Greenbone Appliances

Unterschiede zwischen physischen und virtuellen Appliances

Tech Paper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

26.07.2019

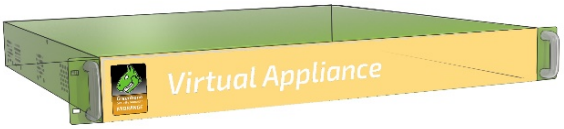
Inhaltsverzeichnis

1. Einführung

Im Produktportfolio von Greenbone Networks gibt es zwei Arten von Appliances.

Zum einen die physischen Appliances, bestehend aus spezieller Server-Hardware, dem Greenbone Operating System (Greenbone OS), der Scan-Applikation und der Subskription zum professionellen Greenbone Security Feed.

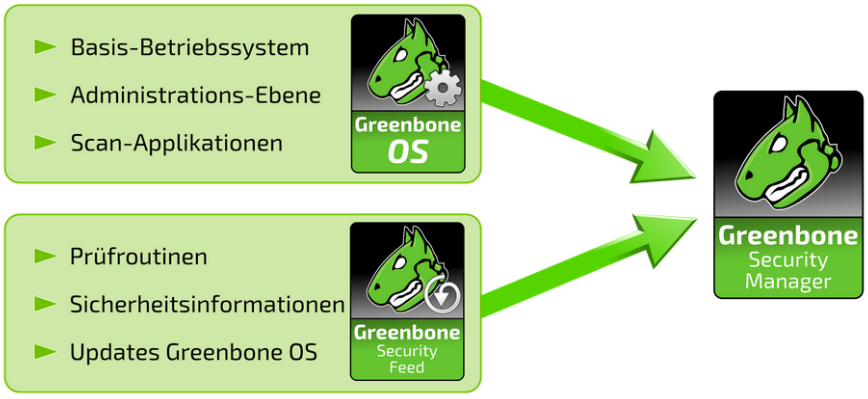
Zum anderen die virtuellen Appliances, deren Hauptkomponenten das Greenbone OS, die Scan-Applikation und die Subskription sind. Wie bei virtuellen Maschinen üblich, wird die eigentliche Hardware durch eine Definition an zu virtualisierenden Ressourcen (CPU, RAM, HD usw.) ersetzt.



Die physischen Appliances unterliegen aufgrund ihrer körperlichen Beschaffenheit einem Generationswechsel, der ca. alle 5 - 7 Jahre zu einem End-of-Life der Hardware führt. Im Rahmen einer laufenden Subskription gibt es verschiedene Varianten auf ein neueres Modell oder gar die virtuelle Linie zu wechseln. Hierfür sprechen Sie bitte mit unserem Sales-Team (sales@greenbone.net).

Dieses Tech Paper erläutert die wesentlichen und für eine Installation potentiell kritischen Aspekte der jeweiligen Art von Appliance. Es soll als Hilfestellung bei der Wahl der passenden Variante dienen. Soweit notwendig, wird auf technische Hintergründe eingegangen. Grundlegende Konzepte, Merkmale und übliche Begriffe der Virtualisierung werden als bekannt angenommen.

Für die weiteren Ausführung ist es nötig, die Lösungarchitektur des Greenbone Security Managers (GSM) aufzuzeigen. Das Bild erläutert die einzelnen Komponenten und ihre Beziehung zueinander.



Siehe auch: https://www.greenbone.net/produkt-architektur/

Bei den physischen Maschinen wird die gesamte Lösung schlüsselfertig auf einer Appliance-Hardware geliefert, wobei die Hardware-Spezifikationen von Greenbone Networks festgelegt wurden (Auftragsfertigung, keine Standardsysteme von großen Hardware-Herstellern). Bei den virtuellen Appliances besteht die Lösung aus dem in einer virtualisierten Maschine enthaltenen Greenbone OS und der Applikation selbst. Die eigentlichen Hardware-Spezifikationen werden in einem für Virtualisierungsumgebungen verständlichen Format definiert und festgelegt (OVA).

Technisch gesehen ist der Unterschied zwischen beiden Varianten nicht nur die Virtualisierung der Hardwarebasis, sondern umfasst auch Hardwareeigenschaften der Appliance die bestimmte

Funktionen wie Hardware-Verschlüsslung und TCP-Beschleunigung unterstützen und virtuell nicht zur Verfügung stehen.

Daraus ergibt sich eine Reihe von Aspekten, die eine Entscheidung für oder gegen eine Variante beeinflussen. Die folgenden fünf Themen betrachten diese Aspekte im Detail.

2. Kosten

Eine Virtualisierung wird häufig mit der Reduktion von Betriebskosten in Verbindung gebracht. Rackspace, Strom und Klimatisierung sind dabei die wesentlichen Faktoren. Die eigentlichen Kosten der Lösung, auch oft als Lizenzkosten gesehen, sind dabei meist vergleichbar, egal ob als physische Turnkey-Appliance oder als Systemlösung in einer Virtualisierungsumgebung. Da Greenbone Networks ein Lizenzmodell auf Basis von Kapazitäten verwendet, ergeben sich hier keine Unterschiede. Jedes Modell unseres Produktportfolios hat eine definierte Kapazität, eine damit einhergehende Lösungs-Lizenz und definierte Spezifikation der Hardwareumgebung (physisch wie virtuell).

