ADLINK
Leading EDGE COMPUTING

Technical Article

DPI and Cloud Computing Security Platforms for the IoT Era

Network Appliances



www.adlinktech.com

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Introduction



ADLINK Technology, as a leading provider of industrial computing platforms, has been focused on the cloud computing needs of industrial equipment for many years. ADLINK's Cyber Security Appliance (CSA) platforms can help customers to quickly build the next generation of DPI or cloud computing security solutions by integrating the necessary hardware and software to address the new security requirements of the IOT era.

Contents

Introduction P1
Requirements of Unified DPI Equipment for Telecom P2
Requirements of Cloud Computing Security Equipment P4
Network Security Platforms from ADLINK Technology P6
Conclusion P9

We are entering an era in which "all things are connected to the Internet", with Internet of Things (IoT) devices expected to experience explosive growth in the next few years, with corresponding network traffic generated by IoT devices also growing rapidly. Network traffic will become more and more complicated as this trend continues since the range the applications used by IoT devices will be much more diverse than those of today's mobile applications. Therefore, the struggle between attack and protection will become even more intense in the IoT era. At the same time, the use of cloud computing is becoming more widespread. The key characteristic of cloud computing being resource allocation on demand allows computing resources to be used more efficiently with reduced resource waste, resulting in its increasing popularity among corporate customers. The intrinsic multi-tenant environment of cloud computing, as well as the constant creation, migration and destruction of virtual machines during the process of the execution of resource allocation on demand, will lead to the disappearance of physical security boundaries. Ensuring cloud computing security in the IoT era will be a huge challenge.

Traditional security devices are built based on a physical boundary and have very limited dynamic adaptability, making them inadequate when applied to a cloud computing environment. With regard to constructing network security equipment that meets cloud computing requirements, the industry has reached some consensus. For example, deep packet inspection (DPI) technology can be employed to visualize flow information such as user, application, and location of network traffic, allowing for fine control over the flow of traffic on the network. Software-defined networking (SDN) technology can be employed to implement programmable network traffic, providing traffic redirection and automatic security policy configuration. Network function virtualization (NFV) technology can be employed to implement security resource pools, providing collaborative deployment between computing and security resources. In order to deal with network security threats in the IoT era, the next generation of network security equipment needs be built using all of these technologies.

This article will first investigate the network security devices used in unified DPI for telecom and cloud computing security, and review the new requirements proposed for network security devices. Then we introduce ADLINK's Cyber Security Appliance (CSA) platforms and explain how they can help customers to quickly build the next generation of DPI or cloud computing security solutions by integrating the necessary hardware and software to address the new security requirements of the IOT era.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Requirements of Unified DPI Equipment for Telecom

Due to massive growth in mobile Internet usage, revenue from data services is comprising an increasing share of the total revenue of telecom operators, who are attaching greater importance to the operation of data related services. DPI as a network traffic visualization technology has become a fundamental element of telecom operations. After network traffic visualization is achieved based on DPI, the telecom operator can optimize their business for specific services, develop value-added services based on user identity, and perform security protection in a much more efficient manner. Before the unified DPI concept was proposed, the deployment of DPI equipment was driven by a concrete DPI application. DPI equipment was tightly coupled with the corresponding DPI application. As the number of DPI applications increases, more and more DPI equipment is required to be deployed in the network.

The unified DPI concept was proposed in order to reduce the waste in investment arising from repeated DPI equipment deployment by implementing DPI equipment sharing through standardization of the visualization of network traffic. By coordinating DPI equipment deployment from a network-wide perspective, the DPI requirements are unified at key network locations and DPI services are shared among multiple DPI applications through a suite of unified northbound API, thus avoiding the repeated deployment of DPI equipment. As shown in Figure 1, through sharing DPI equipment at key points of the telecom network, unified DPI reduces duplication of equipment deployment, allows DPI equipment and DPI applications to evolve independently of each other, and greatly enhances the ability to innovate DPI applications. In the following subsections, the construction requirements of unified DPI equipment will be analyzed from different perspectives.

