ComConsult Research

Der Netzwerk Insider

Mai 2009

Systematische Weiterbildung für Netzwerk- und IT-Professionals

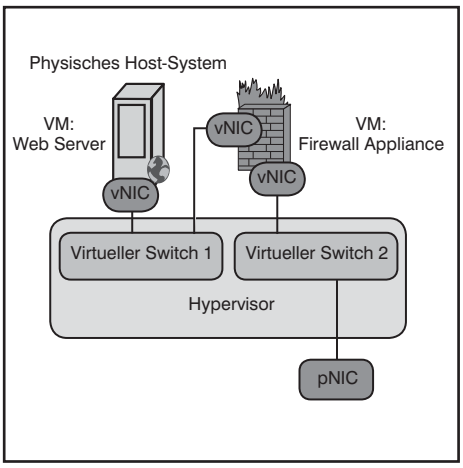
Schwerpunktthema

Virtualisierung:

Mehr Sicherheit durch virtuelle Firewalls?

von Dipl.-Inform. Matthias Egerland, Dipl.-Ing. Björn Korall, Dipl.-Inform. Daniel Meinhold

Nachdem die Server-Virtualisierung in die meisten Rechenzentren Einzug gehalten hat, ist nun die Virtualisierung weiterer Infrastruktur-Komponenten die logische Konsequenz. Wird dieser Ansatz zielgerichtet zu Ende gedacht, gipfelt er in Konzepten wie „Office-in-a-Box“ bzw. „Datacenter-in-a-Box“. Ein besonderes Augenmerk ist bei der Virtualisierung weiterer Rechenzentrumsbestandteile auf Sicherheitselemente zu richten, da diese naturgemäß besonderen Anforderungen hinsichtlich Funktionalität, Verfügbarkeit und Leistung unterliegen.



Im Rahmen dieses Artikels werden die Auswirkungen von virtuellen Firewalls auf die Rechenzentrumsinfrastruktur betrachtet. Hierbei liegt der Schwerpunkt auf dem Einfluss, den Firewalls auf Aspekte des Netzdesigns und des Netzwerkmanagements haben, wenn sie in Form von virtuellen Maschinen innerhalb einer Server-Virtualisierungslösung laufen. Letztlich hängt die Sicherheit auch in einer virtualisierten Umgebung nicht allein von den Leistungsmerkmalen der Sicherheitskomponenten ab, sondern auch entscheidend von der Komplexität und der Managebarkeit des Gesamtsystems.

weiter auf Seite 19

Zweitthema

MS Office Communications Server:

Total Cost of Ownership im Vergleich zu klassischen Unified-Communications-Lösungen - Teil 2

von Dr. Michael Wallbaum und Dr. Frank Imhoff

Um die Gesamtkosten einer modernen Unified-Communications-Lösung gegenüberzustellen, müssen zahlreiche Faktoren einkalkuliert werden. Dazu gehören Wartungs- und Servicekosten ebenso wie Strom, Kühlung, Netzwerk-Anbindungen, Redundanz-Maßnahmen u.v.a.m. Gleichzeitig sind zwar deutliche Einspareffekte mithilfe von Unified Communications (UC) zu erzielen, jedoch sind diese Effekte schwer zu generalisieren und im Vorhinein kaum bezifferbar. Das liegt vor allem an fehlenden Erfahrungswerten, aber auch an der Tatsache, dass die Einführung von UC individuell auf jedes Unternehmen abgestimmt werden muss.

Zunächst bleibt also nur, die reinen Kosten im Sinne der Total Cost of Ownership (TCO) verschiedener UC-Lösungen zu betrachten. Im ersten Teil dieses Artikels haben wir bereits Lösungsansätze der Hersteller Cisco, Siemens Enterprise Networks (SEN) und Microsoft für drei verschiedene Nutzer-Szenarien gegenübergestellt.

weiter auf Seite 8

Sommer-Highlights

IT-Sicherheits-Forum 2009

Netzwerk-Design-Wettbewerb 2009

ab Seite 4

Geleit

Brauchen wir überhaupt Sicherheits-Lösungen?

ab Seite 2

Aktuelle Reports

Wide Area Networks:

Technik und Funktionsweise + Leitfaden für Design, Ausschreibung und Betrieb

ab Seite 17

Zum Geleit

Brauchen wir überhaupt Sicherheits-Lösungen?

