International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:10, 2009

Description and Analysis of Embedded Firewall Techniques

Ahmed Abou Elfarag, A. Baith M., Hassan H. Alkhishali

Abstract**—** With the turn of this century, many researchers started showing interest in Embedded Firewall (EF) implementations. These **are** not the usual firewalls that are used as checkpoints at network gateways. They are, rather, applied near those hosts that need protection. Hence by using them, individual or grouped network components can be protected from the inside as well as from external attacks.

This paper presents a study of EF's, looking at their architecture and problems. A comparative study assesses how practical each kind is. It particularly focuses on the architecture, weak points, and portability of each kind. A look at their use by different categories of users is also presented.

Keywords**—**Embedded Firewall (EF), Network Interface Card (NIC), Virtual Machine Software (VMware), Virtual Firewall (VF).

I. INTRODUCTION

THE term firewall was adopted by security experts to describe a way of keeping unwanted intruders from breaking into a network connected to a larger network. One most likely heard the term used in the building trade [1].

Traditional firewalls are those which are designed to protect the entire network, by putting them on the network's gateway so that the outgoing and incoming traffic filtered through them; so the firewall blocks the bad traffic and allows the rest to go to its destination.

From the functional aspect, Embedded Firewalls can be shown to achieve nearly all the functions that traditional firewalls can do. So the user can choose the embedded firewall and use it in exactly the same way as traditional firewalls, as discussed by Quan Huang et. al. [5].

An issue that forces itself**,** mentioned by Lynn M. [2], that there are big challenges that the firewalls can face inside the network as well as the ones that come from outside**.** Naturally, traditional firewalls cannot handle this kind of challenges. Since the huge evolution of networking technology and since the network resources are needed to be accessed by many people from different places, It is difficult to know if the biggest risk came from outside or from inside the network. But Markham *et. al.* [3] argued that there is an understanding that the security risks that come from inside the network are greater than those coming from outside. Intruders (hackers) understand the availability of traditional firewalls; they can easily bypass them through many ways. They are able to go beyond a traditional firewall and access all the network resources, and all the employee's computers will be without protection. However, by using the EF there will be a firewall to each resource and computer inside the network. It will be more difficult for the hacker to break every firewall to access the computer or server. There will be many checkpoints that the hacker will face. If the hacker himself is working inside the network he can access the resources or make changes to the setting or even infecting the network with any virus easily. So in this case there is a need to rethink network security systems and how they can be better protected by using other technique than the traditional choke point firewalls.

Another important issue is the single choke point firewall. Here the network security of the establishment totally depends on a single firewall, so any breakdown to the firewall by any attack, power outage, or even a failure in the firewall software or hardware, all the people inside the network will be totally disconnected from the Internet, as a protective measure. Another good reason to have a closer look at firewalls that in case any computer inside the network is infected through a flash disk, or e-mail attachment, the whole network will unwittingly be infected within the firewall this leads to thinking seriously about protecting single sites (computers) directly through the use of Embedded Firewalls, Chu-Hsing *et. al.* [4].

To select a good firewall, it is so important to study the different kinds, and make some comparison between them. This paper looks at the Separate Machine EF, the Virtual EF, and the Distributed EF. It presents a summary on the architecture of each kind, and the principle on which it is working on. Each of the three kinds has its own advantages and disadvantages, so anyone who needs to build his firewall must be aware of the characteristics and drawbacks of his choice. This paper is concerned only with the architecture of each kind.

In the next section, categories of EFs will be described, and then an analysis of each kind is carried out. After that there will be point of view description for three different categories of users, and then there will be an illustration of how the main types of firewalls provide the requirements for each category.

II. EMBEDDED FIREWALL ARCHITECTURE

Different architectures are used to implement EFs which**,** according to published work, can be summarized to fall into three categories:

A. Separate Machine Embedded Firewall

This kind of architecture has approximately a similar implementation by Vassilis Prevelakis [7]; through use of a portable "shrink-wrapped" firewall (referred to as Sieve). It is a portable separate machine running on an embedded system which uses the compact Flash (CF). This bootable CF contains an operating system that includes firewall capabilities. The separate machine is usually placed between the general-purpose computer and the network. It can be used wherever the user is. Fig. 1 shows that by accessing network resources, the user workstation runs the risk of having its

communications intercepted, or being attacked by malicious third parties.

