Proceedings of the 2009 IEEE International Conference on Systems, Man, and Cybernetics
San Antonio, TX, USA - October 2009

A Low-Cost Green IT Concept Design of VHSP based on Virtualization Technology

Chih-Hung Chang *Student Member, IEEE*
Degree Program of CS, College of Computer Science
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.
jason.pcs96g@nctu.edu.tw

Tzu-Chien Hsiao
Department of Computer Science / Institute of BME
National Chiao Tung University
Hsinchu, Taiwan, R.O.C.
labview@cs.nctu.edu.tw

***Abstract*—In this paper, we proposed a low-cost and flexible Virtual Honeynet Security Platform (VHSP) and a design methodology of the Virtual Honeypot Redirect Mechanism (VHRM), which is All-in-One virtual system architecture, design and implement such platform to verify the effectiveness of the architecture and method that designed in this paper. Moreover, the main contribution of this work is not only to propose a more optimum utilization strategies for S/W and H/W resources, but also a research platform of network security with higher flexibility, usability and this conforms to the latest concept of Green IT design as well.**

***Keywords*—Virtual Honeynet Security Platform (VHSP), Virtual Honeypot Redirect Mechanism (VHRM), Virtualization Technology (VT), Honeypot, Honeynet.**

I. INTRODUCTION

Since 1999, Honeynet Project [4] an international non-profit organization (NPO), has devoted a lot of efforts to improve and strengthened the network security, which is also its major goal as well. Based on the open-source software technology, this NPO has jointly developed many relevant software instruments and trapping technologies, such as Honeypot. The trapping system (Honeypot) adopted by researchers that mostly within a physical network environment, and established in an open network space in accordance with the concept of a distributed and independent single system or virtual system. In addition, it will make use of a great quantity of physical hardware equipment to deploy that may cause the consumption on computer and network resources. Honeynet includes various Honeypots and network security components, thus it has managerial limitation in the flexibility, time limit, technological integration and security for dynamic deployment. After then, software and hardware resource utilization is comparatively low, and meanwhile it also lacks for the effective application of strategic integration; therefore, there are still a lot of space should be improved. Thus, we integrated the virtualization technology (VT) [2][7] and Honeynet technology with the concept of Defense-in-Depth network [6] and adopted the Public Network IP as the basis for the system design, and then properly deployed to the physical network architecture or Internet application. Therefore, its will not only reduce the cost of establishing the physical system, but also can save the spatial cost of physical system's occupation for physical computer engine room, which is conformed to the main idea of latest concept of Green IT [12] design.

The rest of this paper is organized as follows. In Section II, briefly reviews the basic concepts and background information of the virtualization and Honeynet technologies. Next, a design methodology of the virtual honeypot redirect Mechanism (VHRM) and Virtual Honeynet Security Platform (VHSP) logic network architecture will be exposed in Section III. In addition, experiment mentioned in Section IV that conducted on the basis of the feasibility and availability for this All-in-One virtual architecture and the designed network architecture, and the VHSP comparison of different Honeynet design methodology with hardware resource optimum utilization strategy. Finally, section V concludes this work.

II. BACKGROUND INFORMATION

This section provides the necessary background required to appreciate the work presented in this paper. All of the virtualization concepts are presented in Section II-A to D. Xen virtualization concepts and definitions are presented in Section II-E. In Section II-F introduces preliminary Honeynet concepts. While a brief overview of Honeynet composing components is given in Section II-G. The concept of Defense-in-depth network is presented in Section II-H.

A. Virtualization Technologies

Since the development of Virtualization Technology (VT) it is a matured and important concept and technology at present. The earliest conception of Virtualization was a method that proposed by IBM in 1960 [1][4], and set up on the Mainframe of IBM System 360-67; moreover, it has definitely become an important tool and technology [2] for the design and evolutionary development of computer system.

