FortiGate customer UWC: not a single security incident this year

The University of the Western Cape (UWC) reports that its Fortinet security solutions are proving so efficient that no security incidents have occurred to date this year.

Elroy October, Systems Administrator at UWC's central IT department, joined the central IT department five years ago, just as the university was moving from a Linux firewall to Fortinet solutions. Since then, UWC has had on average fewer than five incidents a year, and none at all this year, he says.

"Until five years ago, UWC was running a basic Linux firewall solution. But because UWC takes security very seriously, and in light of the changing threat landscape and a growing need to protect a vast amount of data, we sought a more effective solution that could not only increase data protection, but also support bandwidth management and reduce the time spent on managing the security system," Elroy October says. UWC wanted IPS, application control, advanced firewall features, antivirus and bandwidth management functionality with automation, effective dashboards for simplified management and simplified compilation of logs and historical data.

With around 300 servers in the UWC datacentre, a key need was to protect the server environment. "While tertiary education institutions may not be a prime target for attack, important personal information on students and staff, research and educational materials had to be secured. The website had to be protected from defacement, and the risk of fraud and cyber crime mitigated," says Elroy October.

The university also needed to manage bandwidth use, assign permissions for bandwidth and data access. Elroy October explains: "The FortiGate web filtering feature is particularly important to UWC. While the university is quite open in terms of what users access, it must have in place certain restrictions and must also manage bandwidth consumption and user access. With 25000 students all connecting through the UWC wi-fi zones, the cost of

bandwidth and risk of a downgraded user experience must be carefully managed. With the FortiGate bandwidth management feature, UWC does per IP bandwidth shaping, so supplying each user with a certain amount of bandwidth to ensure their usage does not impact on other users. Certain users, such as researchers, are allocated unshaped bandwidth."

With a relatively small IT team of around 50 professionals operating across various campuses in IT operations, application development, networking and service and support, UWC also needed a solution that was easy to manage and could be managed by IT professionals with a broad range of skills.

To meet these new needs, UWC installed two Fortigate 3910 A appliances in 2009, then upgraded to two Fortigate 3243Cs in 2013. UWC is now running the FortiGate 3240 C appliances in network address translation (NAT) mode, with two virtual firewalls BDOMs running in the actual hardware – one for VPN users, one for all other traffic. Running the devices in a cluster provides redundancy in case of device failure, notes Elroy October. UWC also subscribes to Fortinet IPS, application control, antivirus, vulnerability scanning and email filtering services and runs the FortiAnalyzer 1000b real-time network logging, analysing and reporting system that securely aggregates log data from Fortinet and third-party devices. This solution simplifies aggregation of logs and generating of reports, real time checking of logs and analysis of trends and performance.

Elroy October says the implementations were quick and efficient. The first implementation – during which UWC migrated from the Linux firewall to Fortigate 3810 A, involved the vendor testing the devices off campus, tweaking and streamlining the configurations for several weeks before actual implementation. Once testing was complete, installation was simply a case of plugging the appliances in. The upgrade to the 3240 C appliances was simpler and faster. Elroy October also underwent training on managing the new solutions. "The solution is simple to manage, but introductory training is recommended. Undergoing FortiGate professional training at the outset – with two weeks' Fortigate Admin and

Fortigate professional training and exams to fully understand the solution," he says.

The solutions have proved highly stable and effective, supporting UWC's needs and reducing the amount of time spent managing IT security, says Elroy October. "Due to the simplicity of its system management, only one Systems Administrator is needed to manage the appliances. With effective dashboards, automation and a simple GUI, the time required for management is significantly reduced, allowing for more effective use of resources. Now, I don't need to sit in front of device and monitor it the entire day – there are alerts if there is a problem. Changing policies or rules is a lot easier too," says Elroy October. "In addition, UWC's goal of managing bandwidth is achieved. The Fortinet solutions support effective bandwidth allocation and permissions management to ensure that all users enjoy high quality bandwidth access, while bandwidth costs are controlled. Reporting is simplified and important data is secured."