ADLINK
Leading EDGE COMPUTING

Intrusion Detection Systems and
Intrusion Prevention Systems (IDS/IPS) Solution

100G+ IDS/IPS Solutions that Enable Monitoring for, Detecting and Preventing Attacks

Joint release by
ADLINK Technology
NSFOCUS



www.adlinktech.com

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

100G+ IDS/IPS Solutions that Enable Monitoring for, Detecting and Preventing Attacks



Table of Contents

Introduction P1

New requirements and challenges for IDS/IPS P2

NSFOCUS NIDS/NIPS solutions and hardware platform requirements P4

ADLINK Network Security Platform CSA-7400 ..... P6

Conclusions P8

About NSFOCUS P8

Introduction

Network security challenges have become increasingly serious as we evolve from the Internet era to the IoT era. Not only has the number of organized, premeditated attacks across all networks increased, but the form of cyberattacks has become more and more complex and advanced.

In this new age of network security, the roles of the intrusion detection systems (IDS) and intrusion prevention systems (IPS) are gaining increasing importance with their continuous development and innovations. After outlining the new requirements for IDS/IPS equipment to maintain network security in the IoT era, this article will introduce how ADLINK's CSA-7400 high performance, high density and high scalability platform helped NSFOCUS to build next-generation 100G+ grade IDS and IPS that offer safer, more reliable and more stable solutions for carriers.

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

New requirements and challenges for IDS/IPS

As traditional firewalls find it increasingly difficult to handle the new types of intrusions in the cyber world, today's network protection requires more sophisticated and diversified capabilities. As a result, IDS/IPS have gradually become indispensable components for building an effective network security system. An IDS monitors network operations security by gathering and analyzing information on the entire network in order to instruct the operator of the required adjustments of security rules, while an IPS blocks intrusions by executing security rules in real time after in-depth analysis of network data.

Traditional detection technologies

- To enhance detection rates and minimize error rates, both IDS and IPS are equipped with comprehensive detection technologies including feature matching, protocol analysis and anomaly detection.
- Feature matching is by far the most commonly used due to its high accuracy and speed. Maximum efficiency of feature matching is dependent on the accuracy of the overall feature library and the feature matching capacity of the equipment.
- By discerning the operating principles of a protocol (usually based on RFC standards), protocol analysis searches for suspicious visit behaviors to detect overflow and denial of service (DoS) attacks. Effective use of this technology enables a high detection rate and a near-zero error rate.
- Anomaly detection discovers unexpected abnormal traffic through learning and adjusting the normal traffic criteria of a specific network environment. When the actual traffic statistics exceed the threshold value for a given traffic criterion, an anomaly detection alarm is sent.
- Despite their advantages, each technology has its flaws. For example, feature matching requires regular updates of the feature library to avoid omissions. Due to the wide variances in each protocol's implementation and unavailability of complete details for proprietary protocols, protocol analysis can usually only be realized for common protocols such as HTTP, FTP and SMTP. When threshold values are set improperly, anomaly detection can result in false positives. As the number of web-based networks and advanced persistent threats (APTs) continues to increase, the deployment of IDS/IPS relying on these traditional technologies will be inadequate.

Challenges of protecting web-based networks

HTTP is by far the most common source of network traffic. According to the TCP port traffic ranking statistics of the National Computer Network Emergency Response Technical Team/Coordination Center of China (CNCERT), the traffic on port 80 is far higher than that of other ports. Under such circumstances, increasing numbers of viruses, Trojans and botnets will naturally launch attacks via HTTP. New-generation web threats and cyberattacks are increasingly covert as a result of interest orientation. As they are hidden in legitimate traffic on the web, enterprises are often prone to attacks due to their dependency on the Internet for routine operations, thus exposing their information assets and key business to tremendous threats.

