Solution Brief

Communications Service Providers
Edge Security

Lanner Partners to Deliver Scalable Firewall for Edge Security

CyberElastic™ firewall designed for helping protect applications and services at network edge; solution combines software from Red Hat, NoviFlow, and Fortinet running on Intel®-powered Lanner HTCA-6600 MEC platform

Edge computing systems are gaining market traction because they deliver new services, reduce backbone network traffic, and offer much lower latency services. Securing these new services is a challenge due to the complexity of integrating the access, core, and cloud network elements required for their deployment. Firewalls are the state-of-the-art first line of defense for edge-based applications, but to be successful in these newer and more dynamic environments requires firewall solutions that are both agile and elastically scalable. Lanner has partnered with key industry players to assemble an all-in-one switch-server solution with the agility and performance required for high-performance edge data protection.

Edge Security Complexity Grows

Edge cloud computing and networking is growing dramatically in response to increased demand for low-latency services, but also as a way for communications service providers (CoSPs) to better manage all the data created by virtualization, cloud computing, and video streaming from mobile devices.

Edge servers use virtualization techniques such as hypervisors for virtual machines and Docker for containers to deliver network and application services to customers. Enabling multiple virtualized services to run on a single server helps to monetize that server by delivering services tailored to each customer. But the evolving mix of virtualized or containerized services, complex service chains, and constant changes in customer demand make providing data security a challenge.

Firewalls provide the first line of data security defense in an edge server as communications service providers (CoSPs) connect their users through the firewalls as part of a multi-tiered security implementation. Firewalls in these implementations must scale as edge services will grow over time. In a virtualized server, additional firewall instances can be deployed automatically or remotely, allowing for cost-effective elastic scaling of network security.

This scalability depends on complex interactions with other network hardware and software resources. Load balancing is one example of an application that needs to scale in sync with the new firewall instances to maintain high data rates and full data security protection.

Such interactions are driving increased complexity for edge security and becoming a limiting factor to protecting data, identity, and network resources. These interactions are also becoming a barrier to network adaptability, latency, and scalability, and they are increasing both operating and capital expenses.

To address edge firewall challenges, Lanner has partnered with Red Hat, NoviFlow, and Fortinet to create CyberElastic™, a firewall solution that runs on Lanner's HTCA-6600 multi-access edge computing (MEC) platform solution. CyberElastic makes use

of Intel® architecture processors for performance and Intel® Tofino™ P4-programmable switch ASICs for high-throughput data networking and innovative load balancing functionality. CyberElastic delivers a pre-integrated, scale-out edge firewall service featuring pay-as-you-grow economics, analytics, easy installation, configuration, and remote monitoring.

Components of the CyberElastic Firewall

The CyberElastic solution utilizes the following technologies.

Lanner HTCA-6600 MEC platform

The HTCA-6600 is a scalable all-in-one, zero-touch configuration, software-defined MEC switch-server platform that leverages Intel's flexible and programmable compute and networking technology.

The HTCA-6600 has a scalable and modular architecture that provides compute and storage along with network switching to deliver robust and more secure edge services with elastic capacity. The platform features up to six dual-CPU blades (HMB 6110), supporting up to 12 Intel® Xeon® Scalable processor CPUs with a total of 336 physical cores.

Figure 1. Lanner HTCA-6600.

Intel Xeon Scalable processors are the next-generation CPU platforms for cloud-optimized edge networks. Industry-standard Intel Xeon Scalable processor platforms support the convergence of key workloads that are essential in MEC deployments, including applications and services, control plane processing, high-performance packet processing, and signal processing that take place on edge networks. This delivers a virtualized, software-defined infrastructure to enable cloud capabilities for agile service delivery throughout the network.

With an open architecture that scales and adapts with ease to handle the demands of emerging applications, the Intel Xeon Scalable processor provides a future-ready foundation for agile networks that can operate with cloud economics, be highly automated and responsive, and support rapid and more secure delivery of new and enhanced services.[1]

Networking

Ethernet switching in the HTCA-6600 is provided by the Intel Tofino programmable switch ASIC on the HLM-1100. Intel Tofino switches support the P4 programming language, an open source programming language for defining packet forwarding flows in a wide range of networking systems. The programmability of Intel Tofino switches allows enterprises, data centers, or CoSPs to customize the data plane to support new protocols, run networking programs on the switch, and deliver detailed in-band network telemetry allowing real-time network visibility.

