Greenbone Professional Edition

Die Unterschiede zwischen physischen und virtuellen Appliances

WhitePaper

Greenbone Networks GmbH
Neumarkt 12
49074 Osnabrück

www.greenbone.net

Greenbone
Sustainable Resilience

2020-10-29

Inhalt

1 Einleitung

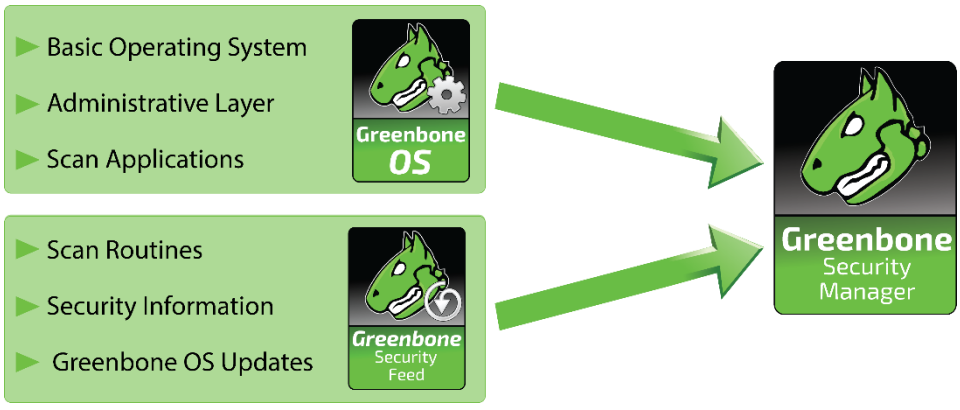
Im Produktportfolio von Greenbone Networks gibt es zwei Arten von Appliances der Greenbone Professional Edition (GPE).

Zum einen die physischen Appliances, bestehend aus einer speziellen Server-Hardware, dem Greenbone Operating System (GOS), der Scan-Anwendung und der Subskription des professionellen Greenbone Security Feeds. Auf der anderen Seite die virtuellen Appliances mit GOS, der Scan-Anwendung und der Subskription als Hauptkomponenten. Wie bei virtuellen Maschinen üblich, wird die eigentliche Hardware durch eine Definition der zu virtualisierenden Ressourcen (CPU, RAM, HD usw.) ersetzt.

Aufgrund ihrer physischen Beschaffenheit unterliegen die hardwarebasierten Geräte einem Generationswechsel, der etwa alle 5 – 7 Jahre zu einem Auslaufen der Hardware führt. Im Rahmen einer laufenden Subskription gibt es verschiedene Möglichkeiten, auf ein neueres Modell oder sogar auf die virtuelle Linie zu wechseln. Kontaktieren Sie dazu bitte einfach unser Sales-Team (sales@greenbone.net).

Dieses WhitePaper erläutert die wesentlichen und potenziell kritischen Aspekte einer Installation für jeden Appliancetyp und soll bei der Auswahl des geeigneten Modells helfen. Falls erforderlich, werden technische Hintergründe erläutert. Grundlegende Konzepte, Funktionen und allgemeine Begriffe der Virtualisierung werden als bekannt vorausgesetzt.

Für die folgenden Ausführungen ist es notwendig, die Architektur des Greenbone Security Managers (GSM) zu zeigen. Die Abbildung zeigt die einzelnen Komponenten und ihre Beziehung zueinander. Weitere Informationen sind hier zu finden.



Für die physischen Appliances wird die gesamte Lösung als schlüsselfertige Lösung auf einer Hardware mit von Greenbone Networks definierten Spezifikationen geliefert. Die Hardware wird auf Bestellung produziert.

Für die virtuellen Appliances besteht die Lösung aus GOS, das in einer virtuellen Maschine enthalten ist und der Anwendung selbst. Die eigentlichen Hardwarespezifikationen werden in einem für Virtualisierungsumgebungen verständlichen Format (z. B. OVA-Format) definiert und festgelegt.

Technisch gesehen besteht der Unterschied zwischen den beiden Varianten nicht nur in der Virtualisierung der Hardware-Basis, sondern umfasst auch Hardware-Features der Appliance, die bestimmte Funktionen wie Hardware-Verschlüsselung und TCP-Beschleunigung unterstützen und virtuell nicht umsetzbar sind.

Daraus ergeben sich mehrere Aspekte, die eine Entscheidung für oder gegeneine Variante beeinflussen. Das folgende Kapitel behandelt diese Aspekte im Detail.

2 Vergleich der Aspekte

2.1 Kosten

Virtualisierung wird oft mit einer Senkung der Betriebskosten in Verbindung gebracht. Rackspace, Strom und Klimatisierung sind die wichtigsten Faktoren. Die tatsächlichen Kosten der Lösung, die oft als Lizenzkosten angesehen werden, sind in der Regel vergleichbar, ob als physische, schlüsselfertige Appliance oder als Systemlösung in einer Virtualisierungsumgebung.

