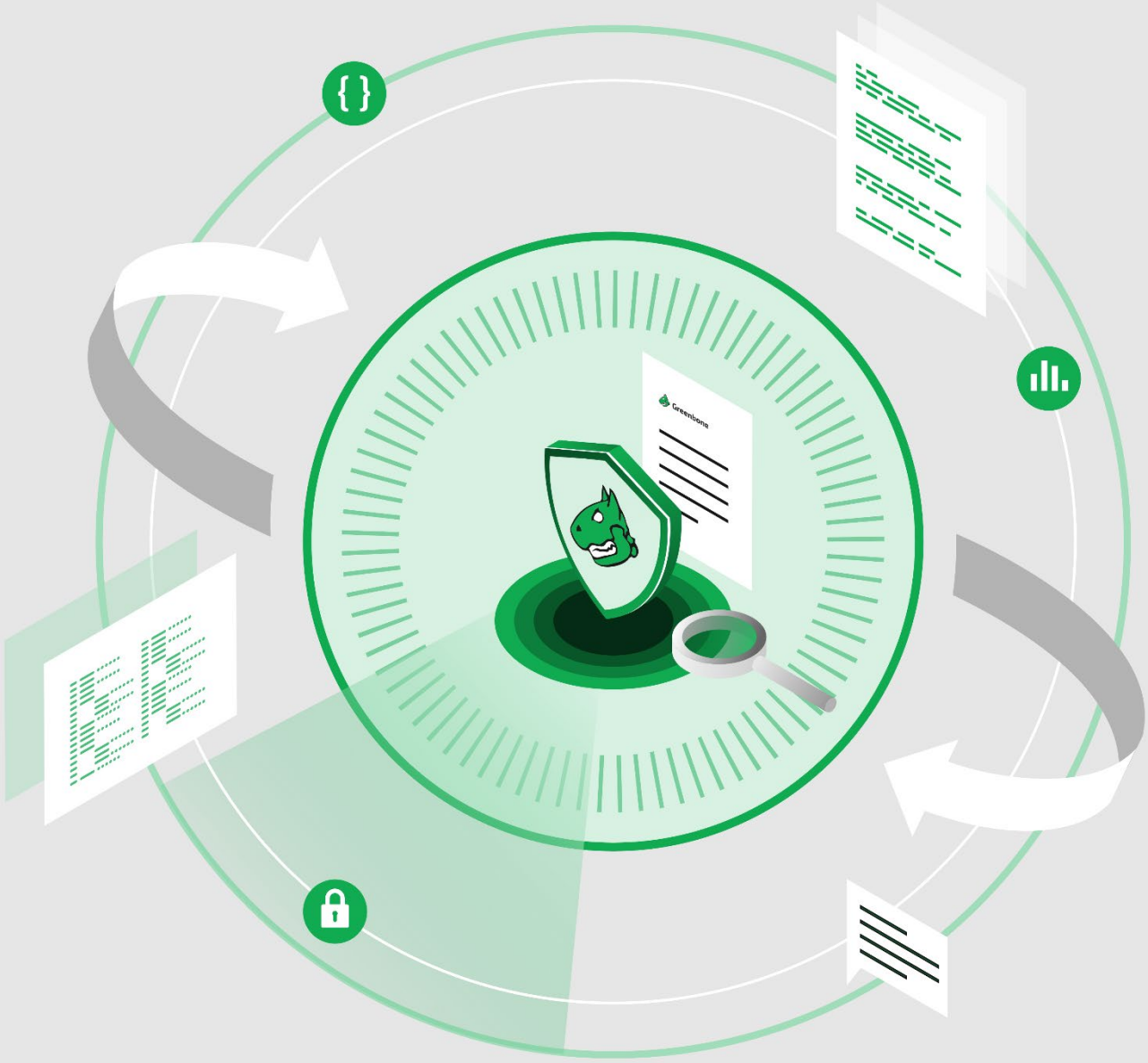
Greenbone

Greenbone Enterprise Appliances

The Differences Between Hardware and Virtual Appliances



Date: 2022-09-15

Contents

1 Introduction

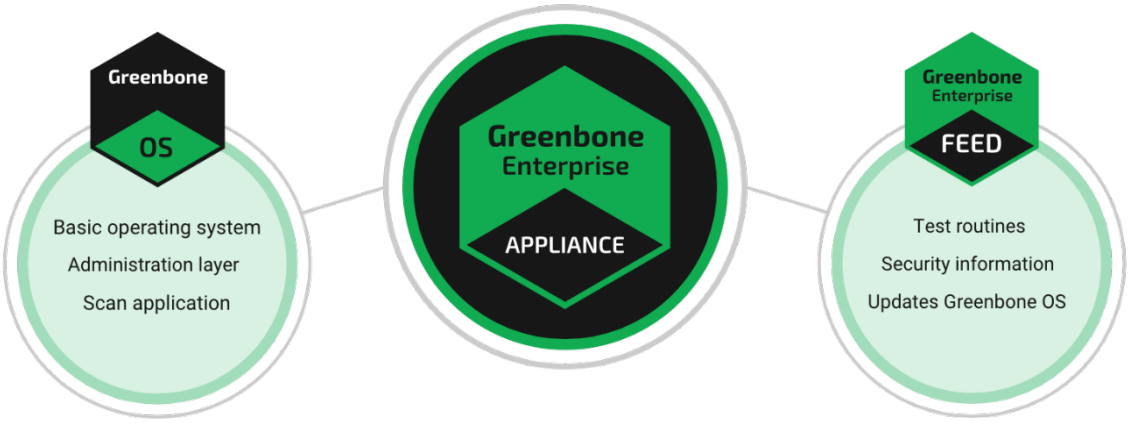
In the product portfolio of Greenbone, there are two types of Greenbone Enterprise Appliances.

On the one hand, the hardware appliances consisting of a special server hardware, the Greenbone Operating System, the scan application and the subscription to the professional Greenbone Enterprise Feed. On the other hand, the virtual appliances with the Greenbone Operating System, 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 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 document explains the essential and potentially critical aspects of an installation for each type of appliance. It is intended to assist in selecting the appropriate type. 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 Enterprise Appliances. The figure shows the individual components and their relationships to each other.



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

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

Neumarkt 12 • 49074 Osnabrück • Germany • www.greenbone.net/en/

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 turnkey hardware appliance or as a solution in a virtualization environment.

Since Greenbone 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 licensing model is based on the scan capacity of an appliance – number of assets/IP addresses that can be scanned in 24 hours –, performance is not a decisive factor. For licensing reasons, the hardware specifications of the virtual appliances must not be changed.

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.

Nevertheless, the efficient use of resources such as CPU and RAM as an essential advantage of virtualization is maintained.

2.3 Security

Backup & Disaster Recovery are simplified and centrally manageable within a virtualization environment, while a hardware 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., found vulnerabilities, 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's clean-source approach applies to both variants of the appliances. 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 users must take the necessary measures themselves.

The user management of virtualization environments may allow intervention in the virtual 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 hardware and virtual appliances.

VLANs can be supported with hardware tagging on the network interface cards of a hardware appliance. In contrast, on virtualized environments, this must be done independently of the appliance.

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 high-security 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 hardware and the virtual appliances and the type of maintenance by Greenbone is identical for both variants.

Full support including free replacement of defective hardware can only be provided for the hardware version. Greenbone 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 document is to highlight the differences between hardware and virtual appliances and help to choose the right appliance type. Depending on the deployment environment and existing infrastructure, Greenbone's hardware and virtual appliances can be used equally. Hardware 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