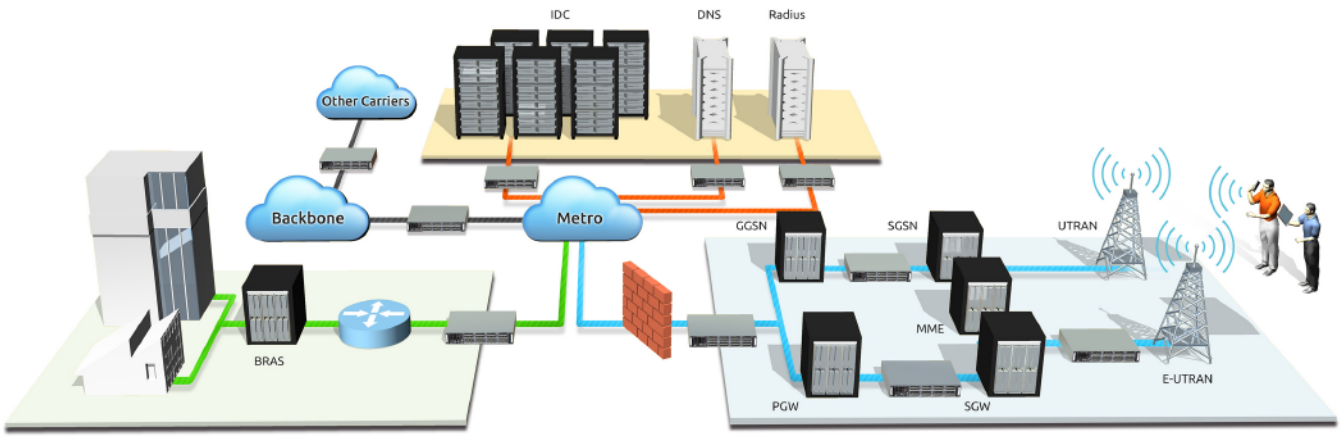


Figure 1. Key deployment points of unified DPI equipment

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Computing Performance

Currently, the 4G network provides sufficient bandwidth for the thousands of constantly changing mobile applications, as well as the numerous social media applications that are integrating more and more functions. However, with more and more IoT devices connecting to the telecom network, the types of network traffic will become even more diverse. The creative value of DPI equipment depends mostly on how many traffic types it can identify, which is the foundation of all upper layer DPI application innovations. The analytics capabilities of DPI equipment depends on the DPI software design, and to a greater extent depends on the computing performance of the DPI hardware platform. Only powerful computing performance can ensure that DPI equipment can identify more types of traffic in real-time.

Rich and Flexible Network IO

To avoid coupling between upper layer DPI applications and lower layer DPI equipment, to allow a range of deployment locations, and to be compatible with different DPI application hardware, unified DPI specifies the requirements for hardware interface support. Depending on the deployment location in the telecom network, DPI equipment needs support ingress/egress network traffic with 1G/10G WAN/LAN, 2.5G/10G POS networks or 100GbE. For DPI equipment that needs be concatenated in the network, the required network interfaces must be implemented natively on the DPI equipment, with implementation by using external splitters, switches, or protocol convertors being disallowed in order to prevent the added devices from introducing extra failure risk. Therefore, in addition to providing sufficient ingress/egress ports and processing bandwidth, unified DPI equipment must also provide flexible network IO configuration, i.e. the appropriate interface modules can be selected to adapt to different deployment locations.

