



Greenbone Professional Edition

*The Differences Between Physical
and Virtual Appliances*

WhitePaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net



Greenbone
Sustainable Resilience



Contents

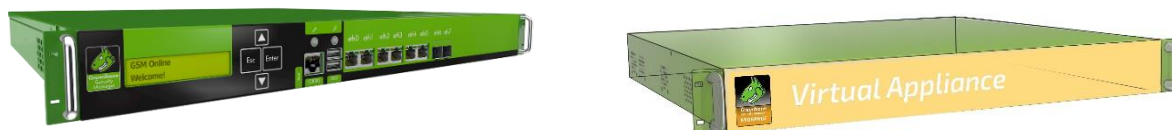
1 Introduction	3
2 Comparison of Aspects	4
2.1 Costs	4
2.2 Performance	4
2.3 Security	4
2.4 Functionality & Features	5
2.5 Installation, Maintenance & Support	5
3 Conclusion	5
4 Further Sources	5



1 Introduction

In the product portfolio of Greenbone Networks, there are two types of appliances of the Greenbone Professional Edition (GPE).

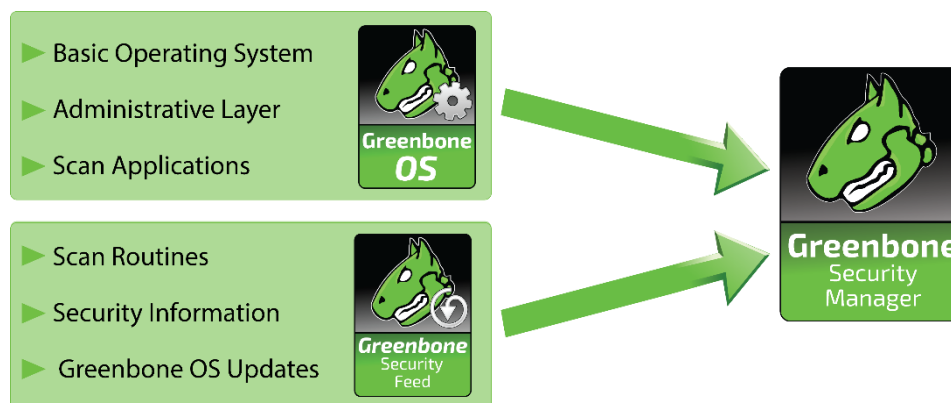
On the one hand, the physical appliances consisting of a special server hardware, the Greenbone Operating System (GOS), the scan application and the subscription to the professional Greenbone Security Feed. On the other hand, the virtual appliances with GOS, the scan application and the subscription as main components. 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 hardware-based appliances are subject to a generation change leading 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 to the virtual line. Please feel free to ask our sales team (sales@greenbone.net) about it.

This WhitePaper 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 following explanations it is necessary to show the architecture of the Greenbone Security Manager (GSM). The figure shows the individual components and their relationship to each other. More information can be found [here](#).



For the physical appliances, the entire solution is delivered as a turnkey solution on a hardware with specifications defined by Greenbone Networks. The hardware is produced on order.

For the virtual appliances, the solution consists of GOS contained in a virtualized machine and the application itself. The actual hardware specifications are defined and determined in a format that is understandable for virtualization environments (e.g., OVA format).



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 virtually not realizable.

This results in several aspects that influence a decision for or against one variant. The following chapter looks at these aspects in detail.

2 Comparison of Aspects

2.1 Costs

Virtualization is often associated with a 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).

2.2 Performance

Since the Greenbone Networks licensing model is based on the capacity, i.e., 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 rules 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 scan targets.

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

2.3 Security

Backup & Disaster Recovery are simplified and centrally manageable within a virtualization environment, while a physical appliance requires individual measures.

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

Greenbone Networks' *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 Networks' appliance design. For the virtualization server used, the users must take the necessary measures themselves.

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

2.4 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 network 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 Airgap FTP variant is only possible to a certain degree. This is particularly important in deployment scenarios in which highly secure network areas separated from the public Internet should be scanned.

2.5 Installation, Maintenance & Support

Both variants have the typical advantages and disadvantages of the installation of a system. The evaluation of each must be done 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 version, including free replacement of defective hardware. Greenbone Networks cannot provide support for the respective virtualization environment of a virtual appliances. Here the responsibility lies with the user.

3 Conclusion

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

4 Further Sources

- [ENISA, European Union Agency for Cybersecurity: Security aspects of virtualization](#)
- [RIT Scholar Works, NAT Denial of Service](#)