Behind NTT Com's network security roadmap

Michael Wheeler, EVP of the NTT Communications Global IP Network at NTT America, spoke to Jason McGee-Abe to discuss how automation is the final piece of the puzzle for its DDoS Protection Services (DPS) offering

The first day of the Capacity Asia conference saw NTT Com announce the launch of an upgraded detection solution, DPS Detect, to enhance its distributed denial of serviceDDoS protection services. I booked in some time with Wheeler in NTT Com's meeting room, which overlooks Hong Kong from the fortieth floor of the Conrad Hotel.

We immediately discuss the news that customers of NTT Com's global IP network can now select the level of mitigation support that best fits their cyber security strategy, helping them to detect potential attacks directed to their networks and initiate mitigations faster.

The new DPS Detect solution option provides an advanced level of service above DPS Core as it adds detection capabilities to help identify potential attacks using state-of-the-art technology while working with customer-defined thresholds.

"Network security is one of the top priorities for our company," starts Wheeler. "As DDoS attacks continue to grow in frequency, size and complexity, it is important to give our global IP network customers more solution options and the opportunity to choose the level of support they need."

As customer requirements have evolved, and the types of frequency of attacks have grown, Wheeler says there is a real need to further expand the product in terms of features and functionality.

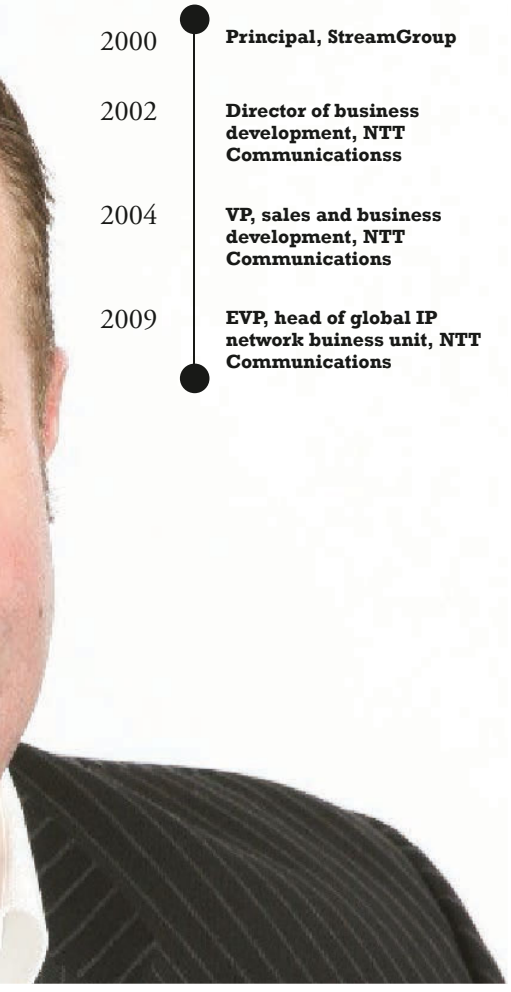
Subscribers to DPS Detect also have access to the Network Security team and enjoy exclusive use of the company's DPS Portal, a platform where they can request or self-initiate mitigations based upon a DDoS detection alert, review past mitigation reports, and request configuration changes. "DPS Detect goes deeper into how customers can interact with our infrastructure, letting them trigger their own mitigation as opposed to going through NTT Com's own network security team," he adds.

DDoS attacks can strike at any time, potentially crippling network infrastructure and severely degrading the performance and reachability of a website or other IP-accessible assets. The expanded DPS suite of services will enable global IP network customers around the world to easily customise the level of service and assistance that best fits their needs, which can vary vastly.

The DPS roadmap

Expanding the product line has been carefully planned as part of a roadmap developed by NTT Com around one-and-a-half years ago, Wheeler explains. NTT Communications first launched its original DDoS protection services product and since then it has slowly evolved. "Fast-forward to today and we're seeing another phase of our roadmap being rolled out."

DPS Control is an entry-level tier of service that provides support on access control lists (ACL) and is intended for customers that don't require full mitigation assistance. Using the service, customers can define permanent ACLs which are deployed on its NTT Com interfaces to block a network from certain types of traffic as defined by the customer.