SDN Support

Unified DPI equipment must not only provide common protocol identification and statistical functions, but also strong flow control logic in order to support various upper layer DPI applications. In order to support fine-grained traffic control required by upper layer applications, the DPI equipment must support flow control based on the identified network traffic, including minimum bandwidth guarantee, maximum bandwidth limit, flow pass-through, and flow discarding. In order to develop network security applications on DPI equipment, it must support white-list and black-list settings based on flow metadata such as source address, destination address, protocol number, source port, destination port, domain name, user ID. If these functional requirements are implemented with traditional methods, not only is the functional implementation not transparent, but the available upgrade space is also very limited. SDN technology can be used to classify traffic flow based on multi-dimensional metadata, and then set different flow control strategies. When the DPI service logic is constructed based on SDN architecture, not only can the DPI analysis, statistics, control, multiplex, and security functions be centralized, but for a wide range of possible DPI application innovations based on SDN become available.

High Availability and LAN Bypass

Unified DPI equipment will become more and more important as telecom network element. As with other parts of the telecom infrastructure, unified DPI equipment must provide 99.999% high availability.

The main service components of DPI equipment, such as the computing and switching units, must provide an appropriate hot-standby solution. The other system components, such as power supply unit and fan tray must provide appropriate redundancy and support online replacement when they experience a failure. In addition, for DPI equipment that needs to be concatenated in the communication link, they must provide a LAN bypass function. When DPI equipment suffers from a power loss or a self-test failure, it can switch the communication link from the main unit to the bypass unit automatically, ensuring continuity of service.

Modular and Scalable Design

Data communications begins at the user and then transmitted sequentially over the access network, metro network, and provincial network and backbone network. Therefore, an overview of network traffic conditions can be determined if DPI equipment is deployed at key points that the data traffic passes through. According to the unified DPI specification from China Mobile, these key deployment points can be summarized as: PS side, IDC export, provincial network export, and inter-provincial network export, and inter-backbone network export. The required external network interfaces are different at these key points, and the network traffic size is also different, so a single device will be unable to meet the different requirements at all deployment points. However, in order to reduce the total cost of ownership, and reserve upgrade capacity for future use, most DPI service providers would prefer a single scalable platform that can deal with most deployment scenarios. The methodology of solving this dilemma is to adopt modular design, and support linear expansion for the computing units.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Requirements of Cloud Computing Security Equipment



The wired Internet has developed into the mobile Internet, and is now entering the IoT era in which "all things are connected to Internet". As more and more devices are being connected to the cloud, and network security has become increasingly important. Traditional network security uses firewalls, unified threat management (UTM), intrusion prevention systems (IPS) or other network security products to block attacks at the network entrance boundary. In other words, traditional network security protection systems are constructed at the network boundary. This network boundary is formed when networks that have different security levels are connected together. For example, the private network of an enterprise has a higher security level requirement than the public Internet. Therefore, the connection point between private network and public Internet forms
the natural security boundary. In order to prevent an intrusion from outside the enterprise network, it is sufficient to establish reliable security protection measures at the network security boundary.

With the advent of the cloud computing, enterprises and organizations are now moving more of their business operations to the public cloud. As a result, the network boundary between private and public networks is becoming blurred. Network security equipment that is deployed based on traditional concept of the network security boundary will lose the effectiveness, or even have no functionality. Cloud computing needs a new generation of network security equipment that has new characteristics as described in the following sub-sections.

Computing Performance

In network security, DPI has played an increasingly important role, and it is becoming the cornerstone of cloud computing security in the IoT era. Since the advent of the mobile Internet, more and more end-user applications are using HTTP/HTTPS protocols to exchange data. If traditional matching techniques based on TCP/IP 5-tuples are used, most of traffic flows belonging to other applications will be misidentified as normal Web surfing. Whether for business optimization, content review, or security defense, it is necessary to know the identity of the traffic flow using DPI analysis first, and then perform the appropriate control strategy based on protection needs. Because the working mode of DPI analytics engines is generally concatenated, the average computational workload will increase linearly as the number of application types to be identified is increased. Therefore, in order to guarantee a smooth implementation of DPI analytics, DPI equipment must be equipped with adequate computing power based on the application types to be identified and the traffic size to be handled.