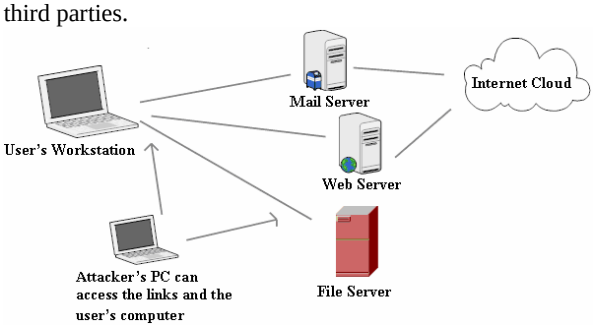

Fig. 1 The risk of not having a firewall

While fig. 2 shows that the firewall (Sieve) provides the firewall protection services and creates secure links to other servers in the network, establishing a secure overlay network that is inaccessible by third parties [7].

In order to use a platform that could accommodate tools for remote monitoring and management**,** OpenBSD 2.9, from the available UNIX or UNIX-like systems**,** was used. This system was chosen because it has built-in Support for the transport layer security protocols (IPSec) that offers secure communication channel, It is similar to other free UNIX clones, a large number of programs such as tcpdump, snmpd, ssh, and so on are either supported in the base release or are available through the system ports, and it has a good security. The designers of the OpenBSD have paid a lot of attention to the security profile of the system, creating a robust environment.

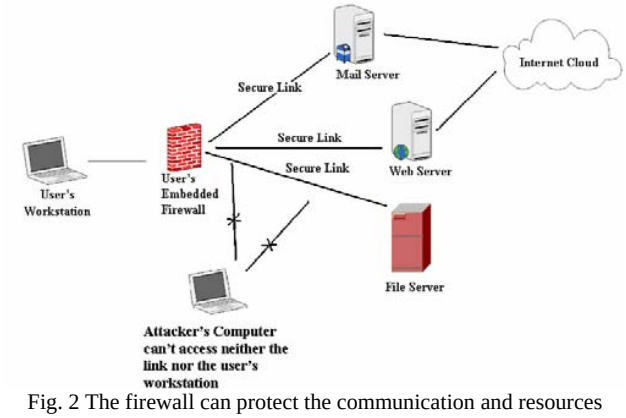

Fig. 2 The firewall can protect the communication and resources

B. *Virtual Firewalls*

The firewalls in this category run under the host operating system within a virtual machine. The usual virtual machine environment used is VMware, which means that the technique described here can be used for both Windows and Linux platforms. The virtual firewall imitates the hardware firewall device with the exception that it is entirely software-based. This kind of firewalls has been implemented also by Vassilis Prevelakis [8]. Fig. 3 shows the integration of the VF within a Windows host environment. The host operating system has minimal access to the network (enough to support bridging between the guest VM running the Virtual Firewall and the network). As far as the host OS is concerned the VF is its default gateway (i.e. the only way for IP traffic to reach the outside world). The VF has to have at least two Network Interface Cards (NIC), an internal (virtual) interface for communication with the host OS and the external, which is bridged to the outside network. The VF runs an embedded version of the OpenBSD 3.7 system which boots off a read-only medium and contains only firewall-related software.

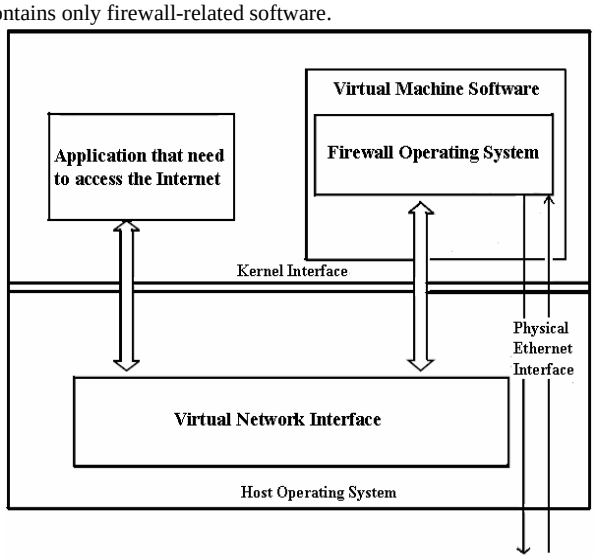

Fig. 3 Integration of the VF within an OS host environment

C. *Distributed Embedded Firewall System*

The Distributed Firewalls project developed an innovative and complementary approach to traditional perimeter solutions. This approach split the traditional perimeter firewall into a central policy server and distributed policy enforcement points, allowing an organization to set security policy from a central location, but *enforce* policy at host machines [2].

