AN INTERVIEW WITH EDUARDO CERVANTES
CEO, CORSA SECURITY

SCALING NETWORK SECURITY WITH VIRTUALIZATION

NETWORK traffic inspection has evolved from simple firewall appliances blocking bad IP addresses to more sophisticated next generation firewalls (NGFW). And this worked well enough until a new killer app has arrived on the scene: SSL/TLS encrypted traffic. And now the reality is inspection is not keeping up. The combination of SSL/TLS adoption and huge bandwidth demands is resulting in decreased inspection capability for high capacity links. We find ourselves with a model that is broken where the traditional approaches to inspection aren't working.

Corsa Security has its roots in SDN and sees network security through that lens. It is enabling the transformation to scaling traffic inspection and security services by using two of their oldest tricks: horizontal scaling and virtualization. We recently chatted with Eduardo Cervantes, CEO of Corsa Security, to learn more about how his company is addressing network security virtualization, something we have often referred to as software-defined network security.

EA Your team has been well-known for scaling SSL traffic inspection and load balancing. Before we get into your newer capabilities, tell us about how these functions are supported at Corsa.

EC With the exponential increases in traffic volumes, and with most traffic now being encrypted – by some estimates, over 72%, even the largest security devices suffer from an unacceptable performance degradation when trying to decrypt SSL traffic. The result is an SSL inspection gap, which reflects the point where an enterprise can no longer decrypt incoming traffic and also maintain sufficient levels of network performance. To address this problem, our team at Corsa has developed a security services load balancer that provides a simple way to scale SSL/TLS inspection capabilities horizontally. It redirects traffic into multiple virtual security appliances, so that operators of high-throughput networks can gain full visibility into their SSL/TLS traffic.

EA You've embraced the concept of security service chaining in the context of virtualizing network security. Help us understand how this provides Corsa with such powerful capability.

EC Service chaining is an important component of our software-defined network security vision. It supports dynamic scaling of network security services, and this goes beyond just traffic inspection. Service chaining also supports dynamic creation of per-tenant security. On the road to the development of chaining, we started with a fully turnkey network security virtualization platform that economically scales up virtualized firewall instances, on-demand, to maintain 100% traffic inspection, under all conditions. In other words, we essentially created a virtual NGFW that elastically expands and contracts inspection capacity to meet demand. It's the tight integration of the elements of the platform – namely, the load balancer, commodity server, virtual firewall instances from leading vendors, and the Corsa virtualized infrastructure manager – which produces a solution that is instantly usable by the customer. This packaged approach to virtualizing network security is compelling, because network and security engineers can focus on policy and performance while the platform takes care of inspection capacity. Then, as networks establish the use of virtualization for traffic inspection, the Corsa platform can support the evolution to multiple security services and chaining those services into per-tenant security service chains.

EA Is it possible, given the vantage point of your Corsa platform in a typical architecture, for firewall functions to become embedded into the platform itself?

EC Firewall functions are crucial for the Corsa platform, which is tuned specifically for the demands of dynamic firewalling. Our integrated virtualization solution uses load balancing to redirect traffic into virtual firewall instances, and builds up an entire security stack using commodity compute and a VM manager. The firewall functions are more overlays than embedded, in the same way that a mobile application becomes an overlay to a handset's operating system. Beyond firewalls, we are also evolving the same platform to support any type of virtual security service, like IDS or IPS. Our platform can thus be viewed as the operating system and compute function for a network security system. When new inspection capacity or security posture is required, a virtual NGFW or any other virtual security service can be added just as one would add applications to any OS. It is a simple matter of software-defining the new security position, which no longer requires any form of hard wiring or physical appliances and offers far better TCO.

EA You've done some interesting partnerships recently. Tell us about these integrations and how your customers benefit.

EC As a turnkey virtualization platform, we are the optimized infrastructure integration that economically scales network security. It's our technology alliance partners who bring decades of security inspection intelligence. We have integrations with firewall, IDS, and IPS vendors. By running the virtual network security functions from this partner ecosystem on general purpose x86 servers, we deliver unlimited scale to any network security function, including such killer apps as SSL visibility. For our customers, this

Even the largest security devices suffer from an unacceptable performance degradation when trying to decrypt SSL traffic.

means being able to inspect all their traffic, all the time, without impacting network performance. Since we provide the necessary network, server, load balancing, and management components in a turnkey hyperconverged infrastructure (HCI) package, customers can focus on security policy and no longer have to spend time struggling to predict network traffic needs to scope required hardware. With the virtualization platform, when more capacity is needed, it's just a matter of licensing more virtual machines from the security vendor, and the platform scales accordingly. Because Corsa is offering the virtualization platform on a subscription basis, customers can disassociate themselves from all forms of hardware refresh-cycles for network security.

EA Any near- or long-term predictions about modern network security?

EC Transition to 5G, IoT, and cloud is forcing network and security engineers to look at network security differently. Security in layers is something that will need to be applied at multiple points in the network. The only way to do this in a timely and effective manner will be to automate, so that responses are dynamic and proactive. At network gateways, this means having virtual security services that auto-scale to meet traffic volume changes, traffic mix changes, and changing threats – all at a per-tenant level. We are well on our way to becoming an integral part of that evolution.