OASis: Towards Extensible Open-Architecture Services Platforms

Yaxuan Qi[1], Fei He[1], Xiang Wang[2], Xinming Chen[1], Yibo Xue[3] and Jun Li[3]
[1]Department of Automation, Tsinghua University, Beijing, China
[2]School of Software Engineering, University of Science and Technology of China, Hefei, China
[3]Tsinghua National Lab for Information Science and Technology, Beijing, China
{yaxuan, yiboxue, junl}@tsinghua.edu.cn, {hefei06, chen-xm09}@mails.tsinghua.edu.cn, kojiroh@mail.ustc.edu.cn

ABSTRACT
In this paper, we propose an extensible Open-Architecture Services platform (OASis) for high-performance network processing. OASis embraces recent advances of open technologies, including open source software, open system standards and open network architectures. Three programming models are proposed for target-specific processing modules: a multi-granularity packet processing model for network processing; a thread-isolated parallel programming model for service processing; and a message-based management model for centralized system administration. As an application example of OASis, a Unified Threat Management (UTM) prototype is implemented. This prototype provides multiple network security services, including stateful firewall, intrusion detection, and virus scanning. Experimental results show that, the OASis-UTM prototype can achieve 40Gbps stateful firewall performance together with 4-8Gbps intrusion detection and anti-virus performance on a 12U 14-slot ATCA platform.

General Terms
Architecture, Security

Keywords
Open Architecture, Network Processor, ATCA, UTM

1. INTRODUCTION
With the increase of Internet traffic and the multitude of network services, the need for both performance and flexibility has become the key challenge for novel network services platforms (NSP). The rapid growth of Data Centers (DCs), the IP convergence of telecom services, and the security requirement of enterprise networks together make the great demand for high-performance NSP. Recently, both academic and industrial world initiated research programs on open technologies, which encourage research innovation and allow third parties to develop software extensions for proprietary hardware [1, 2]. Based on the inherently collaborative and distributive nature, open technologies will benefit the NSP design from multiple aspects: open source software enables faster deployment of novel services; open system standards make it possible to consolidate functionalities from multiple vendors into one physical box; open network architecture reduces network redundancies and thus save unnecessary cost. In this paper, we propose an Open-Architecture Services platform (OASis) by exploiting recent advances of open technologies.

2. OASis Design
OASis embraces multiple open technologies to meet the performance and flexibility requirements: Its software architecture supports existing open source software; its system architecture employs the ATCA open technology; and its data-plane network takes advantages of open network architectures. OASis contains the following processing modules:

1) **Network processing module (NPM)**: NPM provides the external network interfaces and packet forwarding engine for OASis. NPM is responsible for front-end network processing, including packet routing, flow classification, connection state maintenance and traffic management. NPM is also responsible for load-balancing among back-end services processing blades. Due to the high-throughput requirement and relatively simple operations, NPM is implemented on a network processor (NP) based blade.
2) **Service processing module (SPM)**: SPM provides flexible application-level processing capability to meet the requirement for the ever-evolving network services. With the help of front-end load-balancing, the overall performance of OASis can be increased by adding new SPM blades in the ATCA chassis. SPM is implemented on Intel Architecture (IA) based blades to gain maximum programming flexibility.
3) **Control processing module (CPM)**: Because OASis is a cluster system conducting distributed processing, a system-wide control processing module is necessary for centralized management. CPM provides an extensible management model for system initialization, monitoring and update. CPM also provides the GUI/CLI interfaces for OASis administrators.

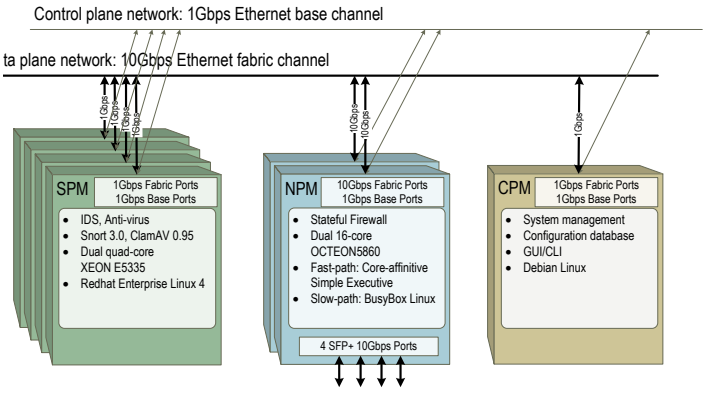

Figure 1. System Architecture of OASis UTM

Table 1. OASis-UTM components

MODULE	FUNCTION	HARDWARE
Chassis	Blades carrier base and fabric switch	Radisys ATCA-6010 12U, 14Slots 1G/10Gbps base/fabric
NPM	Stateful inspection Traffic management	Radisys ATCA-7220 Dual OCTEON5860 NP BusyBox Linux
SPM	Intrusion detection Anti-virus	Intel IA blades Dual XEON E5335 Redhat Linux 4
CPM	System management Device monitor GUI/CLI interfaces	Intel MPCBL-0040 Debian Linux