B. Full Virtualization Technology

Full Virtualization Technology [1][4] will establish a whole new virtual operating system, also known as Guest OS, which is able to operate directly in the local operating system, and can make use of VMM to control the system resources without needing to modify the Guest OS or application program (Apps).

Currently, Full virtualization Technology still adopt the Binary Translation (BT)[9] approach, as a result of implementing CPU command under the Ring 0, thus the hardware equipment of the lowest level can be directly accessed and then sent to VMM for further implementation.

The advantage of the full virtualization is that is able to establish most diverse platforms without modifying the kernel of Guest OS; however, relative lower efficiency is its weakness.

C. Paravirtualization Technology

Paravirtualization Technology [3] is acknowledged as the most rapid and safe software virtualization technology in this industry at present. Comparing with full virtualization, it only needs about less than 10% system efficiency consumption and requirement; as for the basic testing of the Xen Source Virtual Machine, it generally turned to consume less than 5% of system efficiency, and that can be regarded as a breakthrough for related technologies. On the contrary, the system efficient consumption with adopting other virtualization technologies will be reached 35%, or even higher [3][10]. Therefore, the main advantage of using the paravirtualization technology is that can provide a higher application scope of efficiency than the full virtualization technology, but the weakness is need to modify its operation system kernel.

D. Hardware-assisted Virtualization Technology

Currently, Intel ® VT-x [1] and AMD-v™ [9] are 2 types of the hardware virtualization technology, both of they were added new implementation mode into CPU, which called as the root mode. Such mode can make VMM to operate under the root mode and it locates beneath Ring 0 and on the same layer as VMM. The status of Guest OS will preserve in the Virtual Machine Control Structure or the Virtual Machine Control Block of AMD-v™ CPU that supports Intel ® VT-x and AMD-v™ can use the hardware-assisted virtualization function.

E. Xen Virtualization Technology

Xen [3] initialed its developmental in 2002, and developed by the x86 platforms, the Computer Science Lab of University of Cambridge, UK. In addition, based on the open-source software, and conformed to the agreement of GNU Public License (GPL) to make development. Its main purpose is to make use of the most simplified approaches to modify the current operating systems in the x86 Architecture; at the same time, perform more optimum virtualized efficiency in the current virtualization technology [5]. Comparing with the VMware[5] that proposed in 2005, and it is a paravirtualization interface, or named as the Virtual Machine Interface (VMI), the Xen paravirtualization that adopted by Xen, the Xen Guest OS kernel [3] can only be operated in the Xen ® Hypervisor [10][13], but VMI Guest OS can be supported to various Hypervisors. If adopting the Xen paravirtualization, then it needs to modify the system kernel for Guest OS; therefore, due to their respective advantages and defects, they can be flexibly deployed in accordance with the practical requirement.

Xen adopted the Borrowed Virtual Time scheduling algorithm (BVT), which proposed by Kenneth J. Duda and David R. Cheriton [11] in Stanford University in 1999, and the main purpose of applying such algorithm to Xen by its R&D Team is to reduce the system events that may influence the operating efficiency for the virtualization system. When a domain received an event, such algorithm possesses more low-latency after event occurred. Xen virtual system technology, as shown in Figure 1, which includes: Xen managerial programs, virtual domain, virtual domain management and control module, paravirtualization and hardware virtual machine Guest OS. Five major components of Xen [3] are shown as follows:

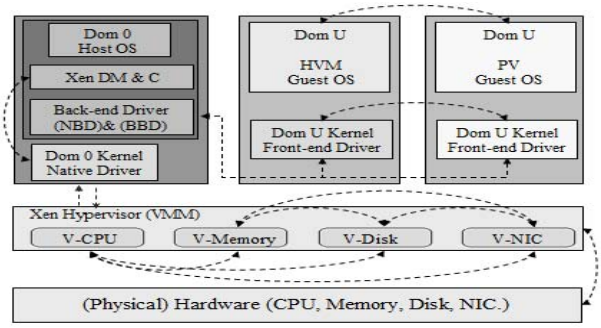

Figure 1. The architecture of Xen 3.x Hypervisor environment.