2000 **Principal, StreamGroup**

2002 **Director of business development, NTT Communicationss**

2004 **VP, sales and business development, NTT Communications**

2009 **EVP, head of global IP network buiness unit, NTT Communications**

"We developed the Core tool as we had heard from some of our biggest customers that they needed something that was scaled down, essentially that didn't have all the bells and whistles but still had the functionality that they had in the original product, Core, to help provide for things like Act Control Lists (ACLs)," the NTT EVP adds. "That was relatively easy so the rollout and implementation was fast as it just required some restructuring from a product capability point of view.

In turn, DPS Core, is an enhanced level of service beyond DPS Control for customers that require full DDoS mitigation support. DPS Core is supported by NTT Com's Network Security Team, the same expert team responsible for keeping the company's tier-1 global IP network (AS2914) infrastructure safe and secure.

"Prior to this there were some tools which were free of charge and provided to customers, including blackhole routing," he says. NTT Com's complete suite of proactive DDoS attack solutions, that also includes blackholing capabilities and access control lists, are designed to support multi-threat security environments on a single best-in-breed platform, with sufficient capacity to combat large-scale attacks.

Wheeler says that it was feedback from its customers coupled with where the company saw the industry is heading towards that were the catalysts to developing the DPS offering. About one-and-a-half years ago we took a step back to take a look at what we needed to do and that's when we put a comprehensive roadmap together for the overall product as a family as opposed to a singular product.

There's no one-size fits all solution and in many instances, companies are using two or three mechanisms to address DDoS attacks. "In the old days the easiest way was for someone to have over-capacity, doing it out of pure volume. So they would buy more capacity than needed so if an attack came through the volume wouldn't affect them. That was a very simplistic different time for network security compared to what we have today," Wheeler recalls.

> ***"When we're able to include the automation components that'll make things even better"***
>
> **Michael Wheeler, EVP, head of global IP network business unit NTT Communications**

"It's not just purely about volume, although it can still be a big cause for concern, but there's a lot of precision that occurs with attacks today that did not occur before. That's not a fail-safe option that works for everyone, particularly in an age with multi-vector attacks or more sophisticated attacks with smokescreens. That will inevitably continue, but that's the battle you fight as a network provider."

Automation: the missing piece

NTT Com has developed a product family here but how is it going to be enhanced further? "Automation," Wheeler quickly responds.

DPS Detect is really a number of steps into that progression in providing enhanced services, more self-control for the customer and more visibility to what NTT Com is doing from a network infrastructure point of view in regards to DDoS mitigation. "But we have another product that's part of the same roadmap that we aren't announcing yet, but it'll be a further step into much higher levels of automation between our infrastructure and a customer's infrastructure," Wheeler says. "That'll be an even deeper enhancement and set of capabilities that customers don't have today even with Detect."

I ask if the fourth tier of its roadmap, the auto-mitigation tool, will be launched in time for ITW 2018 in Chicago and Wheeler says "things are on track and that is certainly a possibility". "So in 2018, we'll have four tiers of DDoS mitigation services for our customers and they can pick the appropriate capability and functionality based on whatever their profile requirements are as a customer. When we're able to include the automation components that'll make things even better."

Separate from this product, over the last year NTT Come has deployed new infrastructure and enhanced the overall capability and ability to manage capacity volumes. "There's been a 400% increase in scrubbing capability that has been added globally," he adds. This enhancement has taken place over the past three quarters and there are still some more pieces of infrastructure to be deployed.

Wheeler is adamant that it won't rest on its laurels and reveals that the company has already started collaborating with NTT Security and looking at more predictive capabilities.

"We're pretty happy where we are in that process, customer feedback has been very positive and we're close to beta trials for the fourth product," he says. "These are being developed concurrently not sequentially as part of the roadmap. But we're not going to sit back now, we'll go from strength-to-strength."

NTT Com's sister company, NTT Security, works with the back-end and is looking heavily at more machine learning and AI capabilities. "That collaboration is something we would like to explore and perhaps push the envelope on regarding enhancing the product, its capabilities and perhaps services that we could provide customers which are predictive in nature," Wheeler says. He admits that it is not close but it's certainly a possibility.

As NTT Com pushes ahead with enhancing its security options for its customers, it is also still keeping its flexibility. DPS Detect is yet another way that is helping Wheeler and his team to differentiate themselves in the market and we look forward to seeing the details of next auto-mitigation capabilities rolled out.