Die Argumentation der Verkäufer von Sicherheits-Lösungen hat etwas Ermüdendes. Danach sind wir umzingelt von Bedrohungen und können uns glücklich schätzen, wenn wir überhaupt noch im Besitz einer lauffähigen IT-Lösung mit privaten Daten sind. Tatsächlich leidet die gesamte Branche unter dem Problem, dass immer wieder in der Vergangenheit Bedrohungs-Szenarien konstruiert worden sind, die in der Praxis bedeutungslos waren. Dies führt über die Zeit zwangsläufig zu einer Abstumpfung auf der Kundenseite. Kernproblem bleibt die Frage der Motivation eines Angreifers und warum er gerade dieses Unternehmen überhaupt angreifen sollte.

Tatsächlich muss unterschieden werden zwischen einem bewussten Angriff auf ein Unternehmen und einem unbewussten zum Beispiel durch ein Robot- /Virenverteilsystem. Die Bedrohung durch Robot- und Virenverteilsysteme muss ohne Frage als gegeben angesehen werden (u.a. als Teil der Technik von SPAM und DoS-Betreibern). Die meisten Unternehmen werden dabei gegen die gängigen Ausprägungen dieser Angriffe gewappnet sein. Bei dem bewussten Abgriff gibt es ganz unterschiedliche Formen des Angriffs, als Beispiele sind zu nennen:

- die gezielte Sabotage (zum Beispiel von Webservern)
- Spieltrieb innerhalb der Hacker-Community
- der gezielte Versuch des Datendiebstahls oder der Datenmanipulation

Die Dimension des Diebstahls vertraulicher Informationen muss in jedem Fall separat betrachtet werden, da die Absicherung dieses Bereichs ein weiter gefasstes Konzept erfordert und auch eine Menge nicht technischer Elemente beinhaltet. Tatsächlich wird es für einen Angreifer in diesem Bereich in der Regel eine Option sein, die traditionellen Angriffsformen zu benutzen (Einschleusung bzw. Nutzung eines Mitarbeiters durch Bestechung, Bedrohung...).

Wie real ist nun das Risiko, in dem sich

ein Unternehmen befindet, wirklich? Ein wesentlicher Punkt in der Risikobewertung ist die Einfachheit des Angriffs. Wie hoch sind die technischen Hürden, die der Angreifer tatsächlich zu nehmen hat? Für sehr professionelle Angreifer wird die Frage gar nicht so entscheidend sein (diese werden im Zweifelsfall sowieso mit einem anderen Portfolio von Angriffsinstrumenten arbeiten), aber für die Frage, wie viele weniger professionelle Angreifer Zugang zum Unternehmen erhalten, ist dies der zentrale Knackpunkt.

Und auch ohne in das permanente Predigen von Bedrohungen mit einfallen zu wollen, ist gerade in diesem Bereich zur Zeit eine messbare und deutliche Veränderung zu beobachten. Tatsächlich sind wir in Mitten einer Technologie-Veränderung, die die Hürden für einen Angreifer senkt oder die Menge seiner Möglichkeiten erhöht. Betroffen davon sind u.a. die zentralen Infrastrukturen der Unternehmen und nicht nur die Endgeräte.