Xen VMM, or named as Xen ® Hypervisor, its major function is to allocate and manage the hardware resources to each Guest OS. In Hypervisor, through Hypercalls [3], it can request service from the system, such as using the system call to communication in the kernel of physical operating system.

Domain 0, or also known as Dom 0, which possesses special authority in the Xen architecture, and can access physical I/O resources and coordinate the system and network operations of Guest OS. Dom 0 includes 2 drivers, and they respectively are (1) Network Back-end Driver (NBD) and (2) Block Back-end Driver (BBD), where NBD is responsible for network communication and BBD is for the disk storage. Xen Domain Management and Control (Xen DM&C), its main function is conducted comprehensive control and management for all system services, processes and virtual domain environment on all Domain U. Paravirtualization (PV) Guest: All of the virtual machine will be called as the Domain U or Dom U or Paravirtualization (PV) Guest and XenoLinux that operated in the Xen Hypervisor; its System Kernel should be the complier of Xen. Hardware Virtual Machine (HVM) Guest will simulate the BIOS of real operation system through the Xen Virtual Firmware. Xen Virtual Network Technology [13] Dom 0 Network default is adopted the Virtual Network-Bridge technology to preset all network communication of Dom U, and it should be connected to the network with using the outbound bridge method. Xen Virtual Network-Route will generate the routing table for all Dom U in the Dom 0, and use IP router approach to communicate physical network. Xen Virtual Local Area Network (VLAN) supports multiple tagged IEEE 802.1Q VLANs technology. It is mainly used to conduct the network subnet segregation for Dom U; meanwhile, it also can communicate other Dom U with network cross-subnet.

F. Honeynet Environment

Most Honeynet architectures [15] are in the public physical network, and are the network that composed of many Honeypots. Honeynet is able to operate the real operation system environment, and, currently, most of they were designed in the High-Interaction architecture. In addition, it can be mixed to sue with Honeyd [13] which is used to simulate the operating system and service software and it is categorized as the Low-Interaction system architecture.

G. *Honeynet Composing Components*

The five major Honeynet components such as Firewall which is to control all internal and external network packets for whether they conformed to the Firewall Security Policy, inspect the Network Protocols, IP Address and Port. IPS [8] is mainly functioned to identify the threat in network and can be effectively defended through the deep packet inspection technology. The Honeypot seemed like an insecure system with defects and vulnerabilities. Its main purpose is used as a trap against the intrusion activity, or an early warning mechanism for the network security defense. Back-end Database System's major function is stored related Log into the system. The Monitor & Management System primary function is to monitor and collect all data and Logs from various equipment and devices, and it can be defined in accordance with monitoring scope.

H. *Concept of Defense-in-depth Network*

The major function of the Defense in Depth network [6] is to strengthen and enhance the defense level for network security. It is not a single barrier that can be intruded, but is a complex and multilayer defense system with integrating various information security technologies and security policies. In terms of the information security technology, it is an integrated application that included various network security components and various applicable software defense systems.

III. DESIGN AND IMPLEMENTATION

The design methodology in this section is to take Xen open-source software as the basis; we were mainly used the paravirtualization and hardware virtualization technology to support the full virtualization environment; in addition, as for the virtual Honeynet components, we adopted the open-source software of Honeywall [7] to design and implement.

A. *VHSP Architecture Design*

The network logic architecture that designed as shown in Figure 2, We adopted the concept of defense in depth network with integrating the firewall, IPS, Honeypot and DB system as the basis of data collection, and through the Web Management Interface (WMI) to conduct system monitor and management.

