was difficult to test a potential product fully as it required (simulating real email traffic using) large volumes of unsolicited email to test effectively," said Bill. "This is why a 30-day evaluation unit from Barracuda Networks was put straight into a live environment, not something we would do lightly, but the benefits were immediately obvious."

The results were impressive; spam virtually disappeared from users' inboxes soon after the Barracuda Spam Firewall 400 was installed. In addition, the Barracuda Spam Firewall provided complete protection against email-borne viruses and malware. Further, the entire Barracuda Spam Firewall line features simultaneous inbound and outbound email filtering with the inclusion of sophisticated outbound email filtering techniques, such as rate controls, domain restrictions, user authentication (SASL), keyword and attachment blocking, dual layer virus blocking, and remote user support for outbound email filtering.

Bill and DEK's MIS department were also pleased by the Barracuda Spam Firewall's per-user settings and quarantine.

"One man's spam is another man's ham and with the Barracuda Spam Firewall users can decide for themselves which email is to be whitelisted and which not," said Bill. "I may be interested in my weekly fishing e-zine but perhaps no one else is."

DEK was so impressed with the results of the trial and the Barracuda Spam Firewall's affordable price that the company purchased four Barracuda Spam Firewall models. DEK has two mail gateways; the primary MX in its UK headquarters, and a secondary MX in its office in Germany. The company purchased two Barracuda Spam Firewall 400s and placed one on each gateway, in a clustered environment for redundancy. This allowed the units to share one rule base and users needed only to access one site to check their own quarantine areas.

DEK also purchased two Barracuda Spam Firewall 300s for outbound email filtering in both the UK and German offices. Internal mail servers direct email to the Barracuda Spam Firewalls in outbound mode via a fake MX zone which ensures that the most available Barracuda Spam Firewall receives the email to send out, which reduces the risk of downtime due to connectivity issues.

Barracuda Spam Firewall continues to impress

"We went from receiving approximately 20 percent of the spam email sent to us to about two percent, with extremely low false positives – those numbers speak for themselves," said Bill.

Bill continues to be impressed with the Barracuda Spam Firewall. According to Bill, between January 2005 and October 2007 DEK received 4.3 million emails of which only 850,000 were allowed as legitimate email.

"The Barracuda Spam Firewall does what is says on the tin: It stops spam, helps with compliance, protects our email users from viruses and needs very little maintenance," said Bill.

Overall, the Barracuda Spam Firewall has saved DEK an immeasurable amount of time and resources.

"Previously we had someone virtually full-time manually sifting through the email to determine what was spam and what was not," said Bill. "The time this person spent doing a miserable job is now spent doing something more interesting and constructive."



About the Barracuda Spam Firewall

The Barracuda Spam Firewall is available in seven models and supports up to 30,000 active users with no per user licensing fees.

Its architecture leverages 12 defense layers: denial of service and security protection, rate control, IP analysis, sender authentication, recipient verification, virus protection, policy (user-specified rules), Fingerprint Analysis, Intent Analysis, Image Analysis, Bayesian Analysis, and a Spam Rules Scoring engine.

In addition, the entire Barracuda Spam Firewall line features simultaneous inbound and outbound email filtering with the inclusion of sophisticated outbound email filtering techniques, such as rate controls, domain restrictions, user authentication (SASL), keyword and attachment blocking, dual layer virus blocking, and remote user support for outbound email filtering.

The Barracuda Spam Firewall's layered approach minimises the processing of each email, which yields the performance required to process millions of messages per day.



Barracuda Networks, Inc.

www.barracuda.com

info@barracuda.com



**Royal College
of Physicians**
Setting higher medical standards

Royal College of Physicians Sails Past PCI Exam

About Royal College of Physicians

The Royal College of Physicians of London (RCP), a registered charity based in the United Kingdom, is a professional membership organization dedicated to ensuring that doctors are educated and trained to the highest of standards, and that patient care is delivered consistently with maximum quality. To help meet this aim, RCP, which represents more than 21,000 Fellows and Collegiate Members, provides education, training, medical examinations, and other services that aim to further the practice of medicine.

Strong security essential for new Web infrastructure

The IT department of Royal College of Physicians of London runs the medical examination Web site on behalf of the Federation of Royal Colleges of Physicians of the UK. When the department sought to make certain its new Web site met PCI DSS compliance, it turned to Barracuda Networks, which acquired leading Web application and security vendor NetContinuum in 2007, and found a way to not only meet Payment Card industry Data Security Standard (PCI DSS) requirements, but also to simplify the management of its entire Web DMZ architecture.

Further, when RCP readied the rollout of its new Web infrastructure, it wanted to be certain all 14 of its Web sites were deployed and maintained as securely as possible. The rollout kicked off with the launch of a new e-learning site dedicated to providing physicians easy access to educational resources and support, as well as an enhanced site for the Membership of The Royal Colleges of Physicians of the United Kingdom, MRCP (UK), on behalf of the Federation of Royal Colleges of Physicians of the UK. The MRCP (UK) site provides physicians with all of the information they need to take the three-part MRCP (UK) examination enabling physicians to apply, register, as well as pay for their exams, and receive their results all on one site.

Virtualized Web architecture and PCI Data Security Standard compliance

RCP expects several million pounds of transactions to flow through the site, with most payments conducted by credit card. Therefore it was crucial that the examination site be highly secured to protect the privacy of the physicians' personal information as well as the availability of the applications, and the site had to be PCI DSS compliant before it could go live.

