



Security: Not just a sprint to the line



Security effectiveness is critical, but performance cannot be

diminished. *Paul Judd*, regional director for Fortinet explains why bolt-on solutions won't champion any security objective.

IF ONLY everything was as simple as sprint racing. Point A to point B, as fast as you can, stay in lane, don't jump the gun. It's an uncomplicated business for sprinters, but if you introduce hurdles or, heaven forbid, a bend, you've got trouble. They don't even breathe during a 100m dash, because of the performance trade-off.

They might not know it but the Usain Bolts of this world accurately represent what's wrong with many network security strategies. The world has moved on from single point product solutions that have to concentrate on one thing at a time. IP traffic is as latency-sensitive as ever, but now it must traverse an assault course of network security obstacles. Security isn't as easy as a 100m dash; it's more like a track and field tournament.

Picking a winner

Picking out future winners in the security arena just a few years ago, you'd have made some impressive returns putting your money on the newly-coined security phenomenon of Unified Threat Management. UTM has since grown exponentially across all sectors (notably the high-end market at least as much as SME) to become a multi-billion dollar market within a very short space of time.



They might not know it but the Usain Bolts of this world accurately represent what's wrong with many network security strategies. The world has moved on from single point product solutions that have to concentrate on one thing at a time. IP traffic is as latency-sensitive as ever, but now it must traverse an assault course of network security obstacles. Security isn't as easy as a 100m dash; it's more like a track and field tournament.

During the same period, we've also experienced an explosion in virtualization and other technologies supporting the consolidation of hardware and processes into less places and smaller footprints.

The rises of UTM, and that of virtualization, share the same origins. Ever increasing traffic loads on converged enterprise and telco networks are making multi-gigabit the way to go; critical IP data like telephony, video and web communications are causing network managers to be more latency sensitive than ever. In the largest networks, convoluted 'point-product' security architectures create too much performance impingement. It makes perfect sense that with so much demand toward loading multiple security capabilities into the same place (ie UTM, or integrated network security), advantage is taken of virtualization to make those places fewer still.

Where does this leave 'athletic' security systems?

Straight out of the blocks, you've got to look at the security architectures as a team rather than an individual. In a point product set-up, those team members are separated onto their own exclusive appliance – or server-based hardware. With integrated network security, the team members are united into a single unit. The latter approach boasts efficiency gains for easier management, smaller power and space drains etc which are highly compelling – but what about performance? What about security effectiveness?

The maturity of commercially available network security technologies tells us that the individual 'team members' of any given solution are going to be broadly equal in stature. The

difference between the best and the worse comparable AV systems, spam filters and firewalls is narrower than it has ever been. If any team is going to perform, teamwork is essential. Ask Real Madrid how much success their mega-expensive squad of 'Galacticos' has won them, and you get the picture.

The most successful teams grow up together, learn together and can communicate extremely effectively. Communication underpins teamwork, which is why relay races typically result in calamity, and why market-leading products rarely interoperate. Running an alignment of point products creates obstacles to teamwork, but many integrated network security approaches also fall foul of this problem.

Security performance degradation

At the technical level, the transit of IP traffic going into one end of any network gateway security infrastructure and out the other side is going to involve a degree of packet disassembly and reassembly. This is one of the core principles of security performance degradation. Going through the same practice of disassembly/reassembly to check for a different security problem each time, results in lots of redundant processing. In other words, lots of wasted throughput capacity and lots of wasted time. Doesn't an integrated network security approach suffer from this? Well, not all examples of it.

As well as repeatedly queuing for packet assembly/disassembly, IP traffic typically has to deal with security functions based upon multiple, disparate source codes. Herein lies the interoperability question. Again, most

'cobbled together' UTM approaches suffer from this as much as point architectures do. The result is greater latency, greater risk of security ineffectiveness and complete confusion about the root of the problem should any failures arise. The shortcomings don't end there either. Any security system is only as good as the threat intelligence that constantly updates it. A given UTM vendor might do its own AV research, but contract out for web content filtering or IPS. Where does that leave you? Is that good teamwork?

Uniform architecture approach

True UTM is derived from a uniform architecture approach, in which each security function has been developed on the same source code, and can optimise security performance by eliminating redundant traffic processing. How? Through the use of specialised hardware based on ASIC technology to accelerate the security inspection process.

The development and application of specialised hardware security-specific ASIC processors to accelerate UTM has demolished institutionalised thinking around this security approach. Those harbouring lingering concerns about the applicability of integrated network security within their high-speed, real-time critical networks should only have cause to worry if they follow the wrong kind of approach.

Security effectiveness of course is critical, but performance cannot be diminished. Avoid compromise, put your money where your mouth is, you can't pause for breath in this game. Only teamwork wins success. **Vital** www.fortinet.com