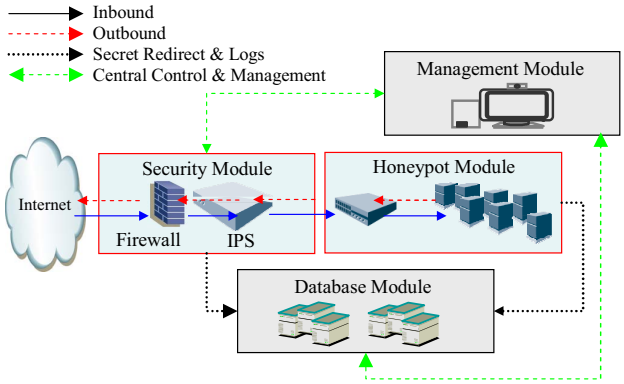

Figure 2. The architecture of VHSP network environment.

B. *VHSP Module Design*

The five basic modules that designed in this section as shown in Figure 3:

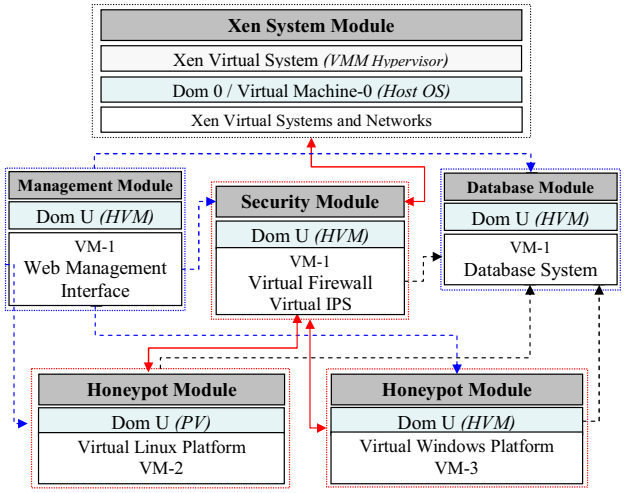

Figure 3. The structure of VHSP Module based on Xen environment.

1) *Xen System Module*

Xen module has been described in Figure 1 of this paper, which is a basic component of the virtual system operation.

2) *Security Module*

Security Module includes two major components:

a) Virtual Firewall

We adopted iptables as the checkpoint of the network interface connection and the establishment of packet in/out regulations.

b) Virtual Intrusion Prevention System (Virtual IPS)

We adopted the technology integration of IDS Snort-inline as the components of intrusion detection prevention and deep packet inspection.

3) *Honeypot Module*

As for all Virtual Honeypots that included in the Honeypot Module, we adopted Sebek's Rootkit Technology. Sebek client can confidentially return the information and Log of honeypot back to Sebek server for the purpose of data collection.

This work is mainly taken Linux and Windows platforms as the components of Honeypot Module.

4) *Database Module*

We adopted the MySql DB as the storage center for all information and record.

5) *Management Module*

We adopted HTML and Perl webpage program as the management and monitor components for the module and network events in the virtual system.

C. *VHSP Virtual System Design*

As shown in Figure 3, by considering the future flexible deployment and application strategy, all modules; therefore, it can be dynamically increased, reduced and modified. Furthermore, under the virtualization, all Guest OS, regardless of PV or HVM Guest, are image format files (ISO) and can be strategically made backup.

D. *VHSP Virtual Network Design*

As described in Figure 1 of this paper, due to the network default of Dom 0 is the front-end of all outbound network communication for Dom U; therefore, it shall go through NBD at first and then connect to the physical network driver. However, Dom U is parallel; thus, all packets that go in/out Honeypot Module will be processed by Network-Bridge of NBD, as shown in the solid black-line path of Figure 4, and directly connected to the physical network driver; however, it will ignored the Security Module and cannot monitor and make log. In order to solve the Network Flows, therefore, we modify Guest OS are parallel questions. This section has proposed the Virtual Honeypot Redirect Mechanism (VHRM). Its designed approach is to direct packets of Honeypot Module to NBD of the Xen Dom 0 at first, and then redirect to Security Module after processed by Isolated Virtual Network, as shown in dotted red-line path of Figure 4.