The CyberElastic firewall design makes use of the switch fabric to offload the load balancing function, providing line-rate load balancing without added workload on the physical cores.

The HTCA-6600 includes a high-speed backplane capable of delivering 400 Gbps of bandwidth to each server blade through the use of dual Intel® Ethernet Controller E810 interfaces. Each NUMA node has a direct connection to the primary and backup Ethernet switches. SR-IOV is used to offload packet delivery to the virtualized Fortinet FortiGate firewalls, further reducing the utilization of physical cores performing network functions.

Additional I/O can be added to the HTCA-6600's networking capabilities by including up to six front-cabled, field-swappable network I/O blades that can support either 10 GbE, 40 GbE or 100 GbE with a capacity of up to 192 10 GbE SFP+ connections.

The top two networking blade slots are reserved for either the switch blades or network interface blades, while the other four slots are solely used for network interface blades. The HTCA-6600 system offers redundancy on key components of the HTCA-6600, including CPU blades, network interface blades, cooling fans, and power supply units. These backup modules allow the platform to deliver uptime that meets carrier-grade high availability expectations. The system is compliant with NEBS and FIPS carrier safety standards and supports multi-tenancy.

Red Hat OpenShift and Linux

The foundation of the CyberElastic software stack is Red Hat® OpenShift®, an enterprise-ready Kubernetes container platform with full-stack automated operations to manage hybrid cloud, multi-cloud, and edge deployments.

Red Hat OpenShift provides a complete solution (see Figure 2) for hybrid cloud, edge, enterprise container, and Kubernetes development and deployments. It includes container runtime, networking, monitoring, container registry, authentication, and authorization solutions. These components are tested together for unified operations on a complete Kubernetes platform spanning every cloud.

Red Hat OpenShift is integrated with Red Hat Enterprise Linux (RHEL) open source operating system. RHEL is designed to scale existing apps—and roll out emerging technologies—across virtual, container, or bare metal server deployments in all types of cloud deployments.

NoviFlow CyberMapper and Visual Analytics

Lanner collaborated with NoviFlow to deliver load balancing and visual analytics capabilities. NoviFlow CyberMapper™ is a proven load balancing application. NoviFlow makes use of the Intel Tofino switch's programmability by running load balancing and other functionality directly within the data plane. This provides dramatically faster response time and frees up CPU compute cycles for other processing.