3. Leistung

Da das Lizenzmodell von Greenbone Networks auf der Kapazität, also der Performance einer Appliance basiert, genauer gesagt auf der Anzahl an Assets/IP-Adressen die in 24 Stunden gescannt werden können, ist die Leistungsfähigkeit kein entscheidender Faktor. Zu beachten ist, dass die Hardware-Spezifikationen der virtuellen Appliances lizenzrechtlich nicht verändert werden dürfen.

Da die virtuellen Appliances keine Auswirkung auf das Hypervisor-Netz haben, kann es vorkommen, dass gewisse Rahmenbedinungen des Scans die Leistung und Funktionalität einer Virtualisierungsumgebung beeinflussen.

Während Firewall-Regel und Network Address Translation (NAT) für die Hardware-Appliance eher unproblematisch sind, kann insbesondere NAT einen Einfluss auf die Leistung der Virtualisierungsumgebung haben und dort zu DoS-ähnlichen (Denial of Service) Situationen führen. Hier ist speziell auf die Umfänge der Scan-Ziele zu achten.

Die effiziente Ausnutzung von Ressourcen wie CPU und RAM als ein wesentlicher Vorteil der Virtualisierung bleibt dennoch erhalten.

4. Sicherheit

Wenn es um den Vergleich zwischen einer physischen und einer virtuellen Appliance geht, wurden in Bezug auf die Sicherheit einer Installation schon viele Facetten der IT-Sicherheit beleuchtet.

Backup & Disaster Recovery sind innerhalb einer Virtualisierungsumgebung vereinfacht und zentral steuerbar, für eine physikalische Appliance sind hier individuelle Maßnahmen erforderlich.

Sicherheitskonzepte einer hardwarebasierten Turnkey-Appliance wie z. B. die Komplettverschlüsselung oder der Schutz von kryptographischem Material (Aufbewahrung und Handhabung von Keys) sorgen dafür, dass Scan-Informationen, also gefundene Schwachstellen, auch auf der Hardware-Ebene verschlüsselt sind. In einer virtualisierten Umgebung ist diese Absicherung nicht gegeben, da die Hardware-Verschlüsselung nicht sicher virtualisiert werden kann und es nicht auszuschliessen ist, dass Key-Material durch andere virtuelle Instanzen und auch Schwachstellen-Daten aus der virtuellen Appliance ausgelesen werden könnten.

Greenbones *Clean Source Ansatz* gilt für beide Varianten des GSMs. Die Transparenz bzw. Auditierbarkeit der Virtualisierungsumgebung ist anders zu bewerten, da versteckte Funktionalitäten im Virtualisierungsserver, seien sie beabsichtigt oder auch nicht, mangels Clean Source nicht ausgeschlossen werden können.

Hardware-Schwachstellen (Spectre/Meltdown) werden bei Greenbone durch das Appliance-Design mitigiert. Für den genutzten Virtualisierungsserver muss der Anwender selbst die notwendigen Maßnahmen treffen.

Das *User Management* von Virtualisierungsumgebungen erlaubt unter Umständen den Eingriff in die virtuelle GSM-Appliance, bei hardwarebasierenden Appliances ist dies durch Design und RBAC (Role Based Access Control) ausgeschlossen.

5. Funktionalität & Features

Features und Funktionalitäten, die bestimmte Hardware-Eigenschaften verwenden, sorgen für Unterschiede zwischen physischen und virtuellen Appliances.

VLANs können mit Hardware-Tagging auf den Interface-Karten einer Hardware-Appliance unterstützt werden, anders als in virtualisierten Umgebungen, in denen dies unabhängig vom GSM gelöst werden muss.

AirGap lässt sich nur sehr eingeschränkt mit virtualisierten Appliances abbilden. Die LCD-Funktionen stehen nicht zur Verfügung und die Variante über FTP ist nur bedingt möglich. Dies ist besonders bei Einsatzszenarien zu beachten, in denen hochsichere, vom öffentlichen Internet abgetrennte Netzbereiche gescannt werden sollen.

6. Installation, Instandhaltung & Support

Beide Varianten haben die jeweils typischen Vor- und Nachteile bei der Installation eines Systems, deren Bewertung situationsbezogen erfolgen muss.

Feed, Updates und Upgrades sind sowohl für die physischen als auch für die virtuellen Appliances verfügbar und die Art der Wartung durch Greenbone Networks ist für beide Varianten identisch.

Vollumfänglicher Support kann nur für die Hardware-Variante geleistet werden, inkl. des kostenlosen Austauschs bei defekter Hardware. Für die virtuellen Appliances kann Greenbone Networks keine Unterstützung für die jeweilige Virtualisierungsumgebung leisten. Hier liegt die Verantwortung beim Anwender.

7. Zusammenfassung

Ziel dieses Tech Papers ist es, die Unterschiede physische und virtueller Appliances zu beleuchten und eine Hilfestellung bei der Auswahl der geeigneten Appliancesart zu sein.
Je nach Einsatzumfeld und vorhandener Infrastruktur, können Greenbones physische und virtuelle Appliances gleichwertig eingesetzt werden. Für die physischen Appliances sprechen höhere Sicherheitsaspekte, für die virtuellen Appliances ist die Ressourceneffizienz ein Argument.

8. Weitere Quellen

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