Da Greenbone Networks ein Lizenzmodell verwendet, das auf Kapazitäten basiert, gibt es hier keine Unterschiede. Jedes Modell in unserem Produktportfolio hat eine festgelegte Kapazität, eine entsprechende Lösungslizenz und eine definierte Spezifikation der Hardware-Umgebung (physisch und virtuell).

2.2 Leistung

Da das Lizenzmodell von Greenbone Networks auf der Kapazität, d. h. der Leistung eines Geräts, genauer gesagt auf der Anzahl der Assets/IP-Adressen basiert, die innerhalb von 24 Stunden gescannt werden können, ist die Leistung kein entscheidender Faktor. Es ist zu beachten, dass die Hardwarespezifikationen der virtuellen Appliances aus lizenzrechtlichen Gründen nicht geändert werden dürfen.

Da die virtuellen Appliances keine Auswirkungen auf das Hypervisor-Netzwerk haben, können bestimmte Rahmenbedingungen des Scans die Leistung und Funktionalität einer Virtualisierungsumgebung beeinträchtigen.

Während die Firewall-Regeln und Network Address Translation (NAT) für die Hardware-Appliances eher unproblematisch sind, kann insbesondere NAT Einfluss auf die Performance der Virtualisierungsumgebung nehmen und zu DoS-ähnlichen (Denial of Service) Situationen führen. Hier muss besonders auf den Umfang der Scan-Ziele geachtet werden.

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

2.3 Sicherheit

Backup & Disaster Recovery sind innerhalb einer Virtualisierungsumgebung vereinfacht und zentral verwaltbar, während eine physische Appliance individuelle Maßnahmen erfordert.

Sicherheitskonzepte einer hardwarebasierten Appliance wie die vollständige Verschlüsselung oder der Schutz von kryptografischem Material (Speicherung und Handling von Keys) stellen sicher, dass Scan-Informationen, d. h. gefundene Schwachstellen, auch auf der Hardwareebene verschlüsselt werden. In einer virtuellen Umgebung gibt es diesen Schutz nicht, da die Hardware-Verschlüsselung nicht sicher virtualisiert werden kann und damit nicht ausgeschlossen werden kann, dass Schlüsselmaterial und auch Schwachstellendaten aus der virtuellen Appliance gelesen werden können.

Der *Clean-Source-Ansatz* von Greenbone Networks gilt für beide Varianten des GSM. Die Transparenz bzw. Überprüfbarkeit der Virtualisierungsumgebung muss unterschiedlich bewertet werden, da versteckte Funktionalitäten im Virtualisierungsserver, ob beabsichtigt oder nicht, mangels Clean Source nicht ausgeschlossen werden können.

Hardware-Schwachstellen (Spectre/Meltdown) werden durch Greenbone Networks‘ Appliance-Design abgeschwächt. Für den eingesetzten Virtualisierungsserver müssen die Nutzer die notwendigen Maßnahmen selbst ergreifen.

Die *Benutzerverwaltung* von Virtualisierungsumgebungen kann unter bestimmten Umständen einen Eingriff in die virtuelle GSM-Appliance ermöglichen. Bei hardwarebasierten Appliances ist dies durch das Design und die rollenbasierte Zugriffskontrolle Role Based Access Control (RBAC) ausgeschlossen.

2.4 Funktionalität & Features

Features und Funktionen, die bestimmte Hardwareeigenschaften nutzen, führen zu Unterschieden zwischen physischen und virtuellen Appliances.

VLANs können durch Hardware-Tagging auf den Netzwerkkarten einer Hardware-Appliance unterstützt werden, im Gegensatz zu virtualisierten Umgebungen, wo dies unabhängig vom GSM erfolgen muss.

Airgap lässt sich mit virtualisierten Appliances nur sehr eingeschränkt abbilden. Die LCD-Funktionen stehen nicht zur Verfügung und die Airgap-FTP-Variante ist nur bis zu einem gewissen Grad möglich. Dies ist besonders in Einsatzszenarien wichtig, in denen hochsichere, vom öffentlichen Internet getrennte Netzwerkbereiche gescannt werden sollen.

2.5 Installation, Wartung & Support

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

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

Voller Support kann nur für die Hardware-Version gewährt werden, einschließlich des kostenlosen Austauschs defekter Hardware. Greenbone Networks kann keinen Support für die jeweilige Virtualisierungsumgebung einer virtuelle Appliance anbieten. Hier liegt die Verantwortung beim Nutzer.

3 Schlussfolgerung

Zweck dieses WhitePapers ist es, die Unterschiede zwischen physischen und virtuellen Appliances aufzuzeigen und bei der Auswahl des richtigen Appliance-Typs zu helfen. Abhängig von der Einsatzumgebung und der bestehenden Infrastruktur können die physischen und die virtuellen Appliances von Greenbone Networks gleichermaßen eingesetzt werden.

Physische Appliances sind sicherer, während virtuelle Appliances ressourceneffizienter sind.

4 Weitere Quellen

- ENISA, European Union Agency for Cybersecurity: Security aspects of virtualization
- RIT Scholar Works, NAT Denial of Service