Charles Payne *et. al.* [6] illustrated this kind of firewall. The firewall is implemented on the host's Network Interface Card (NIC), and is managed by a central, protected policy server elsewhere in the network. The NIC has a tight processing loop and limited memory, so complex processing is performed elsewhere (e.g. on the embedded firewall policy server).

Also Charles Payne *et. al.* [6] stated that the NIC relies on its driver upon each host reboot to download its runtime image into the firmware. To ensure that the host remains protected, the embedded firewall NIC stores enough information in non-volatile memory, to verify the integrity of its runtime image. Once a NIC is configured for embedded firewall, it cannot be disabled except by performing the appropriate action on the policy server. In other words the embedded firewall NIC will become inoperable if its runtime image fails the integrity check. The helper agent in the NIC sends regular heartbeats to the policy server to help the policy server detect NICs that may not function. Like all other communication with the policy server, the heartbeat is encrypted by the embedded firewall NIC. If a malicious user were to replace the embedded firewall NIC with other NIC, the heartbeats for that NIC would effectively stop, raising the suspicions of the embedded firewall administrator [6].

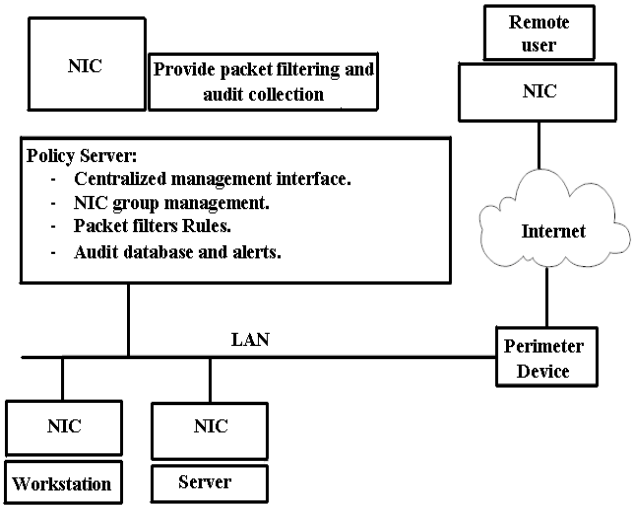

Fig. 4 Distributed Embedded Firewall Architecture

III. Critical EF Analysis

A closer look at the characteristics of each of the EF categories reveals the following:

A. Separate Machine Embedded Firewall

In separate machine architecture, it can be noted that the firewall is fully independent of the user's machine, and does not depend on any other machine or server. This can be considered to be an advantage because being fully independent means any damage to the firewall will not affect the user's computer. Also, any damage to the user's computer will not lead to repair both firewall and computer, or to reconfigure the firewall. This kind is preferred as reconfiguring, upgrading or even replacing the firewall is merely a matter of dealing with the firewall part.

The only problem with this kind is the extra hardware that the user needs to carry wherever he goes. This problem can be solved by using smaller architecture. One also may compare carrying the hardware versus the security risks that may be faced; mostly the decision will be to carry that device with him.

B. Virtual Firewall

Virtual firewalls are easy to implement, can be independently installed in many platforms and adjusted for each platform separately. On a first look one can think they are similar to the separate machines, and may be better since the user does not have to carry an extra device.

However, it is notable that many problems can be faced with this type of EF, not because of the policy or the OS that runs the firewall, but because of how the Virtual Machine (VMware) runs the architecture. An essential characteristic of a virtual machine is that the software running inside is limited to the resources and abstractions provided by the VMware. It cannot break out of its virtual world. Also there is no direct connection between the virtual machine and resources; the connection is through the OS that the VMware is installed onto**.** This leads to two problems regarding the firewall: Firstly, if any damage occurs to the main OS that the VMware is running on, the VMware will be affected directly and if there is no big damage to the firewall there will be a slowing down. Secondly, the overload that the processor will suffer; it is well known that the VMware will use the resources that are already used by the main OS, so the processing time will be affected for both the Firewall, and the main OS, and this will lead to delay that will be noticeable, add to that the bugs that the VMware may have which affects its proper working [9].

It can be concluded here that this kind of EF depends on the operating system that must be protected. How can anyone build a security system that relies on the software that it is meant to protect? In this case the owner of the firewall will need to enhance the host OS so that it can protect the VMware from being affected by any damage that happens to the host OS, and hence it can be said that the owner of the firewall will enter an infinite loop of who is protecting whom?

