BIZCOMMUNITY

Service providers are facing a new security paradigm

By Martin Walshaw

3 Mar 2016

Mobile World Congress 2016 took place last week and what came of it was largely the industry is looking ahead to what the future brings. From new devices to new apps to new services - it's not a surprise that the theme for this year was 'Mobile is Everything'.

One topic that I heard a lot about is security. That's because it's something that affects users and service providers alike; and as the industry grows so too will security threats. Cisco's VNI report predicts that IP traffic will triple between 2014 and 2019.

South Africa and Saudi Arabia will have the highest IP traffic growth rate with a 44% compounded annual growth rate from 2014 to 2019. According to the report, that means 'enhanced security and intelligence [will be] required' to deal with all the new devices that will be connecting to networks.

It's not just the devices; as the networks themselves are re-architected, new threats will emerge. And as the new networks emerge, develop, and scale, service providers will also have to scale their security architectures to keep up with the threats. The two simply have to go hand in hand. So it's scaling, performing and providing security at the same time.

Changing approach

The nature of security approaches is changing rapidly, from being perimeter-oriented with well-defined borders to protect to now being more dynamic in nature with granular requirements across the network, the devices, and the applications. The simplistic approach of placing a security appliance in front of defined perimeter is a thing of the past.

As networks evolve, as they become more virtualised, they will also get more 'open' and network services will continue to become more dispersed. The next generations of devices will also have much greater capabilities and different usage characteristics - where increased connections to the network will be accompanied by exponentially higher connections per second.

This will impact the scaling of security architectures like never before as devices will be launching multiple sessions that are going to touch different domains of the network and increasing rates. Next-generation networks need to support these different traffic models and different security solutions will also be needed in order to accommodate all of this.

However, the issue lies with the fact that many security platforms on the market were not designed to meet the security requirements of 4G or 5G, with the sheer volume of data that will be flowing across networks and the frequency of application access and connection rates.

Mitigating attacks

With these new networks service providers will need to secure all points of the network in real-time and on a dynamic basis. They will need to mitigate DDoS attacks and device-oriented attacks, and absorb high volumes of traffic while quickly detecting and shedding bad traffic.

And as networks evolve and become much more dispersed, they will also have to quickly detect threats and dynamically push out IP blacklisting and other mitigation techniques upstream to other network and security elements. So, if threats are detected in one portion of the network, a mitigation policy can dynamically be pushed out to other points on the network, so you don't have to rely on someone having to first detect and then manually push that policy out, which could take days, weeks or even months.

It really is a new security paradigm that service providers will be facing; high performing solutions that can offer a multi-domain and multi-layer set of services that can be deployed across the network. Ultimately, as service providers evolve to 4G and 5G where they will be deploying incredibly high-performing networks, they also will need incredibly high-performing security.

ABOUT MARTIN WALSHAW

Martin Walshaw is a senior engineer at F5 Networks and has multiple accreditation from being a CCIE to being a CISSP to being an F5 Certified Professional. His background is in security, but he has also has skills in multiple different areas including unified communications, application acceleration and optimisation.

- Visibility: your top defence against rising cyber attacks - 7 Jul 2016
- How context can provide application-centric security - 30 May 2016
- The challenges and benefits of hybrid cloud migration - 12 May 2016
- What does SSDC mean for your business? - 28 Apr 2016
- Check your blindspot on the information superhighway - 13 Apr 2016

View my profile and articles...