Like most organizations, RCP operates on a tight budget with IT support and development teams closely integrated. Building an end-to-end Web infrastructure that was easy to manage and maintain was essential. With that goal in mind, RCP decided to architect and build a virtualized Web server farm. The internally-hosted Web architecture comprises six servers, or blades, including a VMWare management server, a server dedicated to the management of RCP's domain addresses, and four servers that make up the virtual server farm. In addition, the Web applications are based on Microsoft Windows SharePoint Services 3.0.

"This architecture makes it easy for us to centrally manage our SharePoint front-end, the mid-tier systems, as well as our backend databases," said Christopher Venning, IT network and support manager at RCP.

The issue yet to be solved was how RCP could give its new architecture the highest level of security and availability possible, and be able to prove to a team of external auditors that it met PCI DSS compliance, as required by its acquiring bank. Like its Web site architecture, RCP wanted its security to be centrally managed and to feather well with the virtualized application server infrastructure.

"PCI compliance was a strict requirement from the bank. We had to be able to show our compliance before we would be able to conduct transactions," said Venning.

"As part of the process members use to register for examinations, we collect a variety of information, including credit card data. The banks insisted that our Web systems be PCI compliant. Barracuda Networks helped us to get there without a struggle."

-Christopher Venning
Network Manager
Royal College of Physicians



Barracuda Application Gateway NC-1100 AG Fast Facts:

- Easily helps organizations comply with PCI DSS requirements
- Delivers best practices security out of the box
- Single point of protection for inbound and outbound traffic for all Web applications
- Protects Web sites and Web applications against application layer attacks
- Monitors traffic and provides reports about attackers and attack attempts

Of particular importance to RCP was PCI DSS version 1.1, established by the independent PCI Security Standards Council in September 2006. This version included significant changes in how the standard addresses Web application security. For instance, the updated version requires all custom-built application software to be reviewed by an application security specialist for vulnerabilities, or that merchants that accept or store credit card transaction information deploy a Web application firewall.

Venning and his team carefully examined a number of ways to fulfill these standard requirements while maintaining the highest levels of security, including deploying a network firewall, a Web application firewall, or a load balancer, as well as securely managing all of the individual routers and switches in their infrastructure. But none of the architectures they investigated seemed to be easily manageable.

"Everything seemed more complex than it needed to be," said Venning. "We really needed a single point of control for the whole DMZ environment."

While RCP evaluated its options, its solution provider, Matrix Communications Systems, recommended that it look at the application firewalls and gateways provided by Barracuda Networks. Following a careful appraisal, RCP chose to secure its entire application architecture with the Barracuda Application Gateway NC-1100 AG. The Barracuda Application Gateway NC-1100 AG combines best-in-breed application firewall technology with full-load balancing and traffic management that includes connection pooling, caching, compression, and application acceleration from within a single appliance.

"The installation went flawlessly," said Venning. To meet all of its security and high-availability needs, the RCP deployed two Barracuda Application Gateway NC-1100 AG appliances: one dedicated to protect all of its live Web traffic, and the second as part of its fail-over strategy in the event something goes awry with the primary device.

Comprehensive Web application security and streamlined PCI compliance

With the complete implementation of the Barracuda Application Gateway NC-1100 AG, RCP's Web applications are protected from increasingly prevalent forms of attack, including buffer overflows, SQL injections, cross-site scripting, forms tampering, cookie and session stealing, and a multitude of other Web application attack techniques.

Equally important, the Barracuda Application Gateway NC-1100 AG helped RCP easily pass its first two PCI DSS compliance audits. After completing both the e-Learning and MRCP (UK) examination sites, RCP had those sites audited independently to validate that they met the specification. In addition, the device helped RCP streamline the audit process which requires everything to be documented, including configurations for everything from firewalls to routing and switching.

"With this setup, I only have one sheet for the audit, not a raft of documents," added Venning.

Web application security for the long haul

RCP is currently bringing a dozen additional sites online, each is protected by the Barracuda Application Gateway NC-1100 AG.

"The administrative framework is very well suited for front ending a virtualized server environment," said Venning. "Adding new applications behind the Barracuda Application Gateway NC-1100 AG is very easy."

With the Barracuda Application Gateway NC-1100 AG Venning and the RCP IT team no longer have to worry about rapidly spreading, new application threats, or significant portions of the PCI DSS standard.

"With Barracuda Networks we realized that these appliances not only help us to achieve PCI compliance, but also simplify our network infrastructure," said Venning. "As an added bonus, we have improved availability and simplified our management."



About Barracuda Web Application Controllers

Barracuda Web Application Controllers, including both the Barracuda Web Application Firewall and Barracuda Application Gateway, protect Web sites from attackers leveraging protocol or application vulnerabilities to instigate unauthorized access, data theft, denial of service or defacement. Designed to deliver comprehensive Web security, the Barracuda Web Application Controllers acts as a proxy for Web traffic to insulate Web servers from direct access by hackers, enforces data security standards, such as the Payment Card Industry Data Security Standard (PCI DSS), and secures Web sites against the top 10 major Web vulnerabilities compiled by Open Web Application Security Project (OWASP).



Barracuda Networks, Inc.

www.barracuda.com

info@barracuda.com