NFV Support

A fundamental requirement of cloud computing is "resource allocation on demand", which requires that computing, storage, and network resources can be taken from resource pools at will based on the specified requirements of business needs. Resource virtualization is the fundamental technology for achieving this goal. In cloud computing, there are a large number of virtual machines that are continually created, migrated and destroyed. The target of cloud computing security is to protect business services in the cloud. As the business requirements change, the resources they require for computing, storage and networks will vary. Therefore, network security resources that serve the cloud must also be dynamic. Network security equipment for cloud computing must also support virtualization like other cloud computing resources. NFV technology can be used to shape network security equipment into a resource pool, enabling dynamic security allocation based on business changes. In order to better support NFV, network security equipment must abandon proprietary computing technology and be built based on open computing technology, allowing it to support virtualization more easily in order to achieve "security on demand".

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

SDN Support

Traditional network security equipment is deployed at the physical security boundary, monitoring traffic flow that enters and leaves the security zone and then performing the required network security tasks. Due to the multi-tenant environment of cloud computing and the frequent virtual machine migrations that take place, a security zone with a physical boundary does not exist in cloud computing. Even the logical boundaries of the security zone will experience constant changes as virtual machines migrate, resulting in a significant challenge for cloud computing security.

As a virtual machine migration occurs, the network security policies that are configured for that virtual machine must also be adjusted. If the migration does not go beyond the protective scope of the current network security appliance, then the security policies related to that virtual machine can be adjusted accordingly. However, if the virtual machine migration extends beyond the scope of the current network security appliance, then the security policies related to that virtual machine must be migrated to the new network security appliance accordingly. The configurations of traditional network security appliances are often static, localized, and need human intervention, making it difficult to implement dynamic, globalized and automated re-configuration on traditional network security platforms. The industry has been trying to introduce SDN technology in order to overcome the challenges brought by a blurred security boundary in a virtualized network environment. SDN can direct targeted network traffic flow to a virtualized network security appliance through flow diverting and aggregating. And when a virtual
machine migrates, SDN, with its global perspective and flexible programmability, can help to achieve the automated migration of relevant network security policies.

Hardware Acceleration

In order to solve the security isolation issues of a multi-tenant virtualization environment, tunneling technologies such as VXLAN (Virtual eXtensible Local Area Network) can be used extensively. VXLAN is an encapsulation technology that repackages layer 2 packets in a layer 3 protocol and can help solve the limitations of MAC table size and VLAN ID space found in top-of-rack (TOR) switches. Because network security appliances are often concatenated in the communication link, they must support VXLAN in order to handle the network traffic flowing through them. The removal and addition of VXLAN headers consumes significant CPU resources and significantly lowers the overall performance of network security equipment. The appropriate method to handle this issue is to use an extra hardware acceleration unit to assist in VXLAN processing.

Encryption technology is being used more extensively in cloud computing in order to enhance security. As with VXLAN, processing encrypted network traffic will also consume significant CPU resources and can be better managed with an additional hardware unit to assist in the encryption and decryption process. When the CPU is relieved of these resource intensive tasks, it can better focus on the key task of DPI more effectively and efficiently.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Network Security Platforms from ADLINK Technology

Whether for unified DPI for telecom or cloud computing security, the computing performance requirements of DPI equipment are increasing. At the same time, SDN is expected to be supported on DPI equipment to enhance its functionality and adaptability. In addition, there is a trend towards standardization of network security equipment. In order to make better use of NFV, SDN and big data technologies from open platforms, network security equipment is shifting from traditional proprietary computing platforms to open computing platforms based on COTS products. The CSA (Cyber Security Appliance) series of products from ADLINK technology is designed and built to meet these trends and needs. By integrating the special requirements of next generation network security appliances on open computing platforms, ADLINK's CSA products can assist network security providers in constructing services that meet the DPI and cloud computing security requirements in the IoT era.

