CORSA

SPONSORED CONTENT

WHAT'S WRONG WITH THE SWISS ARMY KNIFE?

HOW SDN CAN DELIVER FLEXIBLE, FUTURE-PROOF NETWORK SECURITY ARCHITECTURE

Swiss Army knives are the quintessential symbol for an all-in-one device. But really they are only as good as the functions that were thought up ahead of time, then added once and for all to the knife.

If you don't buy the one with the scissors, then there's no adding scissors later on when you need them. Network security is no different. Fixed function firewalls, fixed function routers, load balancers and packet brokers are all feature rich but only if the manufacturer designed the feature in (and you pay to turn it on). Handy up until now but not sustainable going forward.

Words
Carolyn Raab, CORSA

Enter the Software-defined Firewall Solution

What we need is a better way to add flexible, dynamic, adjustable security to the network. It's all built on SDN principles and harnesses the dynamic power of SDN service chaining to build out network security that provisions functions virtually – at any scale. It's called a software-defined firewall solution and it makes you think about the practicality of Swiss Army knives going forward.

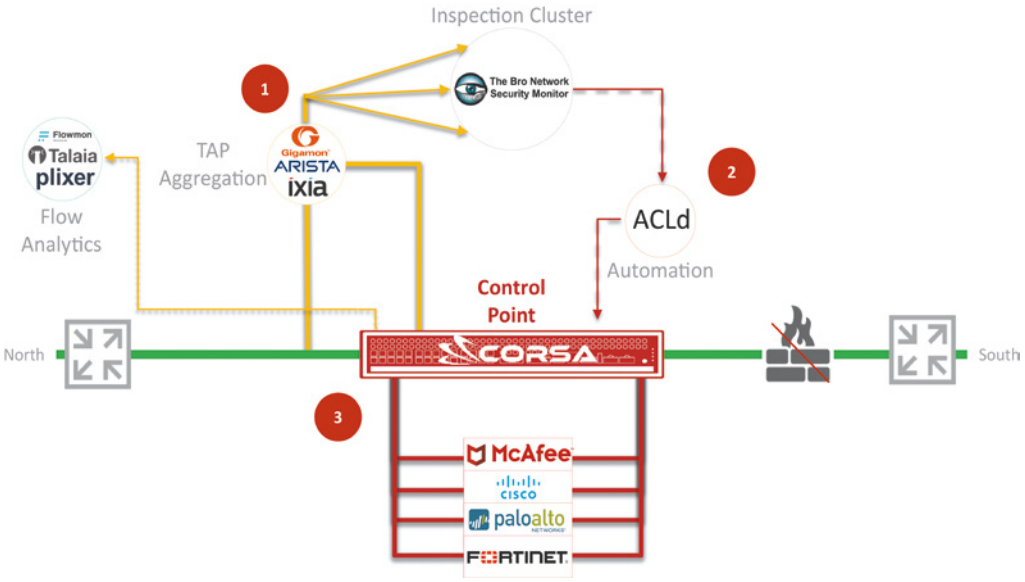
But recall Simply Defined Networking (SDN) core principles

It has to be simple to start. If you have been embroiled in NFV, you know the despair of the sinkhole of service

chaining. We need to avoid that and learn from the important lessons of SDN in the networking space.
So before creating the Nirvana of network security function service chaining that will ultimately be your software-defined firewall architecture, begin with basic firewall offload. Take your network gateway as an example where, in so many cases, the firewall is running hot and there is no relief in sight. Adding more deny rules is not an option. Because it's more or less a fixed function, your choices currently are to keep rushing from emergency to emergency as your firewall overheats, or to spend money and move to the next size of firewall. But consider moving to software-defined firewalling, where Step 1 is to offload your current firewall with a programmable, in-line control point sitting just ahead of your firewall that acts as a pre-filter to the firewall (you can call it 'The Hammer'). And then over time evolve your network security capacity by adding dynamic software-defined security functions as an extension of that same programmable control point.

Steps 1 and 2 of a Programmable Network Security Architecture

Too much time in SDN and NFV is spent on theory. Let's consider a specific software-defined firewall architecture and start with Step 1 which is the simplest, most economical approach to vastly reducing your network exposure to the Internet's badness. For this step you need traffic inspection and it can be what you currently have in place. Bro Network Security Monitor provides an effective, scalable open-source inspection engine that is able to horizontally scale to any size network. Typically, traffic is replicated in the network using simple and economical optical taps. Then it is fed into a Bro cluster via tap aggregation infrastructure. For those wanting more information, there are multiple existing solutions on the market and best practices for building tap aggregation infrastructure as well as deploying Bro clusters. If desired, other inspection technologies can be used, both open-source and commercially available.
Next is step 2 when you need the ability to block traffic ID'd as malicious by your BRO analytics. Corsa NSE7000 is a unique device on the market that is able to block every possible IPv4 entry using its GigaFilter ACL without compromising speed or performance. NSE7000 is controlled via simple REST API which allows for full automation of enforcement from a Bro cluster using ACLd. This two part approach is a high performance yet cost effective way to protect any size network without compromising throughput that works for high speed links with or without existing firewalls.



Evolve at your own pace

Steps 1 and 2 get you extremely effective gateway enforcement while you begin your next phase of network security. Optionally, there is a mid-step for network and security architects looking to improve the accuracy of their anomaly detection and analytics. The NSE7000 Control Point is able to feed unsampled IPFIX data to up to 4 collectors simultaneously. This provides additional visibility for security teams at the level they haven't had before at no additional cost.

3-Steps to a Software-Defined Firewall Architecture

Step 3 is where the major benefit of this new security architecture really takes hold. It is the ability to horizontally scale other in-line inspection devices. You no longer need to buy a bigger in-line device every few years, but rather you can add more devices as needed. NSE7000 supports service chaining of both physical and virtual appliances. It can redirect traffic into up to 512 different service chains based on any Layer3/Layer4 policy. At the same time, NSE7000 can symmetrically load balance the traffic in both directions between up to 128 instances of the inspection appliance within each service chain. So physical and virtual IPS, NGFW or SSL Visibility appliances can all be incorporated into this architecture without compromising speed or performance of the network.

Start Simple, Stay Simple: 1-2-3

The NSE7000 acts as an enforcement point, a traffic visibility and monitoring point as well as a redirection point for service chaining. Because it sits as a transparent in-line device inserted into the network, these different functions can be turned on separately and independently over time, without requiring any redesign, or network re-architecture.

When network security is built up on a software-defined platform, it is inherently programmable. This programmability can start simply with a pre-filter function and be expanded over time to increase functionality and add new features in service chains. This is the beauty of a software-defined firewall architecture because it eliminates the need to define all your features up front and have them baked in to the Swiss Army Knife. It allows for dynamic, scalable security that evolves programmatically with changing threats.

Find out more at **corsa.com**

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.