Greenbone Appliances

Differences Between Physical and Virtual Appliances

Tech Paper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

15.08.2019

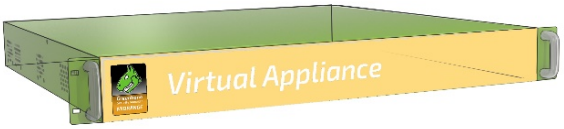
Contents

1. Introduction

There are two types of appliances in the Greenbone Networks product portfolio.

On the one hand, the physical appliances consisting of special server hardware, the Greenbone Operating System (Greenbone OS), the scan application and the subscription to the professional Greenbone Security Feed.

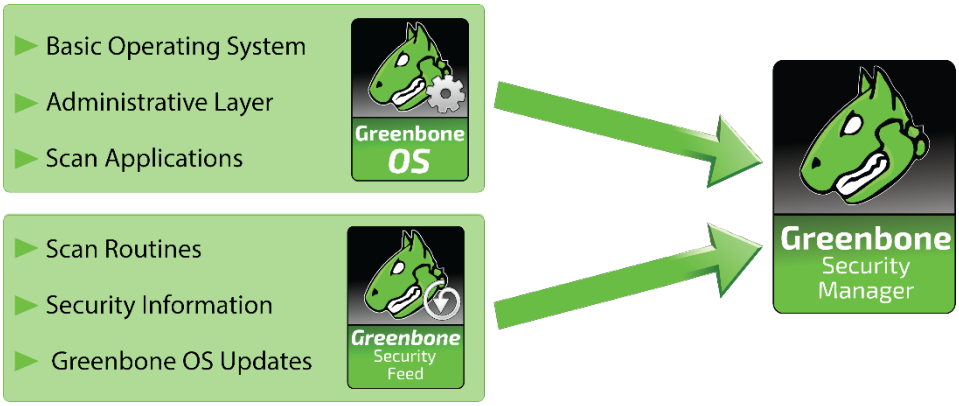
On the other hand, the virtual appliances whose main components are the Greenbone OS, the scan application and the subscription. As usual for virtual machines, the actual hardware is replaced by a definition of resources to be virtualized (CPU, RAM, HD, etc.).



Due to their physical nature, the physical appliances are subject to a generation change, which leads to an end-of-life of the hardware approximately every 5 - 7 years. Within the scope of an ongoing subscription, there are various options to change to a newer model or even the virtual line. Please talk to our sales team (sales@greenbone.net) about this.

This Tech Paper explains the essential and potentially critical aspects of an installation for each type of appliance. It is intended to assist in selecting the appropriate model. If necessary, technical backgrounds will be discussed. Basic concepts, features and common terms of virtualization are assumed to be known.

For the further explanations it is necessary to show the solution architecture of the Greenbone Security Manager (GSM). The figure explains the individual components and their relationship to each other.



See also: https://www.greenbone.net/en/product-architecture/

For the physical appliances, the entire solution is delivered turnkey on the appliance hardware, with hardware specifications defined by Greenbone Networks (manufactured to order, not standard systems like from major hardware manufacturers). For virtual appliances, the solution consists of the Greenbone OS contained in a virtualized machine and the application itself. The actual hardware specifications are defined and determined in the format Open Virtualization Archive (OVA) which is understandable for virtualization environments.

Technically, the difference between the two variants is not only the virtualization of the hardware base but also includes hardware features of the appliance that support certain functions such as hardware encryption and TCP acceleration and are not virtually available.

This results in a number of aspects that influence a decision for or against a variant. The following five topics look at these aspects in detail.

2.Costs

Virtualization is often associated with the reduction of operating costs. Rackspace, power and air conditioning are the most important factors. The actual costs of the solution, often seen as license costs, are usually comparable whether as a physical turnkey appliance or as a system solution in a virtualization environment. Since Greenbone Networks uses a licensing model based on capacities, there are no differences here. Each model in our product portfolio has a defined capacity, a corresponding solution license and a defined specification of the hardware environment (physical and virtual).

3.Performance

Since the Greenbone Networks licensing model is based on the capacity, i.e. on the performance of an appliance or more precisely on the number of assets/IP addresses that can be scanned in 24 hours, performance is not a decisive factor. It should be noted that the hardware specifications of the virtual appliances must not be changed for licensing reasons.

Because the virtual appliances have no impact on the hypervisor network, certain framework conditions of the scan may affect the performance and functionality of a virtualization environment.

While the firewall rule and Network Address Translation (NAT) for the hardware appliance are rather unproblematic, NAT in particular can have an influence on the performance of the virtualization environment and lead to DoS-like (Denial of Service) situations. Here, special attention must be paid to the scope of the scan targets.

The efficient use of resources such as CPU and RAM as an essential advantage of virtualization is nevertheless maintained.

4.Security

When it comes to comparing a physical appliance with a virtual one, many facets of IT security have already been highlighted in relation to the security of an installation.

Backup & Disaster Recovery are simplified and centrally controllable within a virtualization environment, meanwhile individual measures are required for a physical appliance.

Security concepts of a hardware-based turnkey appliance such as complete encryption or the protection of cryptographic material (storage and handling of keys) ensure that scan information, i.e. found vulnerabilities, are also encrypted at the hardware level. This security is not provided in a virtualized environment because the hardware encryption cannot be virtualized securely and it cannot be ruled out that key material and vulnerability data from the virtual appliance could be read by other virtual instances.

Greenbone's *Clean Source approach* applies to both variants of the GSM. The transparency or rather auditability of the virtualization environment must be evaluated differently, since hidden functionalities in the virtualization server, whether intended or not, cannot be excluded due to a lack of clean source.

Hardware Vulnerabilities (Spectre/Meltdown) are mitigated by Greenbone's appliance design. For the virtualization server used, the user must take the necessary measures himself.

The *User Management* of virtualization environments may allow intervention in the virtual GSM appliance under certain circumstances. For hardware-based appliances this is excluded by design and RBAC (Role Based Access Control).

5. Functionality & Features

Features and functionality that use specific hardware properties create differences between physical and virtual appliances.

VLANs can be supported with hardware tagging on the interface cards of a hardware appliance, unlike virtualized environments where this must be done independently of the GSM.

AirGap can only be mapped to a very limited extent with virtualized appliances. The LCD functions are not available and the FTP variant is only possible to a limited extent. This is particularly important in deployment scenarios in which highly secure network areas separated from the public Internet are to be scanned.

6. Installation, Maintanance & Support

Both variants have the typical advantages and disadvantages of the installation of a system. The evaluation of those has to be carried out situation-related.

Feed, updates and upgrades are available for both the physical and the virtual appliances and the type of maintenance by Greenbone Networks is identical for both variants.

Full support can only be provided for the hardware versions including free replacement of defective hardware. Greenbone Networks cannot provide support for the respective virtualization environment for the virtual appliances. Here the responsibility lies with the user.

7. Résumé

The purpose of this Tech Paper is to highlight the differences between physical and virtual appliances and help you choose the right type of appliance. Depending on the deployment environment and existing infrastructure, Greenbone's physical and virtual appliances can be used equally. Physical appliances are more secure, while virtual appliances are more resource-efficient.

8. Further Sources

ENISA, European Union Agency for Cybersecurity: Security aspects of virtualization:
https://www.enisa.europa.eu/publications/security-aspects-of-virtualization

RIT Scholar Works, NAT Denial of Service:
https://scholarworks.rit.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=1756&context=other

Greenbone Networks: Configuring AirGap:
https://docs.greenbone.net/GSM-Manual/gos-4/en/systemadministration.html#configuring-the-gsm-as-an-airgap-master-slave