Wesentliche Bereiche, in denen wir diese Veränderungen beobachten können, sind:

- die Rechenzentren im Übergang zu Virtualisierung
- mobile Mitarbeiter und deren technische Einbindung in das Unternehmen
- der langsame, aber stetige Ausbau von Unified Communications
- die zunehmende Integration von Produktionsanlage in offene Netzwerk-Infrastrukturen

Zweitthema

MS Office Communications Server:

Total Costs of Owner-ship im Vergleich zu klassischen Unified-Communications-Lösungen - Teil 2

Fortsetzung von Seite 1

Dr. Michael Wallbaum ist Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Projekterfahrung in Forschung, Entwicklung und Betrieb im Bereich mobiler Kommunikationssysteme, Voice-over-IP und Groupware zurück. Zu diesen Themenbereichen sind von ihm zahlreiche Veröffentlichungen und Buchbeiträge erschienen.

Dr. Frank Imhoff ist technischer Direktor und Senior Consultant der ComConsult Beratung und Planung GmbH. Er blickt auf jahrelange Erfahrung in Forschung, Entwicklung und Betrieb von lokalen Netzen, Voice-over-IP, Wireless Local Area Networks sowie anderen Mobilfunk- und Telekommunikationssystemen zurück. Zu diesen Themenbereichen sind von ihm bereits zahlreiche Veröffentlichungen erschienen und Seminare betreut worden.

Nun folgen die wirtschaftlichen Aspekte dieser Lösungsansätze. Dabei werden sowohl die erforderlichen Investitionen für Hard- und Software (Capital Expenditure, Capex) als auch die Betriebskosten (Operational Expenditure, Opex) einer Lösung zugrunde gelegt.

Zur Ermittlung der je nach Lösungsansatz erforderlichen Investitionen wurden nach Möglichkeit die aktuellen Listenpreise der Hersteller zugrunde gelegt, die trotz aller Rabatt-Schlachten erfahrungsgemäß einen soliden Richtwert bieten. Darüber hinaus konnte jedoch auch auf die Ergebnisse von zahlreichen Ausschreibungen und einschlägigen Erfahrungen aus vielen Projekten zurückgegriffen werden. Einzig bei Microsoft liegen für die definierten Szenarien derzeit noch keine verwertbaren Erfahrungen vor, da Microsoft bei keinem der hier zugrunde gelegten Szenarien überhaupt mitgeboten hat. Zudem liegen die maßgeblichen Preise für Software-Lizenzen auch von bilateralen Vereinbarungen zwischen Microsoft und dem Kunden bzw. von den Lizenzprogrammen ab. Microsoft ist nach wie vor bestrebt, seinen Office Communications Server 2007 im Markt zu platzieren und bietet daher teilweise entsprechend niedrige (und marktferne) Projektpreise. Es bleibt also zunächst nichts anderes übrig als generell Listenpreise anzusetzen. Darüber hinaus wurde ein Wechselkurs von 1,35 USD zu einem Euro angesetzt und einige Preise im Rahmen von Webrecherchen oder Schätzungen ermittelt.

Unabhängig vom Typ und Einsatzzweck fallen für den Betrieb einer Lösungskomponente Kosten in den Kategorien Infrastruktur und Dienstleistung an. Diese Infrastruktur- und Support-Kosten entstehen letztlich sowohl für Server und Netzwerk-

MS Office Communications Server: Total Cost of Ownership im Vergleich zu klassischen UC-Lösungen - Teil 2

komponenten in einem Rechenzentrum als auch für Endgeräte auf den Schreibtischen der Mitarbeiter und müssen daher für alle Lösungen separat kalkuliert werden. Dazu gehören z.B. folgende Punkte:

- Stellfläche
- Netzwerk-Anbindung
- Strom, Kühlung
- Grundlegende Betriebsüberwachung (Monitoring, Reporting, Statistik, Status etc.)

