Customer

Industry

Managed Services

Challenges

- *Mitigation of DDoS Attacks*
- *Lack of network Insight*
- *Customer reporting*

Deployed products

- *Flowmon Collector 2000 VA*
- *Flowmon DDoS Defender 10Gbps*

Solution benefits

- *Immediate mitigation of distributed denial- of-service attacks*
- *Improved network insight to usage patterns*
- *Customizable reports to meet the requirements of its customers*

Contact

www.aspirets.com

Aspire Technology Solutions

Aspire Technology Solutions is an award-winning managed services company specialising in hosted services, data centre solutions, communications and IT support. Established in 2006 Aspire have grown organically year on year with 95 highly trained staff and now have sites across the North East and London. Aspire provides personal services and avoids selling pre-packaged products. This customer-focused approach has enabled Aspire to attract business from a wide range of prestigious organisations across the UK and Europe.

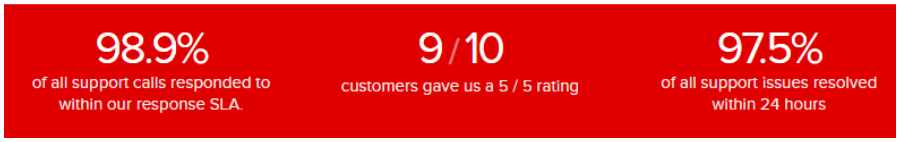

Figure 1: Latest Aspire's statistics

Customer situation

Aspire started to become the victim of several large volumetric style DDoS attacks, aimed at both its network and the networks of its customers. Dealing with these attacks was a manual and time consuming process, and due to the sheer volume of some of the attacks, the disruption was not limited to the attack target – traffic of its other customers could also be affected. It could take up to an hour to fully mitigate the effects of a large DDoS, an unacceptable amount of time when striving to provide a first class service! Aspire understood the urgent requirement to deploy an effective and automated solution to enable it to mitigate the effects of any future attacks in a fraction of the time!

Flowmon solution deployment

Aspire deployed a Flowmon appliance in order to receive Netflow data from its core routers which, among many other benefits, allowed it to easily and quickly identify the attack target of any volumetric style DDoS attacks, and set up mitigation techniques.

Within weeks of setting up a proof-of-concept solution, a real attack occurred. Aspire were immidiately alerted to the attack, and at the click of a button were able to deploy Flowmon's mitigation technique based upon BGP advertisements that allowed Aspire to blackhole the attack target's IP at its borders, and also instruct its upstream Tier 1 ISP peers to do the same instantly. This reduced the time from attack to mitigiation from around one hour to a matter of minutes.

Having been satisified with the speed and accuracy of the Flowmon device, Aspire then enabled automatic mitigation so that any further attacks could be mitigated even sooner. Multiple further attacks have now all been effectively mitigated in approximately 30 seconds from the attack start!

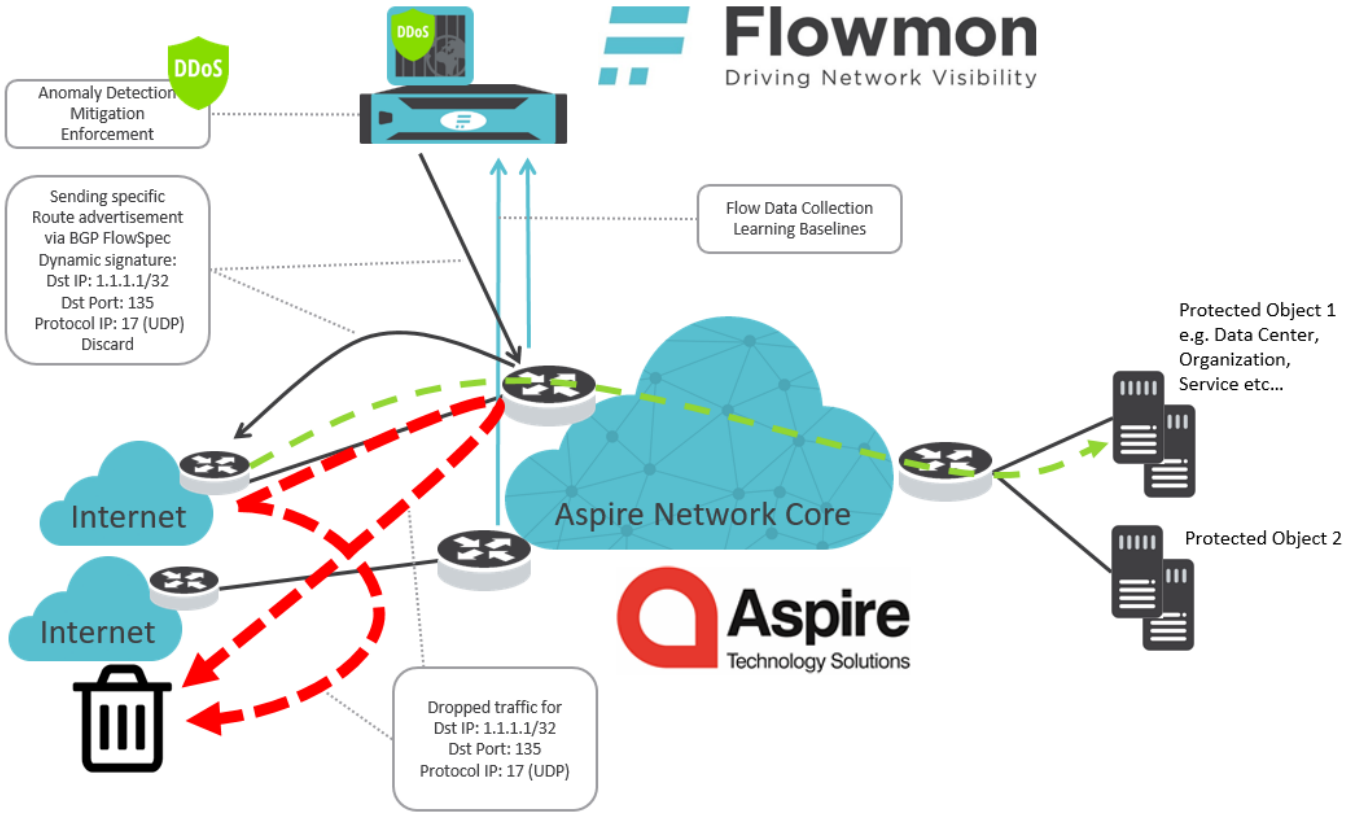

Figure 2: Deployment architecture

Customer review

David George, Network Convergence Consultant at Aspire Technology Solutions, summarizes the Flowmon solution deployment as follows:

"Flowmon has completely transformed the way we deal with DDoS attacks – it has gone from being a very manual and time consuming process to being a fully automated solution with effective mitigation in under one minute. After turning on automatic mitigation, it was actually very difficult to see from our normal monitoring platform that an attack had even occcurred! After several months of deployment, the frequency of attacks has diminished significantly, perhaps a sign that the attackers are aware that their efforts are no longer paying off?

During the early phases, we had concerns that false positives may cause us to start black holing a whole range of IPs and causing us further problems, but due to Flowmon's sophisticated learning algorithms and minimal bandwidth criteria, these fears have been unfounded - we have never had a false positive yet!

While our primary reason to purchase the appliance was for its DDoS defence capabilities, it has acutally given us much more insight into the traffic patterns and nature of our network, with customisable reports providing us with a wealth of data allowing us to see who the heaviest users are, what's consuming the bandwidth and which external networks we transfer the most data with.

Overall, an excellent product with great support!"