Table 1 lists the requirements of next generation of DPI and cloud computing security products in the left column and the corresponding features implemented on CSA products in the right column. ADLINK implements a high-density design in its CSA products to provide the high capacity and high bandwidth required by next generation network security products, as well as introducing the latest computing and communication technologies from the open computing domain. These designs ensure that CSA products have a rich set of new features, allowing the user to easily meet the network security challenges of the IoT era.

Table 1. Network security equipment requirements and the corresponding implementations on CSA products

Network Security Equipment Requirements	Implementations on CSA Products
Provide high-performance and high- capacity DPI analytics to achieve the visualization of network traffic	Top-range CSA products adopt a high-density design that helps to achieve twice the computing density of a common rackmount server. The latest Intel® DPDK, Open vSwitch (OVS), and nDPI software are integrated on CSA products with ADLINK PacketManager, which optimizes the run-time environment and helps achieve data throughput up to 10 times that of a standard Linux environment.
Provide rich and flexible network IOs to adapt to different application scenarios	Mid-range CSA products adopt a modular IO design, allowing users to select different IO cards to assemble the required ports and bandwidth. Top-range CSA products provide dual 64G inter- connections between all CPU nodes via a built-in high-capacity switch node, which also supports 64 uplink 10G ports, and can support other types of uplink ports by customizing the IO mezzanine card.
Support NFV to achieve "security resource allocation on demand"	CSA products implement the latest virtualization technologies from Intel, including VT-x. VT-d. VT-c and PCIe SR-IOV, to ensure excellent virtualization performance. Furthermore, Intel® ONP and Wind River Titanium Server are also integrated and validated on CSA products to provide a turn-key NFV platform.
Support SDN to provide the foundation for global flow scheduling	The compute nodes of CSA products support DPDK accelerated OVS, which supports OpenFlow protocol. Switch nodes use a switch chip that can support flow processing directly, which provides greater flexibility to enable various SDN agents.
Provide VXLAN and crypto hardware offloading to release CPU resources	The network IOs and switch nodes of CSA products have built-in hardware acceleration units for VXLAN, TCP Segment Offload (TSO), IP Checksum offloading, etc. Encryption and decryption requirements can also be achieved by expansion with Intel® QAT and FPGA modules on the reserved PCIe port.
Modular design, support for linear scalability and carrier-grade high availability	CSA products are available in a range of form factors (1U, 2U and 4U) and achieve modularization and scalability through the OCCERA architecture to adapt different deployment needs. ADLINK CSA products also provide an evolution path to OCP and support linear scalability in data center deployments. Moreover, CSA products can meet the high availability requirements of telecom application through redundant, hot-swappable designs.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Network Security Platforms from ADLINK Technology

CSA-5100/5200
1U/2U Rackmount Network Security Platforms



Ideal network security platform for SMEs

The CSA-5100/5200 is designed for low and mid-level security application scenarios, providing an ideal network security platform for small and medium enterprises (SME). Through four IO expansion slots, up to 32 10G SFP+ ports can be provided on this platform. The main features of the CSA-5100/5200 are summarized as follows:

- Supports Intel® Xeon® processor E3 v3 family, four DDR3 memory slots for up to 32GB memory
- Four expansion slots support flexible network IO configurations, adaptable to a variety of network access scenarios
- CPU board and IO expansion modules support LAN bypass, supporting both automatic and manual triggering modes
- CSA-5100 provides one mSATA and one 2.5" hard drive slot; CSA-5200 provides four 2.5" or 3.5" hard drive slots, meeting various storage requirements
- CSA-5200 provides a PCIe x4 Gen2 expansion slot, allowing for addition of hardware acceleration units such as Intel® QAT and FPGA cards

CSA-7200
2U Network Security Platform based on OCCERA Architecture



Multi-purpose network security platform with rich IO interfaces

The ADLINK CSA-7200 is designed to be a next generation network security appliance, featuring high- performance dual Intel® Xeon® processor E5 v3 and up to 64x 10G SFP+ ports through eight Network Interface Modules (NIMs). The main features of the CSA-7200 are summarized as follows:

