



Advantages of Hardware- Based Security

© 2007 Yoggie Inc. All rights reserved.

Introduction

This document presents the advantages of a hardware-based security appliance over a software based solution.

A hardware-based security appliance is a network-based hardware device designed to perform a single or specialized set of functions. It provides end users with a complete hardware and software solution, including a minimal operating system. The device is a "closed box" system that allows for quick installation, ease-of-use, and low maintenance, and is typically managed through a Web browser.

The hardware-based security appliance can be simply taken out of the box, connected to the network, and turned on. With only a few adaptive configurations made by the end user (mostly local network settings and time zones) ,it is ready to go .The end user can deploy this security solution with a minimum of networking and security knowledge.

Abstract

The main advantages of a hardware-based security solution are:

- Improved security
- Improved performance
- Ease of use
- A hassle-free solution

This document describes the benefits of a hardware-based security appliance and provides example scenarios. The software-based firewall solution has a minimal protection level against more sophisticated network attacks such as IP spoofing attacks, denial of service attacks, or buffer overflow attacks. These attacks can bypass the software-based firewall installed on the computer, and cause serious damage to your information assets. A hardware-based security appliance can be more successful at blocking these kinds of attacks because it is a standalone-hardened device, creating a gap between your computer and the Internet. Even if the attack is successful, your computer will still be safe.

This document also describes and provides examples to the advantages of having applications such as IDS, anti-virus, anti-spam and anti-phishing installed on a security hardware appliance over software based solutions. A hardware-based security solution has advantages in the performance of the computer. While in a software-based solution there are various separate protection layers on our computer (anti-virus , anti-spam, firewall, IDS, etc.). The results the computer's resources are utilized for the protection instead of using them for our basic daily needs. In contrast,

hardware-security appliances are dedicated, specialized hardware devices designed to perform a single task.

Last but not least, the ease of use and the "hassle free" advantage that a hardware security appliance has over software-based appliance is very significant. The hardware security appliance solution is a Plug-n-Play solution. It is designed as a "set-and-forget" device. The appliance can be installed by non-technical staff due to the fact that the OS and application software is preloaded and configured.

Improved Security

Security has become a of paramount importance. We must now think about how to protect our information when we are at home, at the airport, at a hotel, or in school.

Many have learned the hard way that hackers, viruses, spam, and spyware are around every corner. To combat these multiple threats, we need an integrated security solution that combines a variety of applications into one unit. The following description and examples show us why the hardware-based security appliance is the preferable choice for this purpose.

Today, every OS comes with built-in firewall capabilities. In addition we can install a firewall product that promises us complete protection from outside attacks. So is this enough? The answer is "No." All software-based firewall solutions have a minimal level of protection against more sophisticated network attacks like IP spoofing or denial of service attacks.

The following are examples of the attacks that can bypass the software-based firewall that is installed on the computer:

- **IP Spoofing Attacks** – The spoofing of IP addresses; that is, inserting a false IP address into a message to disguise the original location of the message or to impersonate an authorized source.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS)** – The overloading or "hogging" of a system's resources so that it cannot provide the required services. In the distributed mode, requests for service from a particular resource may be launched from large numbers of hosts where software has been planted to become active at a particular time, or upon receiving a particular command.

A denial of service attack can cause your CPU and memory to overload thereby causing your firewall application not to respond. In this way, an attacker can bypass these lines of defense and enter your computer.

A hardware-based security appliance can more effectively block these kinds of attacks because they are isolated from the computer and they operate a hardened OS. These devices effectively, create a gap between your computer and the Internet. Even if they are targeted for some kind of attack, your computer is still safe.

Another example would be a layer-2 network attack. Although a layer-2 attack is less popular on the WAN than in the switched LAN environment, it is a major concern when the computer is connected to a public wireless access point or local campus.

The attacks that result in sniffing include:

- ARP cache poisoning
- CAM table flooding
- Man-in-the-middle attacks, which are normally not blocked by software-based firewall

Man-in-the-middle attacks come in many variations and are easy to operate using freely available tools on the Internet. This attack uses Address Resolution Protocol (ARP) spoofing to sniff traffic between hosts. ARP spoofing is possible because of the exploitation of gratuitous ARP. Gratuitous ARP is when an ARP reply is sent without first receiving an ARP request. ARP cache poisoning works by poisoning the ARP cache of the target hosts. The attacker who wants to sniff the traffic essentially inserts his computer between the target hosts, and forwards traffic back and forth between computers.

A hardware security appliance has the capabilities to block layer-2 attacks with its security mechanisms and network topology. Having an intrusion detection and prevention system on a hardware security appliance that inspects all inbound and outbound network activity, it identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system. This is a major advantage over a host-based IPS installed on the computer. Instead of dealing with the attacks in the OS layer, the appliance drops or monitors the attacks in an external defense layer.

