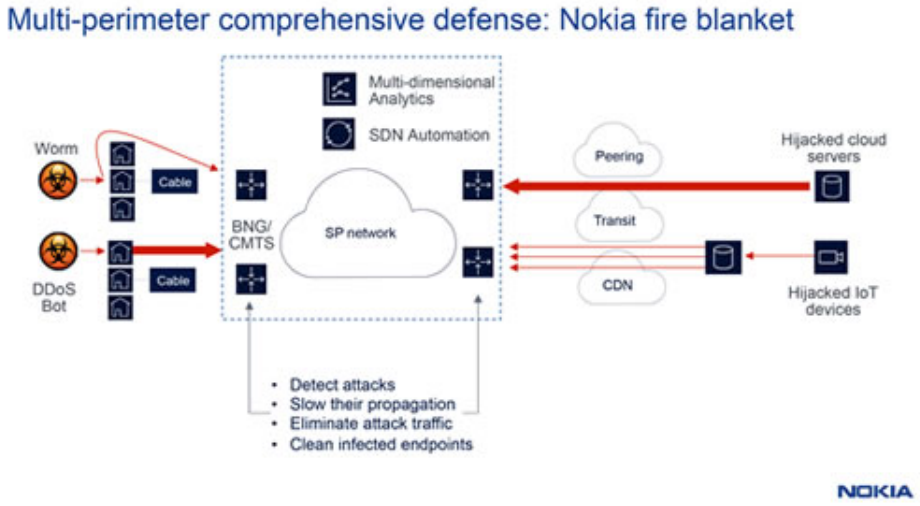

The newspaper headlines are warning of a DDoS Armageddon. Hackers routinely take on ISPs and webscale companies just for sport, bragging about their exploits on the dark web. Meanwhile the scale, frequency and sophistication of DDoS attacks grows daily, creating costs in time and technology, while customers light up call centers complaining of service slowdowns. In response, many providers are throwing money at the problem, putting more and more into specialized hardware and beefed-up scrubbing centers. This is not only expensive; it is also not enough.

Many will remember the recent DYN attack. It was the first of its kind that exploited cloud and IoT security holes to devastating effect. Over 100,000+ IoT devices were hijacked and reprogrammed to participate in the attack. Some created a surge of traffic using DNS reflection techniques, others contributed to the attack stream by redirecting their video feeds to join. At the same time, hundreds of cloud servers with 10 Gbs uplinks were compromised and used to launch a simultaneous TCP/IP attacks. The result was a multi-vector, terabit scale attack that was complex and massive enough to punch large holes through traditional DDoS defense architectures and bring the internet to its knees for several hours.

The problem is that traditional DDoS defense solutions were simply not designed for the cloud and IoT era. To start with, DDoS detection is too simplistic to keep up with these types of sophisticated threats. Specialized detection appliances that look for abnormally large spikes in traffic flowing towards specific IP addresses. Hardware detection lacks the raw compute necessary to perform the additional analytics required to determine if surge in traffic is a real attack, or a valid event like a large file transfer from Amazon's AWS. This leads to false positives and negatives, with real attacks allowed to pass through, and valid application traffic

dropped. Some providers, especially those in gaming where even small amounts of lag can create havoc, have attempted to address the issue of false negatives by deploying far more bandwidth then they need. The hope is that the extra bandwidth will absorb the attack stream so that links are not saturated and customer experience is not impacted. Experience has revealed this approach to be economically unsustainable, and far from foolproof.

Once a bandwidth surge triggers detection appliances, all traffic headed to IP addresses that are potentially under attack is directed to centralized scrubbing centers where it is cleaned by racks of specialized mitigation appliances. This is a slow and manual process. Keeping up with multi-vector attacks that can change minute by minute is difficult, and hackers are free to cause mass disruption until all vectors are identified and stopped. Scale and cost are also big problems. With attack traffic now regularly crossing the 1TB/s level and continuing to grow, providers must continuously up their investment in bandwidth and appliances, or deal with insufficient coverage.