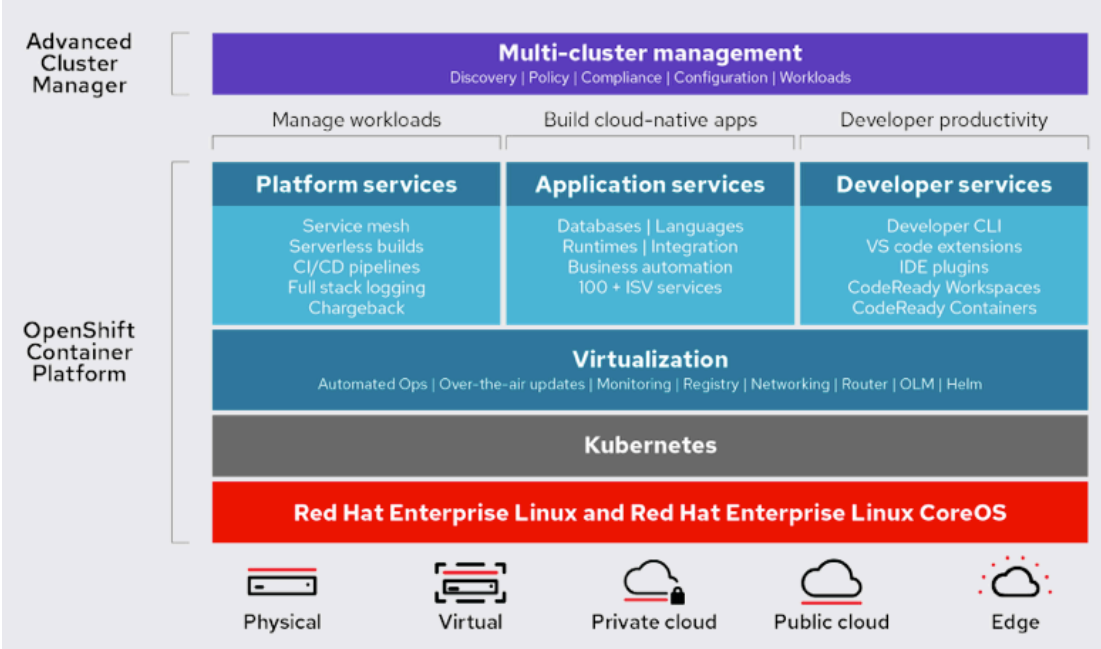

Figure 2. Red Hat OpenShift functionality block diagram.

CyberMapper services include:

- Threat intelligence gateway
- Traffic steering
- Exclusion-list filtering
- Packet broker filtering
- Sticky stateless load balancing
- SRv6 routing
- Service chaining through SRv6

NoviFlow VisualAnalytics™ provides an end-to-end view of the HTCA-6600 platform for hardware and software trouble shooting. It simplifies the operations, administration, and management (OAM) of the HTCA-6600 platform to reduce onsite and preventive maintenance needs and costs.

VisualAnalytics ingests hundreds of data streams and millions of data points and then presents them in graphical trends that allow network managers to visualize the health of their platform. The dashboards are designed to take all of the information and present it using the simple "Green is Go!" concept, taking the complexity and time out of understanding the operational health.

VisualAnalytics leverages a flexible data processing pipeline allowing for programmable datapoints, so that VisualAnalytics can be customized for specific data collection needs. This same data processing pipeline can be configured to output to multiple sources. This allows VisualAnalytics to be integrated with other data collection systems in a network.

Drilling Down On Log Files Visually

VisualAnalytics supports a wide range of data ingestion types, even text-based log files, making it a centralized, and fully searchable, repository for system log files. By visualizing log files, VisualAnalytics makes it easy to find a specific actionable event using easy-to-read time series graphs that highlight the severity of the entry.

Fortinet FortiGate-VM

The FortiGate virtual firewall (FortiGate-VM) is integrated into the CyberElastic system, allowing organizations to more securely migrate any application to a virtual environment and support a variety of use cases, including highly available large-scale virtual private networks (VPNs) in the cloud.

FortiGate-VM has been designed to deliver high performance in virtualized environments using the company's advanced virtual security processing units (vSPUs) architecture. The Fortinet vSPU architecture utilizes the open source Data Plane Development Kit (DPDK) for accelerated packet processing. Several Intel technologies play an important role in the vSPU architecture, including single root I/O virtualization (SR-IOV), PCI pass-through, and Intel® QuickAssist Technology (Intel® QAT).

The FortiGate-VM consolidates NGFW and secure gateway services to help protect users from internet threats, and enables enterprises to enforce policy compliance for their applications. FortiGate-VM uses multiple detection techniques, like web filtering, DNS filtering, data loss prevention, antivirus, intrusion prevention, and advanced threat protection to shield users from network threats.

CyberElastic Firewall Solution

The CyberElastic firewall solution combines the components described above (see Figure 3) into a pre-integrated firewall service that can be turned on by the CoSP to help protect virtualized applications running on the HTCA-6600. The CyberElastic service features scalability, pay-as-you-grow economics, terabit per second throughput, sophisticated analytics, and easy installation, configuration, and remote monitoring.