Bei den Dienstleistungen tragen u.a. folgende Posten zu den Kosten bei:

- Hardware-Wartung (Austausch von Geräten, Netzteilen, Lüftern, Festplatten etc.)
- Software-Wartung (Einspielen von Software-Patches, Konfigurationsänderungen etc.)
- Backup und Restore

Um die Komplexität des Betriebskostenmodells in einem überschaubaren Rahmen zu halten, wurden die oben genannten Kosten nicht einzeln für jede Lösungs-Komponente festgelegt. Stattdessen wurden verschiedene Betriebskosten-Klassen definiert. Hier wird nur grob zwischen Standard-Servern, Appliances und Endgeräten unterschieden. Dazu wurden folgende Annahmen getroffen:

- Kosten für Strom, Wartung und Support von Servern und Appliances wurde für alle Hersteller einheitlich festgelegt. Unterschiede in den Betriebskosten entstehen somit ausschließlich durch verschiedene Architekturen bzw. Komponentenmengen.

- Stromkosten wurden einheitlich mit 0,15 Euro pro Kilowattstunde angesetzt.

- Kosten für Software-Wartung wurden nicht betrachtet.

Die Betriebskosten für Standard-Server hängen u.a. von der Qualität der Infrastruktur im Sinne einer Redundanz der Strom- und Internetanbindung, der Sicherheitsreserven bei der Kühlung sowie der Vorkehrungen gegen Brände usw. ab. Unternehmen in den hier betrachteten Größenordnungen verfolgen in diesem Zusammenhang in der Regel hohe Standards, vor allem vor dem Hintergrund der großen Bedeutung der Telefonie. Das gleiche gilt für Dienstleistungen für die vor allem bei einer externen Vergabe der Aufgaben Service Level Agreement (SLA) definiert werden. Diese unterscheiden sich deutlich hinsichtlich des Umfangs, der Betriebs-, Service- und Reaktionszeiten, jedoch werden bei zentralen TK-Komponenten immer die allerhöchsten Maßstäbe angelegt. Aus diesen Gründen wurde den Wartungs- und Supportkosten der Server-Klassen die Preise (ca. 250 Euro) renommierter Housing- bzw. Hosting-Anbieter zugrunde gelegt. Bei Servern, die an abgesetzten Standorten mit weniger als 100 Mitarbeitern installiert sind, wurden deutlich erhöhte Wartungspauschalen angesetzt (ca. 350 Euro), da hier ein höherer Aufwand aufgrund der Anreise von Servicetechnikern etc. üblich ist.

Im Vergleich zu Standard-Servern zeichnen sich die hier definierten Appliances durch eine größere Vielfalt, typischerweise geringeren Stromverbrauch, weniger Konfigurationsänderungen und geschlossene Systeme aus. Aus den letzten beiden Punkten ergibt sich u.a. ein geringerer Aufwand beim Backup und ein einfacherer Support, da in der Regel keine Reparaturen sondern nur ein Austausch der Geräte stattfindet. Zu den Appliances gehören aber z.B. auch PSTN-Gateways, ATAs oder IP-DECT Basisstationen. Um der Vielfalt gerecht zu werden ist neben der Unterscheidung zwischen zentral und remote installierten Geräten auch eine Unterteilung nach der „Größe“ der Geräte statt, wobei die Einteilung vom Stromverbrauch und dem Preis der Appliance abhängig ist. Dementsprechend reichen die zugrunde gelegten monatlichen Wartungs- und Supportkosten für Appliances von 1 bis zu 300 Euro sowie der der Stromverbrauch von 10 bis 2000 Watt.

Endgeräte

Bei den Endgeräten müssen Basis-, Standard-, Comfort-Geräten und Softphones unterschieden werden. In deren Betriebskosten fließen sowohl die Stromkosten als auch die Wartungs- und Supportkosten ein. Die Stromkosten basieren dabei auf Herstellerangaben für die verwendeten Geräte. Der üblicherweise verwendete Wert für den On-Hook-Status ist jedoch nicht hinreichend aussagekräftig. Ein typisches Arbeitsplatztelefon wird schließlich nur während der Arbeitszeit benötigt und ist damit zwei Drittel des Tages ohne Funktion. Über das Jahr betrachtet liegt der Anteil der „unproduktiven“ Zeit sogar bei rund 80% wenn man Wochenenden, Urlaub, Krankheitstage etc. hinzuzählt. Aus diesem Grund ist der Strombedarf eines Geräts im Standby-Modus – sofern das Gerät über einen solchen Modus verfügt – von besonders großer Bedeutung.

