White Paper

Building Next-Generation Network Security with Wind River® DPI Solutions on Lanner FW-8895

Lanner

intel Embedded Alliance

Table of Contents

Abstract

A new era of pervasive computing has accelerated demands for a system that can guard the Internet from rampant malware and other forms of sophisticated attacks. Lanner Electronics and Wind River®, two pioneers in hardware system architecture and embedded operating systems respectively, have brought their distinct expertise together to create the industry's first performance-driven intelligent system for next generation network security. The system offers a full Deep Packet Inspection (DPI) solution with integrated accelerator and advanced functions for Internet security in an application-ready platform. With stringent performance and hardware requirements analysis, this new breed of intelligent server system is rapidly becoming the central focus of the Universal Threat Management (UTM) industry.

Introduction

From enterprise security to network management to monitoring service level agreements between ISPs and customers, there is a growing need for a better Internet security that is capable of enhanced connectivity, context awareness, and increased adaptability to tomorrow's network infrastructure. The proliferation of Internet threats and malicious attacks also reinforces the call for next generation firewalls that go beyond the conventional approach. What is needed now is a new class of total solution with the required intelligence and agility to support exponentially increasing amounts of data transported through the cloud and processed at line rate as they travel from one appliance to another. In response to this pressing need, Wind River® and Lanner are working together to give telecommunications equipment providers, network operators, and solution providers the ability to develop ultra-fast, highly scalable intelligent network products and services. Following this vision, Lanner Electronics is presenting an application-ready platform, the FW-8895, which incorporates a feature-rich and complete development environment for next-generation firewalls to accelerate, analyze, and secure network traffic. It provides a foundation for major DPI functions encompassing content-aware flow classification, application acceleration and content inspection on an IA multi-core platform. This platform can also accelerate complementary workloads, such as encryption and packet processing, using the Intel® QuickAssist technology and the Intel® Data Plane Development Kit (DPDK). Not only are these new technologies offered on Lanner FW-8895, but service scalability, carrier-class resiliency, and industry-leading network capability are concretely demonstrated in one particular system.

Integrating Wind River® Embedded Development Kit with Lanner's FW-8895

The Wind River® embedded development kit includes a bootable USB flash drive that immediately turns any host computer into a fully integrated development environment (IDE) with absolutely no installation required.

The Wind River® Embedded Development environment is based on the Eclipse framework 3.5 and contains a Wind River® GNU compiler, debuggers as well as configuration tools for the Linux user and kernel space. Run-time analysis tools such as the system viewer, memory analyzer, and the data monitor are essential complements to this kit.

The core of the SDK consists the following 3 engines:

1. Wind River® Application Acceleration Engine, a network stack for accelerating layer 3 packet throughput and layer 4 network protocols with Intel DPDK
2. Wind River® Content Inspection Engine for high-speed software pattern matching of large groups of regular expressions against blocks or streams of data
3. Wind River® Flow Analysis Engine, a set of software libraries and tools that enable deep visibility into layer 4–7 traffic flows, including real-time packet classification and protocol and application identification

Telecom equipment and solution vendors have employed DPI in their network solutions to peer deep into the contents of a data packet, the packet payloads. However, with ever-increasing connection speeds and the boom in cloud-based computing and data exchange, solutions able to provide deeper data stream visibility in real-time will drive a reform that goes beyond traditional DPI. The highly intelligent network inspection built on these engines can be used to identify protocols and extract the metadata for finding alert event correlation and behavioral context, thus further detecting abnormal behavior and preventing harmful intrusions, i.e., Network-Based Anomaly Detection (NBAD). Optimized for Wind River® Linux 4, the Lanner FW-8895 coupled with the Wind River® embedded development kit offers a pre-installed and pre-optimized Internet operating system bundled with virtual routing, forwarding and virtualization. The software and the IA architecture also take advantage of the Intel® Data Plane Development Kit (DPDK) to better accelerate packet forwarding. It also includes other built-in Intel IA platform features such as Intel Virtualization and Intel QuickAssist.

The Advantages of FW-8895 Empowered by Intel IA Technology

The Lanner FW-8895 is a hardware and software consolidated platform targeted for tomorrow's network intelligence. By utilizing Intel's IA multi-core technology and Lanner's modularized hardware design, scalability in network capacity and performance can be achieved without modification of overall system architecture. Additionally, this system demonstrates robust manageability and the highest levels of network availability. We will discuss how this can be accomplished by listing the advantages and other built-in accelerations incorporated into the Lanner FW-8895.