C. Distributed Embedded Firewall

This kind of firewall can be considered as one of the best kinds that can be used to protect the network, since there is a robust connection between the different devices that forms the firewall. Moreover, using the NIC to incorporate the embedded firewall inside it can be used as an advantage since it removes the worry about resource sharing like the virtual firewall, or the burden of carrying an extra device like in the separate machine EF. This type can be considered as integration between the traditional firewalls and EFs.

In the definition of the Distributed firewall in section C (Part II) according to Lynn M. Meredith [2], it is mentioned that the Distributed Firewalls project an innovative and complementary approach to traditional perimeter solutions, i.e. all the advantages and benefits of the traditional firewall can be found; but also many of the traditional firewalls' problems may also exist with this kind of firewall. This firewall depends on two things to work properly, first, the NIC of the protected machine, which must have a special processor and memory, and amended firmware enable it to be used with the firewall embedded within it. This NIC has a tight processing loop, and the solution has to fit within those bounds as. It is also stated that the memory of the NIC is limited and, therefore, complex processing is performed elsewhere leading to extra process time [3]. Also this special NIC is available for desktop computers, but if there is a need to use Laptops, the question will be: is there any similar hardware compatible with it? Even if there is another hardware supporting the USB, or the wireless connections, this means that we will build our firewall depending on single type of connection, changing the type of connection means additional cost to support all the computers with the new special device . Second, a central policy server, which manages the firewall, and its vicinity, is somewhere on the network, and the NIC of the host will rely on its driver upon each host reboot to download its runtime image into the firmware from that server. So if that central policy server suffers from any kind of problems (don't say that a hacker break in it or a flooding attack matter, but say any damage or sudden crash, or power outage), our firewall will be destroyed, and maybe all the work will be stopped till the centralized policy server is fixed. Furthermore, there is a need to protect the links between the policy server and the hosts NICs, and this will present additional security problem other than the main one for which the firewall was built in at the

first place. So there is a need to protect the firewall itself so that it can protect the network!

It is worth to mention here, that it is right that this kind of firewall is an embedded one, but we can not say that it is totally embedded, since there is an extra device which is the policy server, and without this device the firewall cannot work. Strictly, when the firewall is defined as an embedded; it means that the whole firewall including its policy is embedded in the device that is used as a firewall.

We can also note that this kind of firewall has limited portability, since the user can not take the computer and work in a place which is outside the network perimeter, unlike the separate machine or the Virtual EFs, when saying that building an EF is useful, there is a need to include the matter of portability.

IV. A Comparative Look at Types of EFs

The following table gives a comparison summary on the different types of EF:

TABLE I
COMPARISON SUMMARY BETWEEN DIFFERENT TYPES OF EFS

	Separate EF	Virtual EF	Distributed EF
Power	-External Power, or over Ethernet.	-Need no power.	Policy server needs external power.
Processing time	-Depends on the Board hardware.	-Depends on the resources of the pc. -How the VMware can Access the resources?	-Number of hosts requesting a service from the server. -Encryption speed of the data to be transmitted from NIC to server. -Is there processing need to be done in the server due to limited NIC's RAM?
Portability	-Easy to use inside and outside the network.	-Can be used also inside and outside the network.	-Can be used only inside the network.
Firewall Machine Security	-No special security measure needed, due to the independency of the EF.	-Need to secure the firewall by securing the host's OS.	-Connection between NIC and Server need protection. -Policy server needs protection against failures and attacks.
Hardware	-We can get a complete firewall using many kinds of hardware.	-The H/W here is the same of the pc.	-Special NIC's are needed here. -Need additional hardware for the policy Server.
Privacy	-Each user/group can have a firewall device and a different policy than the others.	-Each user has a firewall, and a diff-errant policy from the others.	-Each user has his own first part of the EF in the NIC, but all have a common policy server.
Firewall Flexibility	-Has maximum flexibility, in damage situations' having the CF is enough to run the EF on other hardware.	-Work only as it is, in case of hardware failure, sys-tem must be built from scratch.	-There is no alternative way to implement the firewall with other components.
Cost	-Depends on the cost of the hardware used to implement the firewall. -For companies the EF may be expensive since it needs to provide hardware to each employee.	-The cost here is the price of the VMware. -Most Unix-based OS's are free and they mostly used for firewall's OS	-Depends on the price of the NIC used, which must be available to all the users -Special NIC for each computer and the server cost here need to be taken into consideration.
Connection types	-Can use a H/W that provides all connection types.	-All connection types will be available as the pc provides them.	-Need additional H/W to provide other connection types.
Weak Points	-The user will have to carry an extra device with him. -Need to be careful so that the device not stolen.	-No direct interface with the resources. -No dedicated resources for the firewall. -VMware may have bugs that affect the proper work.	-Single point of failure, which leads to whole system failure, like traditional firewall.