For example, the prevention of a buffer overflow attack, which occurs when a process receives much more data than expected. If the process has no programmed routine to deal with this excessive amount of data, it acts in an unexpected way that the intruder can exploit. Several types of buffer overflow attacks exist, the most common being the "Ping of Death" (large packet ping attack) or user or file names that are longer than 256 characters in e-mails. A large packet ping attack involves the use of the Internet Control Message Protocol (ICMP) ping utility. The intruder sends a "ping" that consists of an illegally-modified and very large IP datagram, thus overfilling the system buffers and causing the system to reboot or hang.

When these kinds of attacks are blocked on the computer, as a software IPS would probably do, it is sometimes too late; some damage has already been done to the computer. A hardware-based security appliance blocks the attack before it reaches the destination.

In the matter of virus protection, some users may think that if there is an anti-virus program installed on the computer, it will protect against all viruses, spyware, and malware. However, there is always a chance that a virus or Trojan would reach your computer by bypassing the antivirus protection. The virus can bypass the anti-virus software in many ways, such as the anti-virus software not being updated with the latest signatures, or the end-user disabling the virus protection on purpose or by mistake. With a dedicated security hardware appliance that examines network traffic and checks for viruses, Trojans or any malware before it reaches your computer, your security is greater: virus protection is always on, all malware is examined and stopped by an external device, and no matter what happens, your computer is safe.

Spam and phishing attacks are one of the more popular attacks we are facing today. Having a device that filters your messages before they reach your mailbox is a better solution. The hardware-based security appliance has anti-spam and anti-phishing mechanisms that are constantly updated from external repositories. They are therefore very accurate and have less false negatives (i.e., fewer legitimate messages being filtered).

Improved **Security**

Comparing the Hardware Appliances

From these and many other examples, we can see how hardware-based security solutions improves the protect your data from outside threats.

Improved Performance

Computer performance and resource management are of major significance. In order to deal with all of the security threats today, we are constantly installing more and more separate protection layers on our computer (anti-virus, anti-spam, firewall, IDS, and more). In addition, from time to time we hear about a new threat and run to install the protection mechanism for the specific threat.

In this way, all our resources are utilized by the protection layers installed in our computer, instead of using these expensive resources for our basic daily needs. No one guarantees that all these separate security protection layers, which usually come from different vendors, will work smoothly together and not cause collisions and memory leaks that result in system failures or service outages.

Every vendor develops its own drives and software, and although there is a standard for developing applications, not everyone works exactly according to these standards or RFCs, creating system failures. Due to this complexity, the system has poor reliability and frequent service outages. The software-based security solutions are installed on hardware and operating systems that were not designed specifically for this task. On the other hand, a hardware security appliance solution is a "closed box" that doesn't require any third-party application in order to function. All applications are built-in, and have passed Quality Assurance testing procedures and certifications. The hardware appliance is a very reliable and stable solution. It reduces downtime for critical assets in the organization, and provides improved SLA.

Comparing the Hardware Appliances

Hardware security appliances are dedicated, specialized, hardware devices that are designed to perform a single task. Performance of the appliance-based solution is generally better than software-based solutions, because the appliances are designed for a specific purpose.

Server appliance software is configured to work well with the hardware provided; because it comes from the same vendor. Another important reason is that hardware security appliances are often checked and benchmarked by the vendors in order to exhibit the best performance in different network environments. If there is a major change or more security features are added, the hardware is changed accordingly.

All these facts show that hardware-based security solution is much more stable, reliable, and promises better performance than software-based solution. For this reason, it can provide a better protection for the end user.

Ease of Use

The hardware security appliance solution is a Plug-n-Play solution. It is designed as a "set-and-forget" device. The appliance can be installed by non-technical staff due to the fact that the OS and application software is preloaded and configured.

In most cases, the hardware security appliance is "network ready," which means that there is no need to install network interfaces or drivers. There is also no need to harden the appliance or to install security patches in order to secure it. All of the self-protecting mechanisms are predefined and are updated automatically by the appliance vendor.

In the case of the software-based solution, it is quite the opposite: most of the software security solutions require advanced IT skills for all installation and pre-installation procedures. It requires a good understanding of hardware and software, and the interoperability between these two elements .

Computer security protection can be a very complex and difficult issue to configure, manage and monitor. When there are several different application that you need to manage and configure separately, the work becomes even more complex.

The hardware security appliance has one focal point (most of the time a Web portal interface) that you can manage, configure, and monitor all security considerations.

Ongoing Maintenance is a Major Concern for an End User

The hardware security appliance solution requires low maintenance. All maintenance procedures are built-in and are self-proceeding. They have auto-update system mechanisms for daily security and system updates. In addition, the fact that there is single vendor to deal with, gives the end user confidence and assurance.

Last but not least is the licensing issue. Software-based security solution licensing parameters are often very complex, and usually differ from one vendor to another. When facing the licensing Issue, there is a need to calculate the OS licensing and each of the software applications combining the solution. This separate licensing methodology must often be monitored which overloads the attention of the finance and IT departments.

On the other hand, a hardware security appliance solution require one license for all functionality that the solution brings, with no cross licensing issues or burdens. Generally, there is one "fixed license" for the product, and the workstations pay no licensing fees for VPN, anti-virus, and anti-spam services. There is one focal point, not only for the technical issues, but also for the licensing and payment parameters.