SOLUTION BRIEF

Communications Service Providers
Network Security

Clavister* Orchestration Plays Key Role in NFV Firewall Services

With support for open source and its own advanced orchestration capabilities, the Clavister NetShield Virtual* delivers firewall services that can scale from branch office to central office with complete lifecycle management.

Network functions virtualization (NFV) provides a new infrastructure for communications service providers (CommSPs) to deploy agile firewall services for customers. But as customer adoption increases, service orchestration is becoming more important to manage service lifecycle. In its latest virtual firewall product, Intel® Network Builders ecosystem partner Clavister* has combined service scalability with robust orchestration to deliver firewall services that meet the needs of the smallest branch office and the largest central office.

clavister

The Challenge: Scaling NFV Firewall Services

NFV provides a cost-effective service delivery vehicle for companies with small or branch offices because they can install a general-purpose Intel® processor-based server as a universal customer premises equipment (uCPE), connect it to the internet and virtualized network services (such as firewall) can be deployed remotely in minutes.

As these services grow in popularity, the role of network orchestration takes on a much larger importance. Advanced orchestration functionality is required to manage the thousands of servers and services deployed across a CommSP's market. NFV orchestration automates the deployment and provisioning of the virtual network functions (VNFs) and other software elements that make up a network service. Orchestration can facilitate new services from an ordering system or can automate deployment to increase resources or initiate services in response to service level agreements or network traffic levels.

In addition, orchestration assists with the management of the physical and virtual resources needed for the services by requesting additional resources (e.g., CPU cores) to support a growing service or automatically spinning up a new virtual instance of the service if needed. Orchestration provides service chaining of the applications that defines a data path through a series of VNFs so that, for example, data packets are directed through a firewall before being routed. VNFs that consume the fewest physical resources allow more flexibility for other services to share that platform.

The resource footprint of the VNF can impact the flexibility of the orchestrated NFV platform. If the VNF needs more compute, memory, or storage resources than are available, then the orchestrator can't initiate the new service. Lower resource consumption makes a VNF more universally deployable and helps the CommSP further its network agility goals. Low resource VNFs also improve profitability by leaving resources available on the uCPE for other VNFs.

Combining orchestration with virtualized firewall capabilities allows service providers to provide a front line of defense for large branch office networks that enhances the firewall's ability to help protect users. Clavister has done that with its Clavister NetShield Virtual* firewall solution.

How Clavister Orchestrates Security with Clavister NetShield Virtual

Clavister NetShield Virtual is a CommSP-grade virtualized firewall that can operate using either VMware vSphere* or KVM* hypervisors. The scalable software has very low processing overhead that allows the VNF to operate on branch office uCPEs using only a single CPU core with 1 GB of RAM in a basic instantiation. And as needs grow, the software can scale from that single core to up to 20 CPU cores for large central office implementations.

Some key features of the Clavister NetShield Virtual include:

- Stateful firewalling with deep traffic inspection
- Internet Key Exchange version 2 (IKEv2) negotiated IP Security (IPsec) tunnels for improved security
- Resilience via multiple WAN links and high availability
- WAN optimization for prioritization of business-critical applications
- Flexible SDN integration and automation via the Clavister InCenter* centralized enterprise management system (EMS)
- Flexible license model to support security-enabled SD-WAN as-a-service
- Low compute footprint for flexible deployment on wide range of vCPE platforms

Orchestration Is Key to Deploying as a Service

Clavister has integrated the NetShield Virtual with OpenStack* open source cloud operating system to leverage the Heat Orchestration Template (HOT)* for orchestration capabilities. Heat is an orchestration system that describes a range of infrastructure resources such as servers, floating IP addresses, volumes, security groups, users, and more. HOT describes the infrastructure that can be understood and created by a network engineer.

With these orchestration capabilities, CommSP personnel set up an automated process for on demand deployment of a uCPE that installs the firewall software and creates a service chain with other NFV services including vRouters, virtual unified communications (vUC), and others for which the Clavister NetShield Virtual will improve security.

Clavister NetShield Virtual also supports configuration and integration with software defined networking (SDN) controllers and other NFV orchestrators through the use of the centrally managed Clavister InCenter. Clavister has developed an open REST interface for Clavister InCenter that allows it to communicate with other elements in the network for complete end-to-end management.

High-Performance Data Plane Adapts with Customer Policies

An important element of the performance of the firewall is its scalable data plane, which facilitates the data flow through the VNF at high data rates. In building the data plane, Clavister utilized the Data Plane Development Kit (DPDK), an open source set of software libraries and drivers for high-performance packet throughput in an Intel® architecture-based server. DPDK processes data packets in user space, avoiding the OS kernel, which reduces latency. DPDK transparently supports and enables Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and Intel® QuickAssist Technology (Intel® QAT). With a proper DPDK implementation, VNFs are able to benefit from those features without significant development and support investments. The performance of these DPDK-enabled servers helped Clavister to implement a universal data plane that can be adapted to do any work specified by the customer's policies. This eliminates the need for dedicated cores for specific processes such as IPsec processing or packet filtering.

Intel® Processors for Encryption Processing

The Clavister solution is specified for Intel architecture CPUs, specifically Intel® Xeon® and Intel Atom® processor-based systems. Intel Atom systems on chips (SoCs), are designed for uCPE and other light scaled-out workloads that require very low power, high density, and high I/O integration. Intel Xeon processors provide significant performance and power efficiency benefits for scaling out data center and network virtualization applications, which is required for distributed orchestration and high-throughput encryption and firewall processing. Clavister software can run on servers using the widely deployed Intel Xeon Processor E5 CPU generations up to the latest advanced Intel Xeon Scalable processors, which offer the scalability to deliver workload-optimized performance in NFV applications.

Clavister firewalls make extensive use of Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) an Intel encryption instruction set that delivers very fast processing for the widely used AES encryption algorithm. When available in a server, Clavister NetShield will also take advantage of Intel® QuickAssist Technology (Intel® QAT) for accelerated IPsec processing. Intel QAT functionality is built into the Intel Atom C3000 SoCs and is available as an accelerator card or chipset-based solution for Intel Xeon processor-based servers. Intel QAT accelerates encryption of customer data, freeing up valuable CPU processor cycles for other critical needs such as data path processing.

Conclusion

Clavister NetShield Virtual provides advanced security features combined with extensive orchestration capabilities to enable widespread virtualized data security services for CommSPs. Leveraging the processing power of Intel architecture processors, the flexible deployment model of the Clavister NetShield Virtual provides a solution that grows with the business success of the CommSP.

About Clavister

Clavister is a leading European cybersecurity vendor with over 20 years of experience. Headquartered in Sweden, the company works with communication service providers, governments, enterprises and managed security service providers (MSSPs) in more than 150 countries. Clavister provides unique security solutions to protect its customers' digital assets and secure business continuity. More information is at https://www.clavister.com.

About Intel® Network Builders

Intel Network Builders is an ecosystem of infrastructure, software, and technology vendors coming together with communications service providers and end users to accelerate the adoption of solutions based on network functions virtualization (NFV) and software defined networking (SDN) in telecommunications and data center networks. The program offers technical support, matchmaking, and co-marketing opportunities to help facilitate joint collaboration through to the trial and deployment of NFV and SDN solutions. Learn more at http://networkbuilders.intel.com.