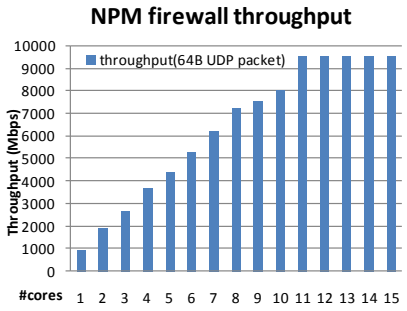

Figure 2. NPM SI performance

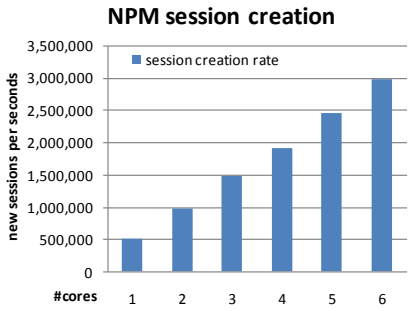

Figure 3. NPM session creation rate

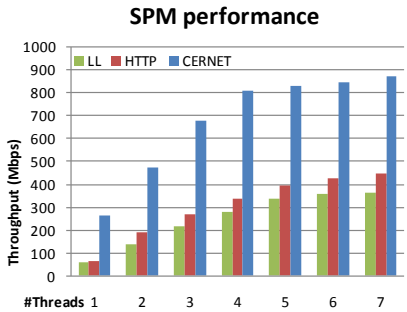

Figure 4. SPM DI performance

3. An Example Application: OASis-UTM

As an application example, a Unified Threat Management (UTM) prototype is implemented on the OASis platform. This prototype provides multiple network security services, including stateful firewall, intrusion detection, and anti-virus. OASis-UTM is based on a 12U 14-Slot ATCA chassis, which provides two switch fabrics at back-plane [3]. The 10Gbps dual-star switch fabric is used for data-plane interconnections and the 1Gbps dual-star switch fabric is for control-plane management. NPMs are based on Cavium OCTEON5860 NP blades, while SPM and CPM are based on Intel XEON IA blades. All incoming packets are first processed by NPMs for stateful inspection (SI). Then, according to user-defined policies, some packets are sent to SPMs for deep inspection (DI). After that, legitimate traffic is sent out from the NPM external interfaces, while malicious ones dropped. CPM provides the GUI/CLI interfaces for system monitoring and policy configurations. Figure 1 is the system overview of OASis-UTM. Blades specifications are shown in Table 1.

4. PERFORMANCE EVALUATION

According to our design, the 12U 14-Slot chassis has 2 switch blades, 2 NPM blades, and 10 SPM blades. Leveraging the NPM, which has two OCTEON5860 processors, and advanced packet classification [4] and session maintenance [5] algorithms, the overall SI performance is expected to be 40Gbps. In addition, each SPM can provide 400~800Mbps intrusion detection and anti-virus performance, so the overall DI performance is 4~8Gbps. Test results are shown in Figure 2~4.

5. ACKNOWLEDGEMENT

This work was supported by National High-Tech R&D 863 Program of China under grant No. 2007AA01Z468, and by an Intel University Program.

6. REFERENCES

[1] P. Crowley, D. McAuley, T. Woo, J. Turner, and C. Kalmanek, Open Router Platforms: Is It Time to Move to An Open Routing Infrastructure? ANCS '07, 2007.

[2] J. Turner and P. Crowley, Internet Scale Overlay Hosting, http://groups.geni.net/geni/wiki/Internet Scale Overlay Hosting

[3] http://www.radisys.com.cn/Products/ATCA/Processing-Modules/Promentum-ATCA-7220.html

[4] Y. Qi, L. Xu, B. Yang, Y. Xue, and J. Li, Packet Classification Algorithms: From Theory to Practice, Proc. of INFOCOM '09, 2009.

[5] F. He, Y. Qi, Y. Xue and J. Li, SANS: A Scalable Architecture for Network Intrusion Prevention with Stateful Frontend, Proc. of ANCS'09, 2009.

[6] http://www.snort.org/

[7] http://www.clamav.net/