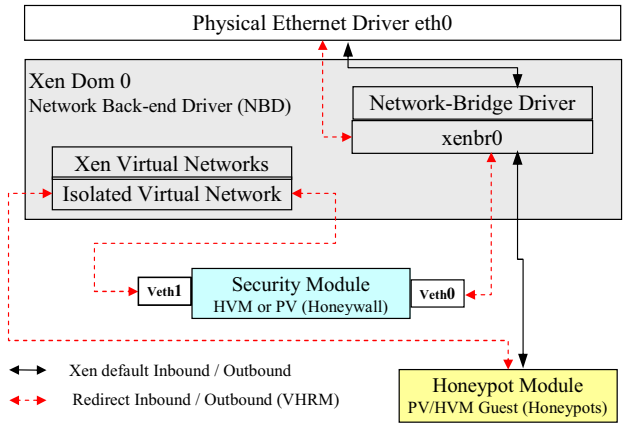

Figure 4. Design of IVN Module based on VHRM approach.

E. *VHSP of Isolated Virtual Network (IVN) Module Design*

In this section, the shortest path will be considered as the design concept, VHRM's major advantage is adopted layer 2 network protocol when data flowing outbound VHSP. In addition, comparing with this, it can be slowed and reduced more efficiency consumption for NBD in Dom0 than layer 3, and the efficiency flows in layer 2 is more rapid than in layer 3. Moreover, Security Module's virtual network interfaces, Veth0 and Veth1, are also adopted the same approach of layer 2 to conduct the network flows, and used the transparent mode to transfer packets; at the same time, through management module and database module to collect data and monitor all network events. The VHSP flow design and steps are shown as follows: We take the outbound design flow which briefly described as the red line. As shown in Figure 5.

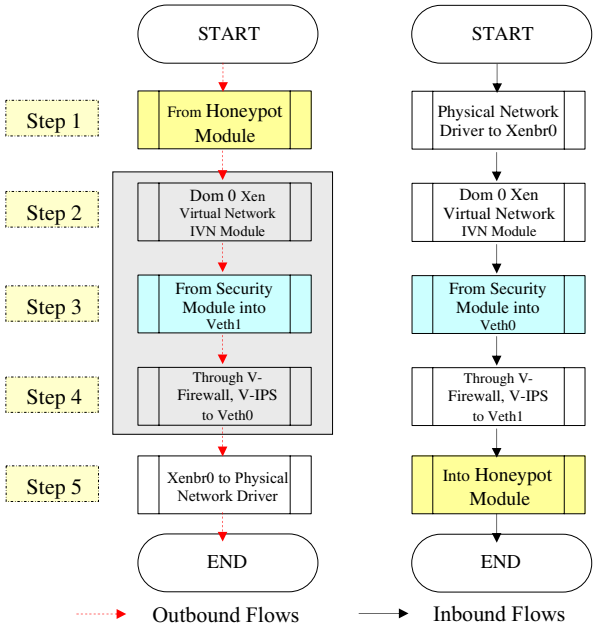

Figure 5. Flow chart of IVN Module design methodology.

- **Step 1 : Honeypot module to IVN Module**
  In the first step, to make all packets inside the Honeypot Module to redirect toward to the Xen Virtual Networks of Dom 0.
- **Step 2 : IVN Module to Security Module of Veth1**
  Connect to Xen Virtual Networks and switch to the IVN module.
- **Step 3 : Veth1 to Veth0**
  Use layer 2 to lead packets from IVN module to the network interface Veth1 of Security Module.
- **Step 4 : Veth0 to xenbr0**
  All data flows are gone through the network interface Veth1 of Security Module to Veth0 with passing Virtual IPS and Virtual Firewall respectively.
- **Step 5 : xenbr0 to Physical Network Driver**
  Data flows are also through the bridge connection mode from Veth0 to directionally connect with the xenbr0, which is the bridge network driver of NBD component in Dom 0. Finally, use bridge mode to transfer data to the eth0, a physical network driver, via xenbr0. The design flow of Inbound is contrary.