- Eight NIM slots support flexible IO interfaces, adaptable to a variety of complex connectivity scenarios
- Advanced LAN bypass features; bypass modes of each NIM can be set independently through BIOS menu
- 12x DDR4 memory slots for up to 192GB memory to meet the high memory requirements of network packet processing
- 3x 2.5" hot-swappable SATA drive bays, supports additional storage expansion via PCIe or M.2
- One PCIe x8 Gen3 expansion slot, allowing for addition of hardware acceleration units such as Intel® QAT and FPGA cards
- Intelligent system management compatible with IPMI specification v2.0, supports SOL and adaptive fan speeds

CSA-7400
4U High-performance Network Security Platform based on OCCERA Architecture



High-performance network security platform providing high-density computing

The ADLINK CSA-7400 is a high-performance high-density computing platform supporting four dual-processor Intel® Xeon® processor E5 v3 computes nodes interconnected by dual redundant switch modules. The CSA-7400 ensures uninterrupted service delivery through hot-swappable compute nodes and switch modules. It is ideally suited for building next generation high-performance firewalls and virtualized telecom elements. The main features of the CSA-7400 are summarized as follows:

- Based on Open Compute Carrier-grade Edge Reference Architecture (OCCERA)
- Intel® Xeon® Processor E5-2600 v3/v4 Family platform
- 4U high-density platform with four dual Intel® Xeon® Processor E5 v3/v4 systems
- Dual switch modules provide 2x 50G internal Ethernet links to each compute node
- 2x 400Gb/s Ethernet bandwidth, 2x 200Gb/s PCIe bandwidth, total 1.2Tb/s bandwidth
- Flexible IO combinations via choice of switch sleds (MXN-3610, MXN-4100) and Network
- Interface Modules (NIM-1610, NIM-0440)
- Advanced chassis management
- Redundant AC/DC PSUs (N+1)

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Application Ready Intelligent Platform (ARiP) for Network Security