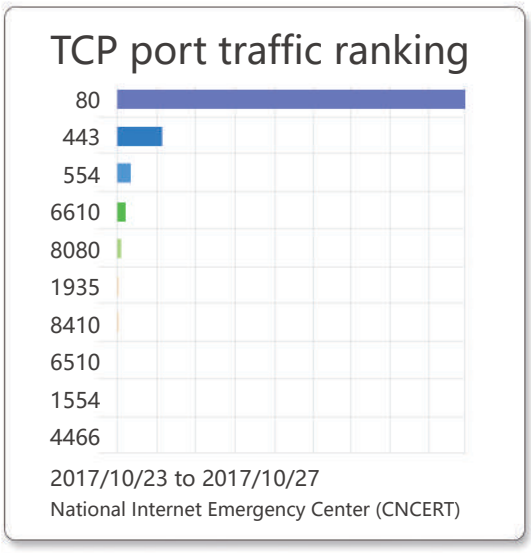


Figure 1 TCP port traffic rankings released by CNCERT.

Hence, a built-in web reputation mechanism is required to allow IDS and IPS to send timely warnings (IDS) or to block attacks (IPS) when users visit a webpage on which a Trojan has been implemented in order to effectively prevent infiltration of network security threats into the corporate intranet, leakage of sensitive data, and other information security incidents.

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

Application of deep packet inspection technology

The main difference between an IPS and a traditional firewall is that the former can perform deep packet inspection (DPI) of packet contents. If a hacker launches attacks through the vulnerability in Layers 2-7, an IPS can detect and then block such attacks from the data flow. By contrast, the traditional firewall can only detect the quintuple of a data packet (source IP address, source port, target IP address, target port, and protocol at the transmission layer), without detecting the contents at the application layer or individual bytes, thus overlooking many attacks. As an IPS checks each byte of data traffic, it identifies most mainstream application protocols based on its protocol recognition framework. Then, through nuanced management of the identified information, it can detect the security vulnerabilities in these applications and take the initiative to prevent web attacks. Application identification using DPI generally requires equipment with large-scale parallel computing ability to filter and detect tens of thousands of packets per second, as well as being able to perform IP defragmentation, TCP stream aggregation and data flow status tracking.

User-based behavioral analysis

In recent years, the mobile network has become an important infrastructure for enterprises, resulting an increasing number of intranet infiltration incidents via wireless networks. In wireless network deployment, open Wi-Fi hotspots for visitors allowing unauthenticated access to the corporate network has become increasingly popular. In addition, employees working off-site may access the company network from their homes, airports and customer's premises. While effective, these wireless networks often lack effective management, allowing hackers to easily bypass the company's firewalls, making wireless networks a stepping stone into the company's intranet.

As the second security gateway after the firewall, IDS/IPS offers user identity and user access control to effectively resolve broken access control (BAC) problems brought about by the roaming of unauthenticated equipment and employees. With the statistical analysis of employee network visit activities of a company, a normal web visit pattern can be built upon features including user identity, geographical location, operating time, visit contents and visit frequency. The system can accurately detect abnormal behavior deviating from the normal visit pattern and send alarms (IDS) or block the activity (IPS).

Advanced Persistent Threats

Stealing core data is often the goal of APTs. Web attacks and intrusions launched on corporate users are often premeditated over a long period of time and highly concealed. APT attacks are like a special forces team equipped with comprehensive and sophisticated weapons that can paralyze the defensive power of the corporate web environment's traditional firewalls and antivirus programs.

IDS/IPS bring better probability for successfully dealing with APTs. By performing network traffic visualization, an IDS will send alarms after detecting traffic anomalies to minimize the losses caused by APTs. Through collaboration with the local threat analysis system and based on the APT sample, behavior analysis and virtual execution technologies, an IPS can discover advanced malicious codes hidden in the traffic and dynamically adjust its protection strategy to block malicious traffic in real time.

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

NSFOCUS NIDS/NIPS solutions and hardware platform requirements

To allow customers monitor for, detect, and prevent attacks, NSFOCUS offers its brand new NIDS and NIPS intrusion protection solutions.



- In addition to a having an advanced attack rule feature library for detecting known security threats, NSFOCUS' NIDS is equipped with a continually updated reputation feature library that can reduce hazards brought by unknown malware and effectively prevent persistent intranet infiltration with its intranet security function, thus minimizing leakage of sensitive data and abnormal external connections to servers.

