Top 8 Enterprise Network Infrastructure & Security Trends for 2015

By Perry Hutton, Fortinet Africa Regional Director

The networking and security industries are evolving rapidly. Here are Fortinet's views on the most important developments and technologies to look out for in 2015:

1. Security breaches are harder to stop

Security breaches and data leakage will continue to trouble companies of all sizes. The threat timeline over the last 10-15 years has shown that a new threat tends to be quickly answered by a new defence system. The threat then evolves, and a new defence system is needed. This has led to a myriad of disparate security appliances, software agents and management systems that in many cases are unable to talk to one other. When the bad guys tweak the Threat Life Cycle, for example via the creation of Advanced Persistent Threats or APTs, it becomes very difficult to stay ahead of the curve. Next-generation security architectures will integrate discrete security systems into a platform, which can correlate threat life elements and break the infection chain in different places.

2. Cloud technologies are finally taking root

All forms of cloud are starting to make inroads as a viable part of the enterprise infrastructure. Software as a Service (SaaS) has reached a tipping point as most organizations trust a provider's security capabilities. Infrastructure as a service (IaaS) is still focused on web applications for elasticity and redundancy. Cloud bursting, hybrid clouds and personal clouds will mean more sharing of distributed services, management and security.

3. **Diversity in mobile apps and management**

Unlike the PC market, the mobile device market (handsets and tablets) will not be dominated by Microsoft. There will be at least two to three platforms across the globe. This mobile diversity will

mean management systems will need to be more flexible and open. Improved JavaScript performance will begin to push HTML5 and the browser as a mainstream enterprise application development environment. This will lead to richer applications and more focus on their usability, rather than larger and cumbersome applications.

4. Software defined modular infrastructure becomes the norm

The control layer is being detached and centralized for many different parts of the infrastructure. Most of the initial focus is on the data center with virtualization, Software Defined Networking (SDN), Software Defined Storage (SDS) and standalone switch fabrics. The effect is that API's are being consumed at a much higher rate. In a world where the infrastructure is being dissected and segmented, API's themselves are very important but is also a potential security hole to the network element.

5. Internet of Things and Industrial Control Systems (ICS) collide

The Internet of Things (IoT) is already estimated by Gartner to be made up of some 26 billion devices by 2020. Industrial control systems are rolling out IP all the way to the control and measurement points. These networks are separate today and individual in nature. However, both need to deal with cyber threats, which can cause huge damage across industrial complexes, public operational networks (i.e. power grids) or consumers.

6. **Wireless continues to replace wired access**

Wireless access is ubiquitous across most organizations. New enterprise buildings are less and less wired. Wireless systems are becoming the primary network access control mechanism, meaning that tight integration with authentication systems is essential. Wireless technology itself continues to improve with ac Wave 1 now rolling out rapidly and Wave 2 on the horizon in 2015.

7. Networking bandwidth continues to double every 10 months

Networking bandwidth requirements continue to expand at a rapid pace. The transition from 1G data centres to 10G data centres took about 10 years. The transition from 10G to 100G will be much

faster. All parts of the infrastructure need to perform within the high-speed infrastructure. Traditionally CPU-based firewalls have fallen way behind the performance curve. More recently ASIC-based firewall appliances have taken a quantum leap in performance, allowing 100G interfaces and throughput in the hundreds of Gbps, saving space and power. Now high-speed networks can design security into the architecture without creating bottlenecks.

8. **Analytics for everything that's attached to the network**

Big Data and analytics can be applied for different reasons. The biggest need is business intelligence but it's also very important for security. The amount of data being gathered is staggering but segmenting the data can lead to more actionable results. For example, collecting WiFi presence of consumers in retail stores can lead to understanding their buying behavior. Monitoring where and when clients connect to the network can help determine security posture. Forecasting shipments based on real time data can lead to more efficient operations.