SPONSORED CONTENT

ARE YOU STILL TALKING ABOUT SDN? WE'RE DOING IT.

But it's a very different creature from when software defined networking was first discussed and (glibly) defined as open, programmable networking. In its life it's gone through some troubling moments (too complicated, not enough vendor support, incomplete ecosystem). And been the brunt of some (lame) jokes: what does SDN stand for? Still Does Nothing. Or twisted into Security Defined Networking – what is that?

Carolyn Raab, co-founder of Corsa Technology puts forward the case for SDN

I want to put forth the definitive SDN acronym standing for "Simply Defined Networking". We all have learned a tremendous amount over the last few years. And I believe it has lead us to this very important point where we actually do understand SDN properly and we have identified that a crucial underpinning of the success of SDN is to keep things very, very simple. Whether you are dealing with routing at the core of the network or network security at the perimeter, open programmable networking must be synonymous with simplicity. I'd like to highlight a couple examples of this simplified networking in action.

Deriving Flexible, Dynamic Networks and Services

Let me start with the success of GÉANT's Testbed as a Service offering as a prime example of SDN.

"GTS is designed to support research teams investigating innovative SDN solutions and needing a high performance distributed infrastructure. GTS can simultaneously support multiple projects and isolates them from each other and from the production GÉANT network to provide security and safety. The network testbed resources are dynamically allocated from real e-infrastructure distributed throughout the GÉANT core service area allowing researchers to define, build, test and rebuild highly scalable, high capacity virtual networks quickly, easily and cost-effectively."

In essence, GTS is a very programmable, dynamic network. What is running in behind the scenes (the real infrastructure) is perfectly simple, openly programmable, high capacity SDN hardware with virtual forwarding contexts that can be spun and down via compact, dedicated controllers for each defined service offering.

Instead of trying to create one overlord controller that can do all things for all people, GTS took an SDN approach that allowed them to cut down the problem space into simplified, bite-size chunks that could be readily implemented, were logically isolated from one another and (as important) maintained over time.

When a researcher requires network resources, GTS provides dynamically provisioned network environments consisting of computational servers, data transport circuits, and switching/forwarding elements. These environments become unique testbeds for each researcher which can be scheduled in advance and are selected from any of the GEANT core points of presence that have GTS services available. Each testbed constitutes an isolated and insulated virtual environment that can function autonomously from other testbeds or other production services. Keeping it simple for the user of the service, they need only create controller software for their particular network environment, independent of other services and functions on the network.

Securing Networks with Disaggregated Network Security

If we turn to network security, SDN is also able to play an important role in evolving how networks are protected. Instead of trying to force everything into monolithic, complicated platforms, disaggregate network security the SDN way. Rethink network security built on a performant yet simplified flow-forwarding hardware appliance that excels at traffic export for data acquisition and network statistics as well as traffic enforcement for precision traffic filtering to maintain integrity of the network. And put all the best, super capable analytics, policy and smarts into the software cloud (where they should be).

In this context, we call the flow-based appliance a Network Security Control Point and it follows the SDN evolution seen in networking architectures of separating data plane (for network security, it's data export for visibility and filtering for enforcement) from control plane (software analytics). The control point is a transparent, in-line L3/L4 network security device that is simple to use and universal in that you can place it anywhere in your network, to perform any security action, and that it uses open interfaces for everything it does.

We can then use the foundation of a SDN control point for network security service chaining that works at scale, in a manageable way. We all acknowledge that true dynamic security service chaining for the network core is proving to be challenging. Network architects and security engineers are challenged to develop real-time defenses that ensure their networks always operate with integrity and are properly protected. They are looking to create dynamic security service chains in the network to be able to spin up and down the right type of network security, at the right time and for the right segment of the network.

A network security control point drops into any existing network today with no reliance on changes to the control plane whatsoever, and it uses simple vlan tag switching for forwarding. It is elegant in its simplicity, which has pushed the complexity of previous attempts out of the problem. And at the same time it is a really powerful architecture that allows you to service chain virtual security instances or existing appliances to do pretty much anything you like when it comes to securing and protecting your perimeter.

I believe simplified networking is on the cusp of becoming broad spread. I look to initiatives beyond GEANT's testbed service that are destined for the production side of the network that are part of this trend. Network operators' efforts will focus on the applications and the underlying network and its security mustn't be a distraction. Keeping next generation networks simple will be very important for that. We need to all pull together to make this happen.

Corsa is proud to be a sponsor of TNC 2018. We will be there to share real 100G network security service chaining learnings, perimeter security concepts and SDN routing examples. We are actually doing it and will show live demonstrations of (perfectly simple) SDN!

Carolyn Raab

With over 25 years industry experience in the networking and communications industry, Carolyn brings to Corsa product management, sales, marketing and business development experience in networking and security markets. As a co-founder at Corsa, Carolyn has enjoyed all the twists and turns of SDN in the last years and has presented at previous industry conferences on various topics around SDN.

With the growth of cloud and network traffic, network security is taking a front and center seat and this is where Carolyn now spends most of her attention.