V. Firewall Point of Views

The intention here is to match the kinds of firewall previously presented with the needs of different categories who consider the firewall as important to their work.

There will be a discussion to the important points that are needed by each category (Employee in the company, Firewall Administrator, and Company Management).

A. Employees point of view

This category opinion is important, because they can provide the company management and the administrator with criteria that can be used to decide on the kind of firewall to be provided.

This category will be interested in the flexibility of the firewall, since the ease of accessing the network of his company remotely and securely is so important, also the privacy will be one of the points that the employee may need. For example, if the employee is a team leader, he must be able to access more resources and perform more tasks than the rest

of the team; in this case his firewall policy must be different. Another example, in a company have many job levels and also many departments, so the employee in the sales department of course needs different policy than the one in the technical department, and both have different levels of policy than the employees in the accounting department.

B. Firewall Administrator point of view

This category is responsible for the firewall and its proper operation. They have to provide the requirements of both the employee and the company management at the same time.

Any administrator wants the best resources that are available in the markets, so that he can implement a strong firewall; without any cost concern. The matter of power can be considered very important to the firewall administrator. Any failure to the firewall due to power outage will lead to big vulnerability to his network.

The type of the firewall is so important for this category. Choosing a kind that can be available to every machine is better for the administrator, since controlling the situation is better with this type. Choosing this kind of firewalls will also be good so that he can control who can access which server, and will be better than monitoring the server's log to see if there is any intruders from inside the company. Add to that there will be a protection to the network from the uncontrolled data flow which is resulted from the infection of one of the computers with worm.

It can be said that security can be provided by any kind of Internet security products like Norton, Kaspersky, etc. The answer here is simple, that the administrator is dealing with people who are not experts in network security or network risks. So, an employee who is prevented from opening a site due to Internet security might just turnoff or override this prevention and, possibly, cause the contamination of this machine and the network. When the specific EF used, the user is not able to unplug the firewall and at the same time continue to have access to the Internet. Some firewalls can not be unplugged like the Virtual and distributed ones, but the separate machine can be unplugged. However, provision can be made so that there will be no Internet and no network resources unless the firewall is in service. A well administered firewall cannot be reconfigured by an employee. But the same employee can easily right click on the Internet security icon and click on Pause Protection!

C. Company management point of view

This category can be considered as the bottleneck that can block many of the requirements of the firewall administrator and the employee.

Cost is a primary concern for management; it plays a great roll in decision making. Due to limited budgets and other requirements, any item receives only a share of the expenditure and, therefore, even an important requirement like a firewall may not receive all the money needed. The mature solution for them can be summarized with two main points:

- Try to find a kind of firewalls that can be evolved without expensive developments. Spend a little more money at the first place, and buy something that can be evolved easily and live with you longer than the other cheap products.

- The way to implement the firewall is so important. A well planned and well designed firewall implementation prevents future unnecessary expenses. One should aim for a robust solution that meets all requirements even at a higher initial price.

A study of the firewall failure or weak points on the specific network helps to decide on the type, i.e. whether to employ a traditional firewall or one of the EF types. The other issue is the power consumption especially for those firewalls which have centralized servers. It is well known that most of the Control Rooms have a UPS (Uninterrupted Power Supply). Choosing the appropriate UPS is related to correctly calculate the power consumption of the devices found in the control room. The robustness of the firewall is also important here; the owner needs a robust firewall that has fewer problems so he has not to pay for fixing.

VI. Discussed Firewalls versus Selected Point of Views

This part will discuss how different firewall types meet the requirement of each category.

1) Traditional Firewall

This type can accommodate many of the requirements of the three selected categories, and also have many drawbacks to them. For the company management, selecting the appropriate hardware and software so that the cost of the firewall decreases, also a good study to the hardware's power consumption can be useful too. Add to that the robustness of the firewall can be guaranteed at least when talking about the incoming stream of data from outside the company. Here the role of the administrator will come; he knows that the above points are good for him too, because the management and the administrator have the same level of desire to have a good and robust firewall. The administrator knows and must tell the management the risks and the danger of leaving the inside of the network unprotected, it looks like having a guard at the gate and he doesn't know what is happening behind him. The management will have a good idea and will start to think as the administrator. But for the employee, he will not have the privacy that he needs, add to that the policy will be implemented for all the departments in the same machine, so they will lose their connection if the firewall has any problem. The employee wants to accomplish his work without restrictions, unless he has other intendance to open malicious sites or to hurt the company with some worms, here the bad points of the traditional firewall will appear since on the other hand we have a good employees that need to accomplish their work with no worms or risks facing their machines.