F. *VHSP Network Operation*

Firstly, the part of VHSP network operating flow design will be displayed by the complete flow of the overall system module and network; and as for the part of network flows, it has been described in Section III-D and Section III-E of this paper. Secondly, as for the part of using the WMI management interface to monitor and manage, researchers can externally access to VHSP via the "NAT to physical device" of "Xen Virtual Network". Veth2 adopted the private IP logon to improve the security of connection. Via the external physical

network to logon the WMI, and access to the Veth2 to manage the Virtual Firewall, Virtual IPS and Virtual Database systems; however, all connections were controlled and limited by system's security policy. Finally, in the future, each module and functionality can be improved respectively.

IV. Experimental Results

In this section, we use the Nessus [14] software and the scan software of Port Scan to verify VHSP which designed in this section. Nessus is a set of open-source software, and a well-functioned Nessus Vulnerability Scanner. Its main function is to conduct the in-depth security examination and system analysis with aiming at various system platforms and network vulnerabilities for Linux, UNIX, Windows, etc. Furthermore, the main purpose of this experiment is to simulate various practical vulnerabilities and online attacks.

First of all, we connect to Web Management Interface (WMI) in VHSP via web, as shown in Figure 6. The overall operating system and network with the logon record of abnormality or attack can be observed from the administration page. Next, on the upper-right corner, a heading listed as: Created: Wed Jan 14 08:50:49 2009 Last Update: Tue Feb 24 16:24:33 2009, and existed a simple real-time flow curve diagram. In such diagram, a yellow right triangle can be seen, and it means that there were more than 2000 Kbytes transferred at the time point of "Feb 24 16:24:33 2009." Moreover, we can see the topics of Bidirectional Flows and Total Flows on the upper-left corner of this figure, and the numbers of "In and Out" logon are displayed under them respectively. The underneath "1 Hour" and "24Hour" are indicated that 19794 logons existed within previous 24 hours, and the number of total flows is 19886; in addition, the most important key is that the number of flows for "1 Hour" has hit the mark as high as 18212; at the same time, we correspondingly reflect the rightmost "ids" on this column and that indicated 8 warning Logs in 18212 logons.

Next, a column titled as the "Top 10 Honeypots" on the lower-left corner of the WMI management interface, and showed 16 events of sending 19779 session IDS for one IP's connections within a short period of time (most of them were the attack connections). In such figure, other related basic information for network statuses existed respectively, including the information of Host, connections, IDS events, etc., and can implement the real-time analysis on the abnormal flow status and warning.