- NSFOCUS' NIPS is equipped with a world-leading attack feature library and real-time reputation library. To respond to advanced threats, an integrated sandbox detection capability is used to realize 3D protection for both known and unknown threats. The use of flow virus detection technology can capture hotspot viruses to maximally enhance antivirus capacity. The integrated mobile phone housekeeper realizes a secure enquiry push and secure status real-time monitoring to reduce the workload of maintenance and operation staff.

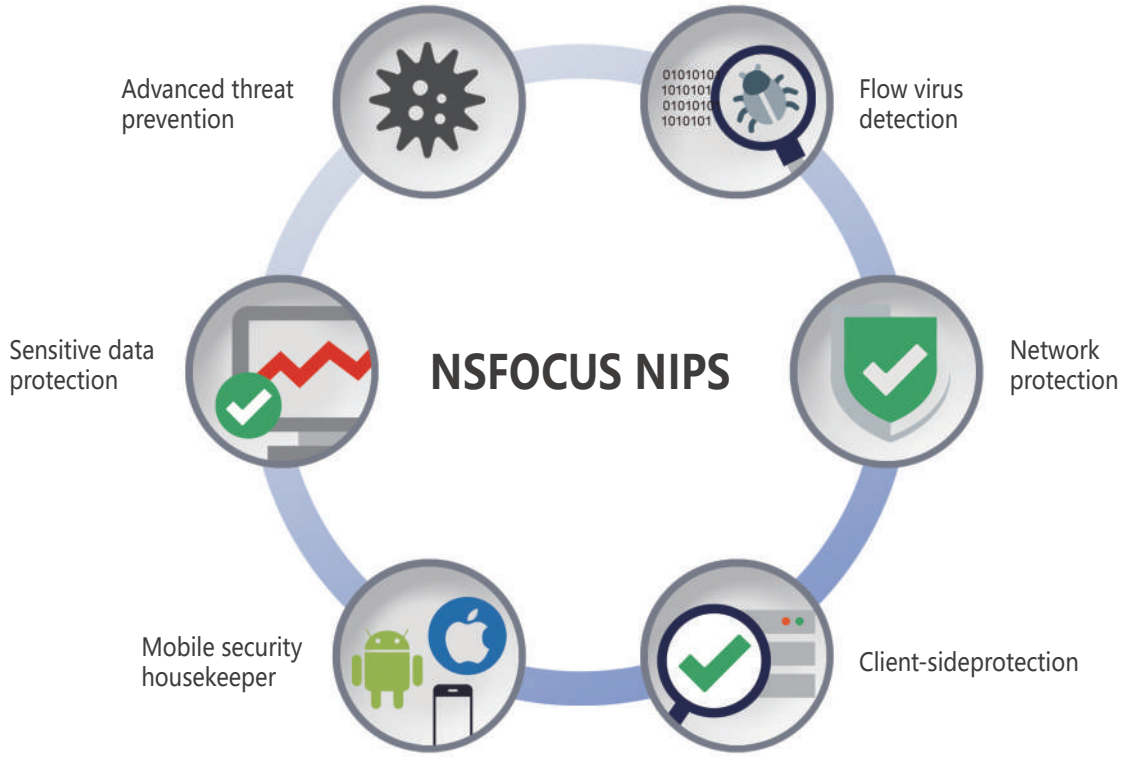


Figure 2 Main technology advantages of NSFOCUS NIPS.

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

To support the security characteristics and requirements of next-generation 100G+ grade NIDS/NIPS platforms, NSFOCUS proposes the following computing platform requirements:

High throughput capacity and I/O density

To better meet the demands of high-end application scenarios of operators such as core networks, cloud computing centers, large enterprises and IDC outlets, NSFOCUS requests support of the 100GB interface on computing platforms for its IDS/IPS products, with each piece of equipment supporting a minimum of 800G traffic connection and of a minimum of 64x 10GB ports. The network ports must support upstream and downstream port consistency and RSS.

Parallel computing and computing density

To support deep packet inspection and other detection methods, NSFOCUS requests that NIDS/NIPS computer platforms support parallel processing capability. In particular, network packet processing platforms should be equipped with wire speed transceiving capability, have the maximum possible computing density per rack unit, and have a zero packet loss rate for small packets of 64 bytes.