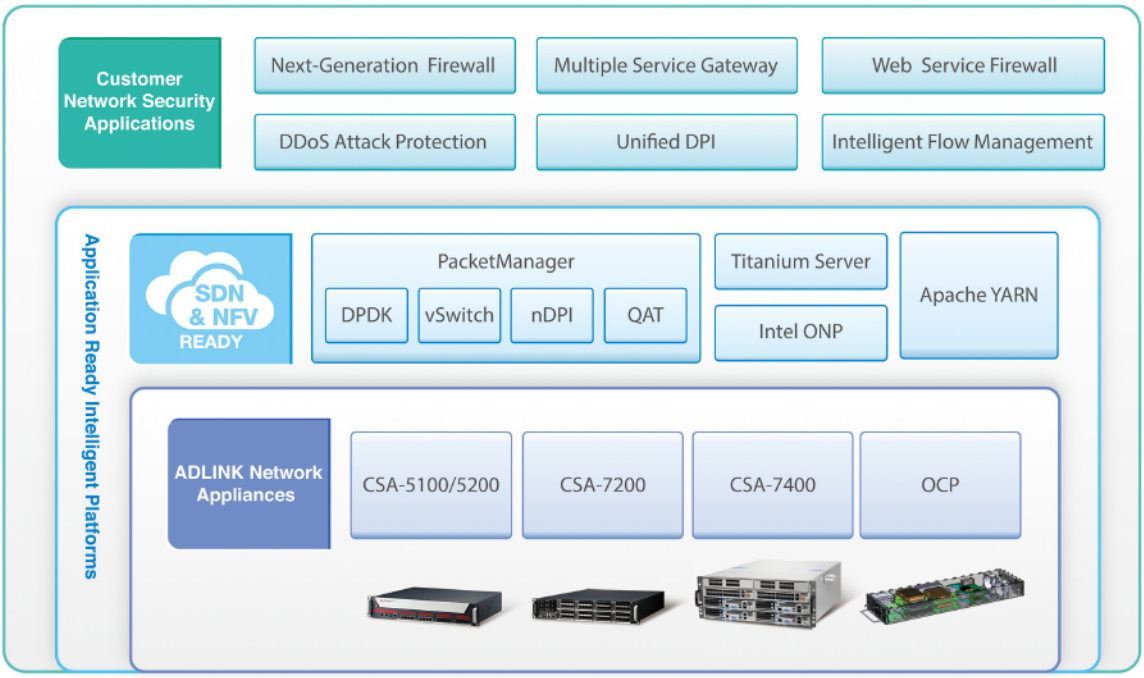


Figure 2. CSA ARiP Platforms from ADLINK Technology

ADLINK Technology provides PacketManager software for CSA platforms which integrates popular open source software such as DPDK and nDPI that are designed for network packet processing. By optimizing the runtime environment, PacketManager can help to develop network security applications that need DPI, flow classification, filtering, diverting, load balancing, and encryption/decryption. For a turn-key NFV solution, ADLINK CSA products integrate Intel® ONP and Wind River Titanium Server, which are both built on DPDK to achieve a high throughput and include support for SDN. For big data based DPI analytics, Apache YARN is also integrated and validated on the CSA platforms. PacketManager and the integrated third-party software stacks increase the performance of the CSA platforms; and also provide a rich set of features for present and future network security applications. Users can develop DPI and cloud computing security products based on CSA products more quickly, and bring new products to market more rapidly.

Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

Conclusion

Remote management and energy efficiency are must-have features when network security products are deployed in data centers. Both mid and top-range CSA products support IPMI specification v2.0 allowing the operating status of compute nodes, PSUs and fan trays to be monitored remotely. The LAN bypass mode of a NIM module can also be monitored or changed through IPMI extension commands. In order to reduce power consumption and achieve significant energy savings, CSA products implement adaptive fan speed control based on IPMI and intelligent CPU resource management enabled by Intel® Node Manager.

ADLINK Technology has taken great efforts to fully understand the requirements of DPI and cloud computing security in the IoT era, and introduced the CSA series of computing platforms to meet these requirements. By integrating high-performance DPI processing capability and support for NFV, SDN and hardware acceleration units, the CSA series forms a solid foundation for developing the next generation of network security equipment. CSA platforms are designed with a modular concept in order to achieve maximum intercompatibility of components across the product line and reduce total cost of ownership. ADLINK has also developed and integrated the requisite software components and open source middleware, reducing development efforts required by customers. The growth of applications in cloud computing is accelerating at a faster pace as we enter the IoT era, bringing with it an increasing number of network security threats. ADLINK Technology is committed to providing high-performance, high-availability ARiP platforms that meet the requirements of network security for industrial IoT, and will continue to analyze new trends and challenges in the network security industry, listen to customer feedback, and provide the best network security platforms built on open computing technologies.



Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000

WORLDWIDE OFFICES

ADLINK Technology, Inc.

9F, No.166 Jian Yi Road, Zhonghe District
New Taipei City 235, Taiwan
新北市中和區建一路166號9樓
Tel: +886-2-8226-5877
Fax: +886-2-8226-5717
Email: service@adlinktech.com

Ampro ADLINK Technology, Inc.

5215 Hellyer Avenue, #110 San Jose, CA 95138, USA
Tel: +1-408-360-0200
Toll Free: +1-800-966-5200 (USA only)
Fax: +1-408-360-0222
Email: info@adlinktech.com

ADLINK Technology Singapore Pte. Ltd.