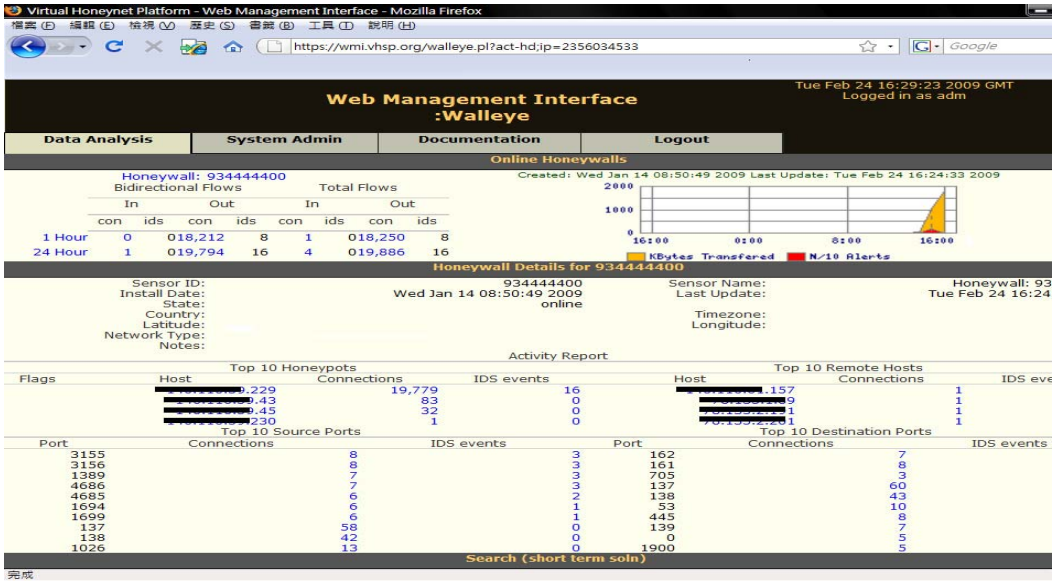

Figure 6. Web Management Interface (WMI) based on Virtual Machine Monitor (VMM) environment.

As displayed as the following Figure 7, we can make use of the Virtual Machine Manager for Xen control software to monitor the allocation status of real-time resources for Xen System Module and the efficiency analysis for each module's operation.

In addition, for consideration on performance, one unit of entities equipment is rather difficult to compare with many units of entities equipment, but if we focus for its resource utilization, flexibilities in deployment strategies, re-configurability, as well as the most important of the above-mentioned H/W cost should be a better way.

Finally, we know the Honeynet Project [4][15] against the proposed virtual honeypot possible method [15] are using VMware [5] and other VT, while our proposed design of virtual honeypot platform adopted Ian Pratt's [3] emphasis paravirtualization that it can provide the similar speed to its operating system [3], although we need to modify the Kernel of PV Guest OS.

But take performance into consideration [3], this work propose a virtual Honeynet of the All-in-One VHSP are using paravirtualization based on XenoLinux environment, and also will be the better solution for Honeynet architecture design.

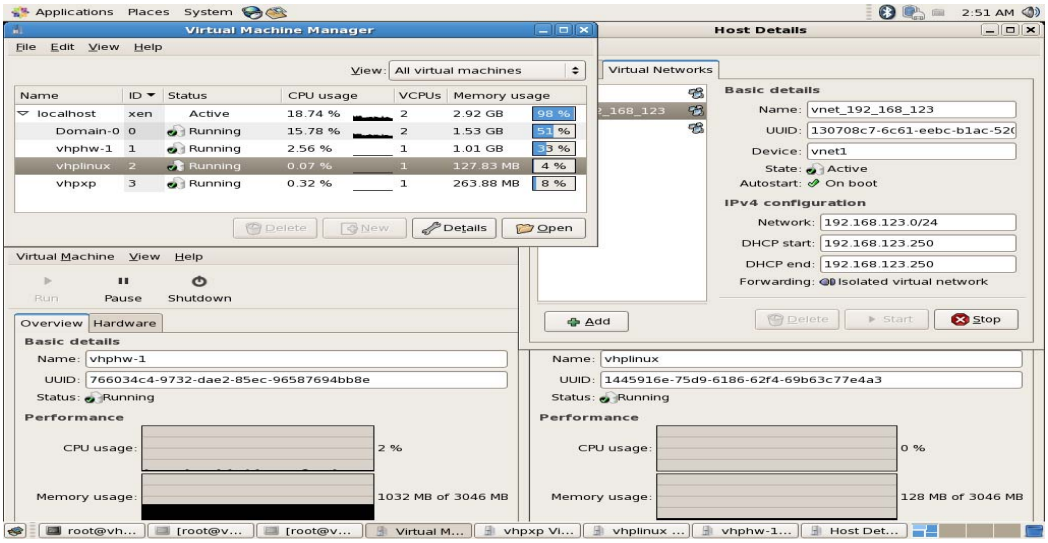

Figure 7. VMM based on VHSP monitor interface.

V. CONCLUSIONS

The main purpose of this paper is to improve the concepts and strategies of Honeynet architecture designed; a low-cost and flexible VHSP is proposed. The VHSP expects to reduce management complexity and H/W cost that it has resulted from great deployment in a traditional system of Honeynet and network environments.