Um den „typischen“ Stromverbrauch eines Endgerätes zu ermitteln, wurde daher ein einfaches Rechenmodell verwendet, das mit den Herstellerwerten parametrisiert wurde. Die Werte für die unterschiedlichen Modi (on-hook, active, ringing und standby) wurden den jeweiligen Datenblättern der Hersteller entnommen bzw. im ComConsult Test-Center gemessen. Die Kosten für Wartung und Support ergeben sich aus marktüblichen Portpreisen, wobei der Anteil des Anschaffungspreises für das Endgerät herausgerechnet wurde. Diese sind schließlich in den Investitionskosten enthalten. Es wird davon ausge-

Schwerpunktthema

Dipl.-Inform. Matthias Egerland ist Leiter des Competence Centers Virtuelle IT und arbeitet als Berater in den Competence Centern IT-Sicherheit und Netze bei der ComConsult Beratung und Planung GmbH. Neben den Schwerpunkten Desktop-, Server- und Infrastruktur-Virtualisierung beschäftigt sich Herr Egerland insbesondere mit der Sicherheit in virtualisierten Umgebungen. Darüber hinaus erstellt er Konzepte und Ausschreibungen von IT-Infrastruktur-Lösungen gemäß UfAB. Herr Egerland ist zertifiziert als Cisco Certified Network Associate (CCNA).

Dipl.-Ing. Björn Korall ist Berater und Netzwerkplaner der ComConsult Beratung und Planung. Bereits während seines Studiums beschäftigte er sich mit drahtloser Datenkommunikation und war in de vergangenen zwei Jahren ausschließlich im Bereich Forschung, Entwicklung und Beratung von WLANs nach IEEE 802.11 tätig. Sein Fokus lag hierbei in der in der Erhöhung der Performance von WLANs und VoIP over WLAN (VoWLAN).

Dipl.-Inform. Daniel Meinhold ist Consultant bei der ComConsult Beratung und Planung GmbH. Dort ist er in den Bereichen Telekommunikationsysteme, Virtualisierung und IT-Sicherheit tätig. Neben diesbezüglichen Praxiserfahrungen in zahlreichen Projekten ist er für die Planung und Durchführung entsprechender Testszenarien im ComConsult-eigenen Labor zuständig.

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

Fortsetzung von Seite 1

1. Sicherheitsstrukturen mit unterschiedlichem Virtualisierungsgrad

Der Einsatz von Server-Virtualisierung hat sich mittlerweile in vielen Unternehmen und Behörden etabliert. Die Absicherung virtueller Serverumgebungen erfordert hierbei die Berücksichtigung von unterschiedlichen Vertrauensbereichen, z.B. Finanz-, Produktions- und Testumgebung. Die Gruppierung der virtuellen Server eines Vertrauensbereiches zu einer Sicherheitszone ist hierbei je nach Anforderung an Sicherheit, Verfügbarkeit und Performance auf unterschiedliche Art möglich. Grundsätzlich kann zwischen drei Architekturen unterschieden werden, welche nachfolgend kurz erläutert werden. Detaillierte Informationen zu Sicherheitszonen in virtuellen und physischen Umgebungen finden sich im Netzwerk Insider vom November 2008 :

1.1 Szenario 1: Dedizierte physische Server je Sicherheitszone

In diesem Szenario werden physische Server dediziert einer Sicherheitszone zugewiesen, z.B. ein Virtualisierungs-Cluster für die Finanzabteilung, ein Virtualisierungs-Cluster für die Entwicklungsabteilung, etc. Physische Sicherheitselemente trennen, wie zuvor ohne Virtualisierung, die verschiedenen Sicherheitszonen voneinander ab (siehe Abbildung 1).