84 Genting Lane #07-02A, Cityneon Design Centre
Singapore 349584
Tel: +65-6844-2261
Fax: +65-6844-2263
Email: singapore@adlinktech.com

ADLINK Technology Singapore Pte. Ltd. (Indian Liaison Office)

#50-56, First Floor, Spearhead Towers
Margosa Main Road (between 16th/17th Cross)
Malleswaram, Bangalore - 560 055, India
Tel: +91-80-65605817, +91-80-42246107
Fax: +91-80-23464606
Email: india@adlinktech.com

ADLINK Technology Japan Corporation

〒101-0045 東京都千代田区神田鍛冶町3-7-4神田374ビル4F
KANDA374 Bldg. 4F, 3-7-4 Kanda Kajicho,
Chiyoda-ku, Tokyo 101-0045, Japan
Tel: +81-3-4455-3722
Fax: +81-3-5209-6013
Email: japan@adlinktech.com

ADLINK Technology, Inc. (Korean Liaison Office)

경기도 성남시 분당구 수내로46번길4 경동빌딩 2층 (수내동 4-4번지)
(우) 463-8252F, Kyungdong B/D, 4 Sunae-ro 46 beon-gilBundang-gu,
Seongnam-si, Gyeonggi-do, Korea, 13595
Toll Free: +82-80-800-0585
Tel: +82-31-786-0585
Fax: +82-31-786-0583
Email: korea@adlinktech.com

ADLINK Technology, Inc. (Israeli Liaison Office)

27 Maskit St., Corex Building PO Box 12777
Herzliya 4673300, Israel
Tel: +972-54-632-5251
Fax: +972-77-208-0230
Email: israel@adlinktech.com

ADLINK Technology (China) Co., Ltd.

上海市浦东新区张江高科技园区芳春路300号 (201203)
300 Fang Chun Rd., Zhangjiang Hi-Tech Park
Pudong New Area, Shanghai, 201203 China
Tel: +86-21-5132-8988
Fax: +86-21-5132-3588
Email: market@adlinktech.com

ADLINK Technology Beijing

北京市海淀区上地东路1号盈创动力大厦E座801室(100085)
Rm. 801, Power Creative E, No. 1 Shang Di East Rd.
Beijing, 100085 China
Tel: +86-10-5885-8666
Fax: +86-10-5885-8626
Email: market@adlinktech.com

ADLINK Technology Shenzhen

深圳市南山区科技园南区高新南七道 数字技术园A1栋2楼C区 (518057)
2F, C Block, Bldg. A1, Cyber-Tech Zone, Gao Xin Ave. Sec. 7
High-Tech Industrial Park S., Shenzhen, 518054 China
Tel: +86-755-2643-4858
Fax: +86-755-2664-6353
Email: market@adlinktech.com

ADLINK Technology GmbH

Hans-Thoma-Strasse 11
D-68163 Mannheim, Germany
Tel: +49-621-43214-0
Fax: +49-621 43214-30
Email: emea@adlinktech.com

PENTA ADLINK Technology GmbH

Ulrichsbergerstrasse 17
94469 Deggendorf, Germany
Tel: +49 (0) 991 290 94 – 10
Fax: +49 (0) 991 290 94 - 29
Email: emea@adlinktech.com

ADLINK Technology, Inc. (French Liaison Office)

6 allée de Londres, Immeuble Ceylan
91940 Les Ulis, France
Tel: +33 (0) 1 60 12 35 66
Fax: +33 (0) 1 60 12 35 66
Email: france@adlinktech.com

ADLINK Technology Inc. (UK Liaison Office)

First Floor West Exeter House,
Chichester Fields Business Park Tangmere,
West Sussex, PO20 2FU, United Kingdom
Tel: +44-1243-859677
Email: uk@adlinktech.com

About the Intel® Internet of Things Solutions Alliance

ADLINK Technology is a Premier member of the IntelR Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 400+ global member companies of the IntelR Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions. Learn more at: intel.com/iotsolutionsalliance

ADLINK® Leading EDGE COMPUTING

intel IoT Solutions Alliance Premier

© 2017 ADLINK Technology Inc. All Rights Reserved. All Specifications are subject to change without further notice.
All products and company names listed are trademarks or trade name of their respective companies. Published in Sep. 2017.

LRI Distribuída no Brasil pela LRI | vendas@lri.com.br | 51 2129-3000