We have contributed a better operating strategy of S/W and H/W resources, a design approach of VHRM with a more flexibility and usability have been certainly proposed.

Therefore, we can prove that the proposed architecture has the superior performance for the research platform of Internet and network security and is able to enable researchers to make use of the development and application. In the near future, we can then be based on the energy conservation concept of Green IT [12] Design for internet security.

REFERENCES

[1] Xiantao Zhang, Yaozu Dong, "Optimizing Xen VMM Based on Intel Virtualization Technology", in Proceedings of the IEEE ICICSE International Conference on Internet Computing in Science and Engineering, pp. 367-374, 2008.

[2] Uhlig, R., Neiger, G., Rodgers, A.L., Martins, F.C.M., Anderson, A.V., Bennett, S.M., Kagi, A., Leung, F.H., Smith, L. "Intel virtualization technology", IEEE Journal of Computer, vol. 38, pp. 48-56, May. 2005.

[3] Paul Barham, Boris Dragovic, Alex Ho, Rolf Neugebauer, Ian Pratt, Andrew Warfield, "Xen and the art of virtualization", in Proceedings of the ACM symposium on Operating systems principles, pp.164-177, 2003.

[4] Spitzner, L., "The Honeynet Project: trapping the hackers", IEEE Journal of Security & Privacy, vol. 1, pp15-23, Mar. 2003.

[5] Xu, Xianghua, Zhou, Feng, Jiang, "Quantifying Performance Properties of Virtual Machine", in Proceedings of the IEEE ISISE International Symposium on Information Science and Engineering, pp. 24-28, 2008.

[6] Nen-Fu Huang, Chia-Nan Kao, Hsien-Wei Hun, Chia-Lin Lin, " Apply data mining todefense-in-depth network security system", in Proceedings of the IEEE AINA International Conference on Advanced Information Networking and Applications, vol. 1, pp. 159-162, 2005.

[7] Chamales, G., "The Honeywall CD-ROM", IEEE Journal of Security & Privacy, vol. 2, pp. 77-79, Mar. 2004.

[8] Koller, R., Rangaswami, R., Marrero, Smith, G., Barsilai, M., Necula, S., Sadjadi, S.M., Tao Li, Merrill, K., "Anatomy of Real-Time Intrusion Prevention System", in Proceedings of the IEEE ICAC International Conference on Autonomic Computing, pp. 151-160, 2008.

[9] Wei Chen, Hongyi Lu, Li Shen, Zhiying Wang, Nong Xiao, Dan Chen, " A Novel Hardware Assisted Full Virtualization Technique", in Proceedings of the IEEE ICYCS International Conference for Young Computer Scientists, 2008, pp. 1292-1297, 2008.

[10] Xu, Xianghua, Shan, Peipei, Jiang, "Performance Evaluation of the CPU Scheduler in XEN", in Proceedings of the IEEE ISISE International Symposium on Information Science and Engineering, pp.68-72, 2008.

[11] Kenneth J. Duda, David R. Cheriton, "Borrowed-virtual-time (BVT) scheduling", in Proceedings of the ACM symposium on Operating systems principles, pp. 261-276, 1999.

[12] Murugesan, S., "Harnessing Green IT: Principles and Practices", IEEE Journal of IT Professional, vol. 10, pp. 24-33, Jan. 2008.

[13] Wira Zanoramy Ansiry Zakaria,, Ahmad, Siti Rohaidah, Aziz, Norazah Abd, "Deploying virtual honeypots on virtual machine monitor", in Proceedings of the IEEE ITSim International Symposium on Information Technology, pp.1-5, 2008.

[14] Yoshimoto, M., Bista, B.B., Takata, T., "Development of security scanner with high portability and usability", in Proceedings of the IEEE AINA International Conference on Advanced Information Networking and Applications, vol. 2, pp. 407-410, 2005.

[15] Honeynet Project, Know Your Enemy:Learning about Security Threats, Second Edition, Addison-Wesley Professional Publishers. May 27, 2004.