Layer 7, north-south-east-west traffic challenge SA enterprise security

Data centre security in South Africa is being challenged on a number of fronts, notably the move to Layer 7, and the need to lock down both north-south and east-west data centre traffic, says Fortinet.

By Paul Williams, Major Account Manager at Fortinet

Securing the data centre has never been more important or more complex than it is today – a fact South Africa's CIOs and IT managers are well aware of. The increasingly connected world, disruptive technologies, and the pace at which data centres must deliver business value are impacting operations, while at the same time the information security risks facing enterprises grow ever more sophisticated.

Recently, in a conference in which Fortinet participated, delegates focused on the changes impacting data centres, particularly the migration of virtualised workloads, increased changes in traffic types and patterns, new legislation, the introduction of IPv6 and the advent of trends such as mobility and "Internet of Things" which are revolutionising the way Enterprises operate and their employees work within these boundaries. Many delegates expressed concern about finding the skills necessary to secure the data centre in this new environment, about the lack of security awareness by end users, and about the ever-increasing exposure to operational risk.

Our customers across the region report that they are grappling with huge uptake of BYOD, creating a big problem for data centres security trying to cope with the influx of personal data and devices in the workplace. They also note that "Internet of Things" is already here, and is set to add billions of new connections to networks and significantly increase the potential attack vector – across smart devices, their associated networks and even their cloud-based management tools. With that, the large amounts of data that comes behind that raise management and control challenges, not to mention the new network speeds of 10, 40 and 100Gbps which are now being planned for the data centre.

Managing and controlling both north-south traffic in and out of the data centre and east-west traffic is also becoming increasingly important to IT managers with the advent of e-commerce B2B and C2B traffic.

Companies are moving their business applications to Layer 7 in the data centre, which brings on new user access methods and a multiple of new connections traversing the network, which in essence is creating higher security risks.

Locking down this environment without impacting the throughput and limiting business agility is driving a change in the approaches and technologies enterprises use to secure the data centre:

Automation and software defined networking are enabling improved and simplified data centre management and security.

Internal segmentation firewalls that control access by users, devices and network domains in effect 'containerise' the user, rather than attempting to lock down the enterprise within a perimeter, so enabling access control without hampering business agility.

Gaining full visibility and managing the distributed environment off a single pane of glass then allows for simplified, more effective security and enhanced reporting, which is important for audit,corporate compliance and determining ROI on security investment, and for future information security planning.

Business has moved into the cloud, which can make the environment easier to manage, but the other side of the coin is that it may also be easier to hack. By **isolating applications** within this environment, any attack in one area can likewise be contained and isolated.

A **focus on applications** is increasingly important. As enterprises increasingly develop their own applications, security and thorough testing must be given a high priority in the development process. Web application firewalls are also necessary, to protect the enterprise from threats that originate within the network, or to mitigate the damage and protect key resources from threats that get past traditional network perimeter defences; as well as to avoid potential liability should hidden malware on the company site impact the customer.

Enterprises also need to **revisit both skills development and staff training** continuously from a governance point of view. Security and data access policies and procedures need to be clearly spelt out to employees whenever new legislation like POPI comes into effect, and whenever new operating systems or applications are introduced or new cyber threats emerge.

/ENDS.