Workload consolidation for next-generation communications platforms

The Lanner FW-8895 helps service providers and system integrators transform their networks toward intelligent, software-defined networks to support the explosive growth in network traffic while also lowering costs and increasing revenues. It does this by leveraging Intel's control plane and data plane workload consolidation in one system. However, in order to process packets at the required rates without adversely affecting control plane processing like many of the DPI functions on a consolidated platform, functionalities must be offloaded from the main application processors.

The underlying Intel® DPDK driver is able to accelerate applications transparently by speeding up packet processing. The Intel® DPDK, aiming for improving data plane performance on general-purpose platforms, provides Intel architecture-optimized libraries that allow developers to focus on their application. Another key element of this workload consolidation strategy from Intel is Intel® QuickAssist. The Intel® QuickAssist technology is a set of software and hardware modules that accelerate bulk encryption, data compression and other workloads. Together, they deliver unprecedented packet processing performance on FW-8895.

Upgradeability and scalability made possible under the same architecture

The Lanner FW-8895 satisfies vendors who are looking for agile platforms that will provide scalable performance with relative ease to match the desired equipment performance and cost. We designed and manufactured standards-based, general purpose platforms ranging from low power to high-end server systems based on Lanner Electronics' trusted supply line of scalable Intel based products and services. We also design these systems based on modularized concepts to give vendors off-the-shelf customization opportunities. One of the most-recognized and highly accredited is our hot-swappable Ethernet modules. Our Ethernet modules are available with various port numbers and different signaling and speed.

High port density with uninterrupted network connection on Lanner Ethernet modules

Lanner's FW-8895 system can accommodate 8 swappable modules in the front of the system, providing a maximum total of 64 network ports. These Lanner PCIe hot-swappable LAN modules offer both copper and fiber optic cabling for Gigabit ,10 Gigabit Ethernet and 40 Gigabit Ethernet connectivity with Intel controllers on our network server platforms. Furthermore, an integrated I/O performance improving technology called the Intel® Data Direct IO is seamlessly integrated in the Intel Xeon processor E5 family without requiring user programming. The Intel® Data Direct I/O allows Intel Ethernet controllers to talk directly to the CPU cache. Hence, it offers direct benefits to higher bandwidth, lower power utilization, and reduced latency between the interface card and memory.

In addition to the advanced I/O technology, Lanner bypass technology improves on the availability of our network platforms by assuring uninterrupted network connections. Lanner's Third Generation Bypass can be enabled automatically when system failure occurs. Furthermore, the software-based approach of bypass technology makes it a comprehensive utility to be implemented on any Lanner devices regardless of the underlying chipsets on the system. And because of the employment of a microcontroller, precise bypass control can be achieved no matter whether the system is on, off, or in the process of restarting; the net result is to maximize network uptime.

Linear scaling in performance based on the varying number of threads as well as processor choice

By integrating Wind River's IDE into FW-8895 system, we are able to provide a system with a software-enabled DPI solution capable of being developed into next-generation firewalls on the fly. The benchmarking performance of the Content Inspection Engine using a common set of signatures and real-world data stream on the Intel Xeon Processor E5-2600 shows near linear scalability up to 8 threads and tops out at 160 Gbps with 32 threads.* When running the same scenario by varying the processors of Intel E5 family, the throughput also reveals a linear progression. Furthermore, Lanner FW-8895 system offers 8 swappable modules on the front panel. Each module can be used alone or in concert with the desired combination of hard disks and Ethernet LAN ports. With this linear scaling in performance and modularized hardware capacity, the FW-8895 gives system integrators and application vendors options to customize the system based on their needs.

Manageability with IPMI and high availability with power supply redundancy and hot swappable fans

Focused on carrier requirements for lower cost and higher profits as well as high availability for assured services, the Lanner FW-8895 system has incorporated a set of robust features to create a service-optimized network by creating a more intelligent, secure, and reliable infrastructure to the cloud and between clouds. For example, the IPMI function on the management port is for out-of-band management which will proactively monitor the system without requiring a running operating system. Other features such as redundant power supply, and hot-swappable fans and hard disks are also equipped to support 24/7 services. Both the redundant power supply and modular fans can be accessed and replaced easily from the back panel.

Applications

Developed in collaboration with Wind River on Intel's IA platform, this next-generation intelligent system provides "plug and play" capability through a combination of hardware, middleware, and cloud services, enabling designers to develop and test their application's connectivity and performance, then quickly deploy. Some of the applications that have proven time-to-market and other practical uses of Lanner FW-8895 system will be listed below:

QoS function on WAN and Application Optimization
The ultimate goal of WAN optimization is improving the network efficiency in a bandwidth-constrained WAN with heterogeneous network traffic.
In a typical network, the traffic through the network consists of flows from multiple applications and utilities. Different types of traffic have their own requirements and characteristics with respect to delay, jitter, etc.