2) Embedded Firewalls

In general this type is better for both the management of the company and the administrator. It can fill the holes that the traditional firewall may leave. In this type the same cost level can be achieved or maybe less cost than the traditional firewalls. Also implementing the EF can lead to forget about power matter if the selected type is a power over Ethernet one. The robustness side can be obtained just like the traditional firewalls and maybe more. The protection of the network includes both from outside and inside streams of data. So this

kind is perfect for both the management and the administrator. For the employee he is only concerned with doing his job properly and with no restrictions.

To this point this kind appears to be perfect to all categories. But there is a good question here, are all the types of EF provides the same level of cost, power consumption, robustness, and so on? Or the talk was general and each good property can be found in a single kind of EF? Unfortunately, the answer may be near the region of that not all the good properties can be found in one type of the EFs. Here the three categories need to study which of the EFs can possess the majority of these properties and with what property the three of them can sacrifice so that they can get the rest of the properties?

VII. SUMMARY AND CONCLUSION

As per analysis and comparisons carried out in this paper; it may be fairly concluded that a single firewall to protect an entire network is probably not always successful. Arming every machine with an embedded firewall (EF) is possibly a more secure approach to protect a network infrastructure.

This paper was made to show that the firewall implementation is so important because maximum security is much needed nowadays. Since the traditional gateway firewalls has expired in these days with the advance of the security threats that came from inside as well as outside, so the authors introduced the different implementations of Efs, and showed the advantages and disadvantages of each kind of them.

Looking at the three types of firewalls it has been shown that each has its advantages, especially when compared with the traditional gateway firewall which provides no protection from inside attacks, whether designed or not. They also have their own individual drawbacks, to varying degrees. Protection can never be absolute since one is always facing increasing and more ingenious threats. Also, it may be said that threats come from ignorance and lack of ingenuity, not to say stupidity. One such threat comes from the widespread use of media such as flash memory, which can bring disastrous threats to within a network.

REFERENCES

[1] Terry Ogletree. Practical Firewalls. First Edition June 12, 2000.
[2] Lynn M. Meredith. A Summary of the Automatic Distributed Firewalls (ADF) Project, Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03) IEEE 2003.
[3] Tom Markham, Lynn Meredith, and Charlie Payne. Distributed Embedded Firewalls with Virtual Private Groups, Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX'03), IEEE 2003.
[4] Chu-Hsing Lin, Jung-Chun Liu, Chein-Ting Kuo, Mei-Cou, Tsung-Che Yang. Safeguard Intranet Using Embedded and Distributed Firewall System, 2008 Second International Conference on Future Generation Communication and Networking, IEEE 2008.
[5] Quan Huang, Shengke Qiu, Shicun Qin, Cheng Cao. An Embedded Firewall Based on Network Processor, Proceedings of the Second International Conference on Embedded Software and Systems (ICESS'05), IEEE 2005.
[6] Charles Payne, Tom Markham. Architecture and Applications for a Distributed Embedded Firewall, Proceedings of the 17th Annual Computer Security Applications Conference, IEEE 2001.
[7] Vassilis Prevelakis, Angelos Keromytis. Designing an Embedded Firewall/VPN Gateway, Proceedings of the International Network Conference 2002, Plymouth, UK.
[8] Vassilis Prevelakis. The Virtual Firewall, USENIX; login: Magazine, December 2005, Volume 30, Number 6.
[9] Wikipedia, Virtual Machine, http://en.wikipedia.org/wiki/Virtual_machine, Get the Information on Monday, May 18, 2009. 7:49am.

A. **Abd El Baith Mohamed: Professor** at the Arab Academy for Science and Technology, College of Engineering and Technology Computer Engineering Department. IEEE Senior Member. Board member in Computer Scientific Society, Egypt.
baithmm@hotmail.comu

B. **Ahmed Abou Elfarag PhD**. **Assistant professor**. Arab Academy for Science and Technology. College of Engineering. Computer Engineering Department.
abouelfarag@aast.edu

C. **Hassan H. Alkhishali** MSc. candidate at the Arab Academy for Science, Technology and Maritime Transport. College of Engineering, Computer Engineering Department.
hassan.k80@gmail.com