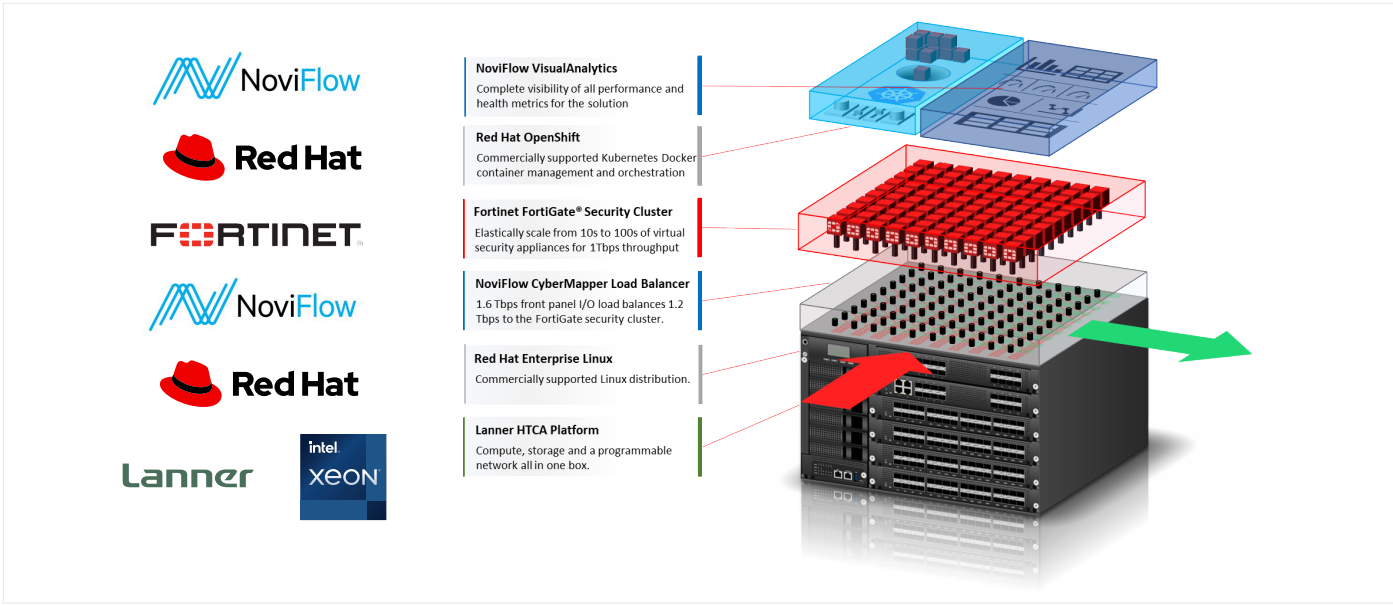

Figure 3. CyberElastic software stack running on the Lanner HTCA-6600.

CyberElastic can be installed into a legacy network by placing the HTCA-6600 at the network ingress. This creates a security domain inside which firewall services are invisible and are independent of the rest of the network. This implementation is designed for network edges and peering points that need scalable and dynamically load balanced firewall services.

CyberElastic also supports segment routing over an IPv6 data plane (SRv6), which makes firewall resources addressable from anywhere in the network. With SRv6, CyberElastic firewall services can be part of a global network service chain, reducing the need to overprovision firewalls to meet peak local demand. The NoviFlow VisualAnalytics built into CyberElastic allows CoSPs' network managers to see trends in firewall usage evolve over time, enabling capacity planning based on utilization. It also allows CoSPs to utilize network orchestration to divert traffic to underutilized firewalls.

Summary

Edge network-based virtualized applications and services need data security solutions with the agility to stay ahead of the complexity and service growth that is normal in dynamic networks. Lanner and its partners have developed the CyberElastic firewall, a novel system that utilizes a software stack from Red Hat, NoviFlow, and Fortinet running on Lanner's HTCA-6600 MEC server. With performance from Intel architecture CPUs and P4-programmable switching from the Intel Tofino switches, the CyberElastic system supports fast data throughput and scalable firewalls and load balancing—the combination of performance and remote scalability needed for today's edge-based services.

Where to Get More Information

Lanner HTCA-6600 MEC platform details

NoviFlow overview

Fortinet overview

Intel® Xeon® Scalable processors

Intel® Tofino™ switches

Intel® Network Builders program

P4-programmable switches

intel

Notices & Disclaimers

[1] https://www.intel.com/content/www/us/en/products/docs/processors/xeon/2nd-gen-xeon-scalable-processors-brief.html

Intel technologies may require enabled hardware, software or service activation.
No product or component can be absolutely secure.
Your costs and results may vary.
Intel does not control or audit third-party data. You should consult other sources to evaluate accuracy.

0221/DO/H09/PDF ♻ Please Recycle 346066-001US