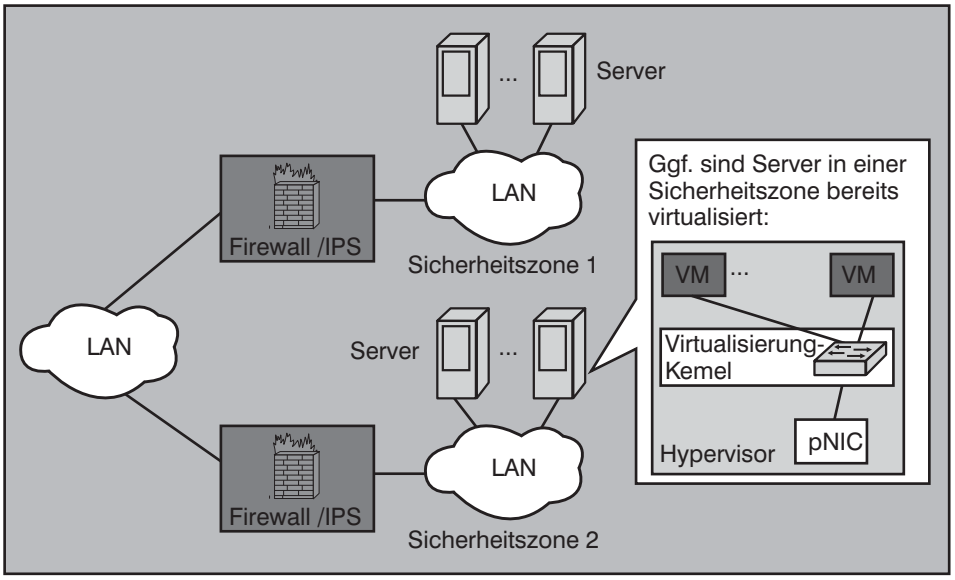


Abbildung 1: Dedizierte physische Server je Sicherheitszone

1.2 Szenario 2: Virtuelle Trennung von Sicherheitszonen

Im zweiten Szenario erfolgt die Trennung innerhalb der virtuellen Umgebung mittels virtueller Switche. Diese werden dediziert oder mittels VLAN-Tagging einer physischen Netzwerkschnittstelle (pNIC) zugeordnet und an externe physische Sicherheitselemente angebunden (Abbildung 2).

heiten abhängig, wie z.B. NICs, Switches, Routern oder anderen Sicherheitselementen. Eine virtualisierte Umgebung erfordert, dass dieser Netz- bzw. Sicherheitskontext (aktuelle Zustände/ Sitzungen, VLANs, QoS-Parameter, Traffic-Zähler etc.) dynamisch auf allen Host-Systemen zur Verfügung steht. Diese Kontexte müssen insbesondere bei dynamischen Leistungsmerkmalen der Virtualisierungslösung nicht nur erhalten, sondern auch konsistent bleiben. Als Beispiele solcher Leistungsmerkmale seien an dieser Stelle VMware HA, VMotion, Citrix XenMotion bzw. Microsoft Live Migration sowie dynamische Ressourcenverteilung durch z.B. VMwares Distributed Ressource Scheduler (DRS) genannt.