In order to apply different treatment for different data flows, QoS will need to classify the traffic first to help identify different applications and protocols that exist in a network. DPI is one of the methods for traffic identification purposes and it may also use statistical method to do more advanced analysis on network traffic. Currently there are many QoS mechanisms that can be used to manage WAN bandwidth, including Congestion Management, Congestion Avoidance, Traffic Policing or Shaping, and Link Efficiency.

Tiered services, price and policy definition, and enforcement in cloud services
The Internet is evolving because new business models, usage patterns, and technologies are introduced frequently. One such example is that of Cloud Computing. To define the levels of service being sold to ensure quality of experience for the end user, Service Level Agreements (SLAs) must be enacted and carried out between the customers and service providers.

Deep Packet Inspection (and filtering) enables advanced user services and maintains the quality of service standard defined in the SLA. With DPI, resources and data on the Internet can be treated differently according to parameters such as user, content, site, platform, or application to achieve network-based traffic optimization. It empowers the service provider to make their platforms unique and personalized to both the industry and individual users. For instance, tiered services with levels of service priority and bandwidth can be offered using DPI. Service differentiation is especially important in developing business models and engaging businesses with customers for the three major types of cloud services, namely, Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS).

For charging and billing in cloud services, tiered service or differentiated service structures allow cloud service providers to charge users on a per-use, per-application basis, allowing customers to receive products best suited to their needs. For example, metered pricing can be imposed based on bandwidth consumption and disk usage.

While the service providers are obligated by the SLA to provide a certain level of service, they also need to enforce policy definitions that cover illegal materials and unfair use of bandwidth by leveraging DPI techniques. Besides the use for finer service granularity and policy enforcement, the DPI-capable system can also improve the effectiveness of user authorization and electronic billing and tracking to aid in more effective service delivery.

Cyber security and Internet management
Enterprise and small and medium businesses have adopted security methods including firewalls to protect against threats and unwanted intrusion. For instance, the technique of port forwarding to hide web application servers, and access lists to block malicious websites are common functionalities of firewalls.

As intrusion detection, intrusion prevention and anti-virus strategies advance, many of the security shortcomings of the open and unprotected Internet as well as service interruptions can be recognized and counteracted by Unified Threat Management. These solution packages have been implemented to replace the traditional firewall to become an all-inclusive security platform that is able to perform multiple security and management functions within one single appliance. Some appliances also incorporate data loss prevention (DLP) into their gateway. Data loss prevention identifies and places controls over sensitive data in motion to safeguard valuable information. Some common techniques used for DLP include pattern matching, data archiving, and document file fingerprinting.

The Lanner FW-8895 is an open architecture platform suited for implementing a complete set of security strategies and Internet applications – such as those included in UTM, user authentication, revenue assurance and network efficiency.

Conclusion

As network infrastructures evolve in tandem with the continuing rise of cloud computing, the delineation of WAN and LAN technologies becomes blurry; consequently, broader and deeper information security breaches are an increasing threat. Adding more security to networks is an immediate priority.

The Lanner FW-8895 together with the plug-and-play Wind River DPI kit can foster multi-layered protection by implementing a total solution in the cloud, at the internet gateway and across network servers. By thoroughly incorporating the requirements to build a secure communication platform at the outset of the product design, factors such as network capacity, low latency and manageability, and reliability have been satisfied to ease service creation and deployment effort. Furthermore, with a single platform that readily scales network throughput and capacity, the Lanner FW-8895 aims to aid in monetizing your network by delivering the best performing solutions efficiently and being adaptable to different market segments.

About the Lanner FW-8895:
Lanner Electronics has a long pedigree of designing and manufacturing network platforms for IDS/IPS and all-inclusive security solution, unified threat management (UTM). The FW-8895 is one of Lanner's representative high-end server platforms, which offers advantages in throughput and advanced processor based on Intel® Xeon processor E5-2600. The system supports 2 CPU configurations, each of which contains up to 8 cores. The system also supports DDR3 memory that features quad-channel memory in 16 DIMMs. For scalability and expansion opportunity, a total of 8 module slots in the front panel can be fitted with either swappable 3.5" HDD or field-serviceable Ethernet modules. In addition, the system also equips with redundant power supply (600W each) and 4 swappable modular fans.

Visit the Lanner website for more information on FW-8895:
http://www.lannerinc.com/products/x86-network-appliances/rackmount/fw-8895

* Based on data from the performance test, "Wind River Content Inspection Engine Performance on Intel® Xeon Processor E5-2600 Series" in the white paper "Accelerated Deep Packet Inspection for Network Security Applications" published by Wind River®.