Fortunately, there are new approaches to DDoS defense that allows providers to use the edge routers they already own. Making them smarter about mitigating threats starts with liberating detection analytics from hardware appliances and placing them in private or public clouds where they gain infinite scale and context.

Virtually all customers we encounter are looking to replace detection appliances with software-based multi-dimensional analytics so they can detect attacks faster and more precisely. Looking, for instance, at ratios of packet types and DNS data streams helps to more precisely identify the nature of a large spike. Multi-dimensional analytics get even better when they have visibility into all cloud applications and services so you can instantly understand where the traffic is originating and whether it is likely to be friend or foe. Is it HBO releasing the season finale of Game of Thrones, for instance, or Amazon moving bulk traffic between its data centers? Or is it a genuine DDoS attack? Multi-dimensional analytics can provide the answer in seconds. Additionally, big data techniques can help compare a potential event to past attack profiles and be more precise about what degree of variability from ‘normal’ is OK.

Armed with this kind of analysis, it enables the use of simple filters like Access Control Lists (ACLs) at the peering edge to drop traffic originating from the zombie PCs, IoT devices and/or cloud servers that are carrying out the attack. The offending traffic is dropped almost as quickly as it is detected, before it has an opportunity to enter the network. Recognizing the pivotal role that routers can play in DDoS defense, some vendors have gone a step further by introducing a new generation of network processors that can run millions of comprehensive DDoS filters, without impacting performance. They can filter with far greater scale and cost effectiveness than DPI appliances, and they dont have to backhaul traffic to a scrubbing center to do it. The routers can be dynamically programmed to look for patterns in an IP payload that reveal

IoT-based DNS attacks, and to use the same filter to root out the attack traffic when using ACLs alone is insufficient.

Combining multi-dimensional analytics with smarter, DDoS-capable routers translates to more precise detection and faster response times, especially since providers now have the means to start automating the mitigation process. There is no need for expensive backhauling and scrubbing to handle the volumetric attacks that constitute well over 90% of attack traffic – these are stopped at the edge of the network, before they can impact services and customer experience. From a bottom-line perspective, providers can significantly reduce spend in backhaul infrastructure, better leverage their investment in peering/edge routers, and refocus scrubbing center equipment to what it does best - complex stateful analysis of application level attacks that constitute the remaining 10% of attack traffic.

Finally, it's not just attacks from the internet that are a problem. A number of ISPs are reporting attacks against their infrastructure that originated from inside their security perimeter, from their own subscriber base. Attackers are starting to use vulnerabilities to plant malware in PCs and to hijack IoT devices in a provider's subscriber base. This malware quickly propagates, and in a short period of time, accumulates enough firepower to launch an attack on the ISPs internal infrastructure. And since today's DDoS defense architectures have a Maginot Line defense strategy – build a wall in the one place you expect the attack to happen and don't bother with the rest - once an attack originates from within the network, there is literally nothing there to stop it.

The solution is to assume a 360 degree attack perimeter. Turn the analytics around to detect attacks and malware propagation across multiple boundaries – your subscriber edge and server farms, as well as your peering edge. Routers can provide assistance at multiple points in the network by looking for payloads that have attack signatures. Once internal attacks are detected, automated mitigation can throw a fire blanket on the network to slow them down. For instance, attacks coming from a cable or DSL subscriber base can trigger an SDN policy that configures a BNG or CMTS to rate limit infected subscribers until the provider can get them to clean their PCs, or reboot their IoT devices.

This is a high stakes game which isn't ending anytime soon. As hackers embrace cloud and IoT to up the scale, frequency and sophistication of DDoS attacks, different methods have to be employed to ensure manageability and, ultimately, profitability. Some of these security tools and approaches are new, such as multi-dimensional analytics. Others, such as your edge routers are already in place and purpose-built for filtering and routing packets at wire speed. As long as you have the deep analytics to make them smarter, they should be your first line of defense.

To find out more, download the Nokia white paper on insight-driven automated networking.
nokia.ly/insight-driven-automated-networking