Load balancing, same source and same host

In NSFOCUS' NIDS/NIPS, all data traffic is connected by means of a switch board which balances the traffic load to individual processor boards. When processor board errors are detected, the switch board can redirect the traffic. To ensure processing of the same conversation at the same CPU node, the switch board must support the same source and the same host to automatically merge the data flow of the same conversation.

Carrier-grade high availability

As a NIPS platform must be incorporated into the traffic path, NSFOCUS requires the modularization of computing platforms in a carrier-grade industrial design to provide uninterrupted services for users with hot swap capability for faulty components (compute, switch, PSU, fan, and storage).

Support for standardized API management

To reduce low-level development burdens, NSFOCUS requires the support for standardized API management of hardware platforms with a set of standardized APIs for traffic and hardware management of all components on the rack, port and VLAN management, commonly used L2/L3 switch protocol stacks, and remote reboot.

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

ADLINK Network Security Platform CSA-7400



Figure 3 CSA-7400, next-gen high-performance telecommunications COTS

Product features

As a next-generation high-performance telecommunications COTS DPI and network security platform, the CSA-7400, built on ADLINK's Open Compute Carrier-grade Edge Reference Architecture (OCCERA), achieves high-speed interconnection of compute nodes with dual-redundant switch nodes to offer front panel I/O up to 800GB. The CSA-7400 supports hot swapping of major chassis components to protect uninterrupted business, making it suitable for the next-generation high-performance IDS/IPS. The main features of the CSA-7400 are summarized as follows:

- Up to four compute nodes with dual Intel® Xeon® Processor E5-2600 v3/v4 or Intel® Xeon® Scalable Processors with support for single sled upgrade or hybrid deployment.
- Dual-redundant switch design with bandwidth of 4x 50GB per node for internal interconnection of four compute nodes, including 4x 100GB or 36x 10G upstream panel I/O.
- Switch supports accelerated processing of NVGRE/VXLAN tunneling protocols to meet the needs of Layer 2 network in cloud computing.
- ADLINK PacketManager software that provides commonly used Layer 2, Layer 3 switch protocol stacks and flow-based strategic control API, load balancing, same source and same host functions to accelerate application development.
- Supports smart system management using IPMI-based specifications for remote system diagnosis, redirection, shutdown, and startup.





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

Meeting NSFOCUS requirements

The requirements for the NSFOCUS next-generation NIDS/NIPS computing platforms are listed in the left column of the table below, and the corresponding features of the CSA-7400 from ADLINK are in the right column.

Requirements for NSFOCUS NIDS/NIPS computing platforms	Features of ADLINK's CSA-7400
Supports ultra-high throughput interface and equipped with 100GB, 40GB and 10GB interfaces.	Modular I/O designed for scalable bandwidth according to actual needs. Supports high speed 100GB/40GB interfaces and provides up to 72x 10GB interfaces. Compared to currently popular 2U network security equipment which support a maximum of 64 x 10GB interfaces in the same 4U rack space.
Supports high density parallel processing and equipped with higher data packet processing performance; 64-byte small packet processing.	The 4U space supports four dual Intel® Xeon® Processor E5-2600 v3/v4 boards or Intel® Xeon® Scalable Processor compute nodes to provide industry-leading processing performance and density. Compared to currently popular 2U network security equipment which support only one dual Intel® Xeon® processor board, the CSA-7400 4U space supports two dual Intel® Xeon® processor boards with the addition of excellent small packet (64 bytes) performance. Each compute node can process over 50GB of data with zero packet loss rate.
Load balancing, same source and same host	In addition to the load balance function for users to set different load weights for individual compute nodes, the switch board supports automatic elimination of faulty nodes in the load balancing process to ensure reliable processing of data flow. The switch board also supports same source and same host realized by hardware to efficiently merge network conversations.
High availability and full protection for hardware stability	Carrier grade high availability is achieved by design including PSU redundancy and component hot swap. These designs also support real-time out-of-band monitoring of module operation through IPMI. Stringent QC for product stability and reliability
A standardized API management interface is provided for packaged interchange and traffic and hardware control.	ADLINK PacketManager equipped on the CSA-7400 platform from offers port and VLAN management and protocol stacks for LACP, LLDP, RSTP, and VRRP. In addition, the CSA-7400 achieves high-performance smart forwarding of traffic via ACL as well as remote monitoring and reboot.

"According to NSFOCUS, With our expertise in attack prevention developed over the years, this in-depth collaboration with ADLINK enables both parties to build IDS/IPS products meeting the demands of high-end application scenarios such as core networks for operations, cloud computing, large enterprises, and data centers. The interconnected redundant module design and hot swap support for both computing nodes and switches of the OCCERA-based CSA-7400 platform from ADLINK offer users uninterrupted delivery service.

NSFOCUS' NIPS products are equipped with various advanced technologies such as the NSFOCUS global threat intelligence system and NSFOCUS unknown threat detection can demonstrate better protection on the CSA-7400. In the future, NSFOCUS will continue close collaboration with ADLINK for its IDS/IPS products to maximize the effectiveness of the excellent features of NSFOCUS' NIDS/NIPS products on CSA-7400 platform for the network security market."

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



Other applications for network security and telecommunications

The table above shows that the CSA-7400's high bandwidth, high density, high performance, and high reliability features meet the overall high computing capability requirements of today's network security products. ADLINK further integrates the latest virtual machine (VM) technology for information and communications into the hardware platform to provide the requisite features for developing security application products. In addition to IDS/IPS computing platforms, the CSA-7400 can be used for next-generation firewalls, telecommunications DPI and network virtualization, and mobile edge computing (MEC).

Conclusions

The CSA-7400 is a next-generation, high performance, carrier grade COTS network security platform built on the Open Compute Carrier-grade Edge Reference Architecture (OCCERA) by ADLINK, integrating network interfaces, switches, and overall computing capacity. The open hardware architecture and platform scalability of the CSA-7400 support NSFOCUS' next-generation 100G+ IDS/IPS solutions, allowing NSFOCUS to launch its high-performance NIDS/NIPS products for the network security market. The CSA-7400's flexibility and configurability enables cross-business product deployment and easy integration to other high-end network security markets, such as next-generation firewalls, telecommunications, and mobile edge computing. In addition to hardware features, the API library provided by ADLINK allows security solution providers focus on their core competence, enhance business migration increase product efficiency, and shorten product launch and delivery cycles.

About NSFOCUS

NSFOCUS is committed to tracking the latest trends in network security vulnerability research around the world, continually extending vulnerability analysis, mining, and engineering technology to enhance the technical standards of IDS/IPS, anti-DDoS, malware, and attached behavior analysis and detection. Furthermore, NSFOCUS spares no effort to actively engage in the research and development of cloud security and virtualization security, software as a service (SaaS)-based security services, security measurement, security reputation, and security intelligence.

Over the past two years, NSFOCUS Security Labs has published integrated reports on trends in security threats, next-gen security architectures, IPv6 security research, and security for industrial control systems. As of the end of 2017, NSFOCUS has published 96 notices on security vulnerability research and assisted Microsoft, Cisco, and Oracle on the discovery and resolution of over 94 security vulnerability problems, making it an important contributor to the national vulnerability database. The NSFOCUS Vulnerability Database (NSVD) is the leading Chinese vulnerability database in China.
NSFOCUS website: https://nsfocusglobal.com/

LRI 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 용인시 수지구 신수로 767 A동 1008호
(동천동, 분당수지유타워) (우) 16827 A-1008, U-TOWER,
767 Sinsu-ro, Suji-gu, Yongin-si, Gyeonggi-do,
Republic of Korea, 16827
Toll Free: +82-80-800-0585
Tel: +82-31-786-0585
Fax: +82-31-786-0583
Email: korea@adlinktech.com

ADLINK Technology, Inc. (Israel 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: +86-21-5192-3588
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

(Mannheim) Hans-Thoma-Strasse 11, D-68163,
Mannheim, Germany
Tel: +49 621 43214-0
Fax: +49 621 43214-30

(Deggendorf) Ulrichsbergerstrasse 17, 94469
Deggendorf, Germany
Tel: +49 (0) 991 290 94 – 10
Tel: +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

ADLINK® Leading EDGE COMPUTING

intel IoT Solutions Alliance Premier

All products and company names listed are trademarks or trade names of their respective companies.
All specifications are subject to change without further notice.

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