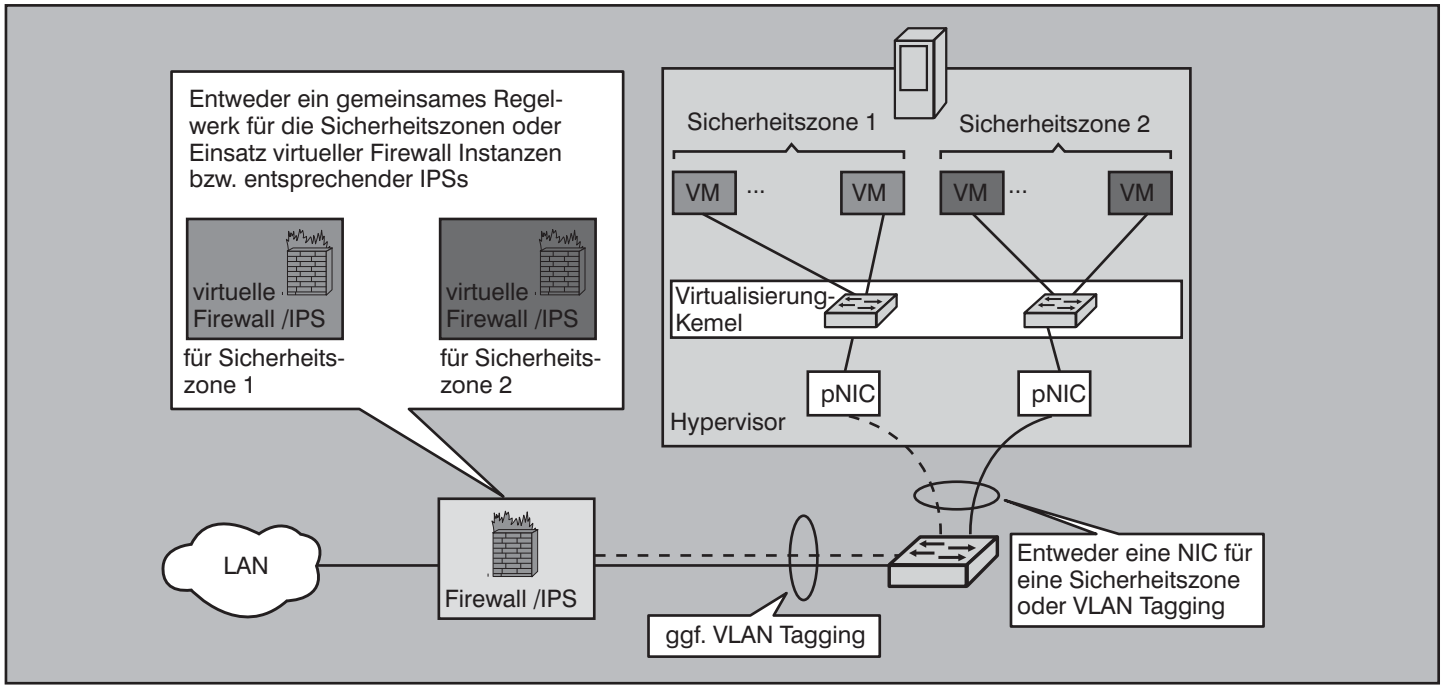


Abbildung 2: Virtuelle Trennung von Sicherheitszonen

1.3 Szenario 3: Vollständige Virtualisierung

Ähnlich wie in Szenario 2 werden auch hier die Sicherheitszonen innerhalb der virtuellen Umgebungen gebildet. Anstatt diese jedoch über physische Sicherheitselemente zu führen, kommen diese in virtualisierter Form zur Anwendung, z.B. virtuelle Firewalls oder IDS/IPS-Systeme (Abbildung 3).

Als Richtlinie gilt in dieser Architektur, dass das Sicherheitsniveau je nach Virtualisierungsgrad abnimmt, d.h. das höchste Sicherheitsniveau wird mittels dedizierter physischer Server für die virtuellen Server eines Vertrauensbereiches erzielt (Szenario 1). Dies steht im Widerspruch zu den grundsätzlichen Vorteilen, die durch die Virtualisierung erreicht werden sollen, wie z.B. einer effizienteren Auslastung der Systeme.

Doch auch die Verwendung von virtuellen Sicherheitselementen, wie in den Szenarien 2 und 3 dargestellt, stellt eine Herausforderung dar. In physischen Infrastrukturen sind Sicherheitsarchitekturen hochgradig von physischen Gegeben-

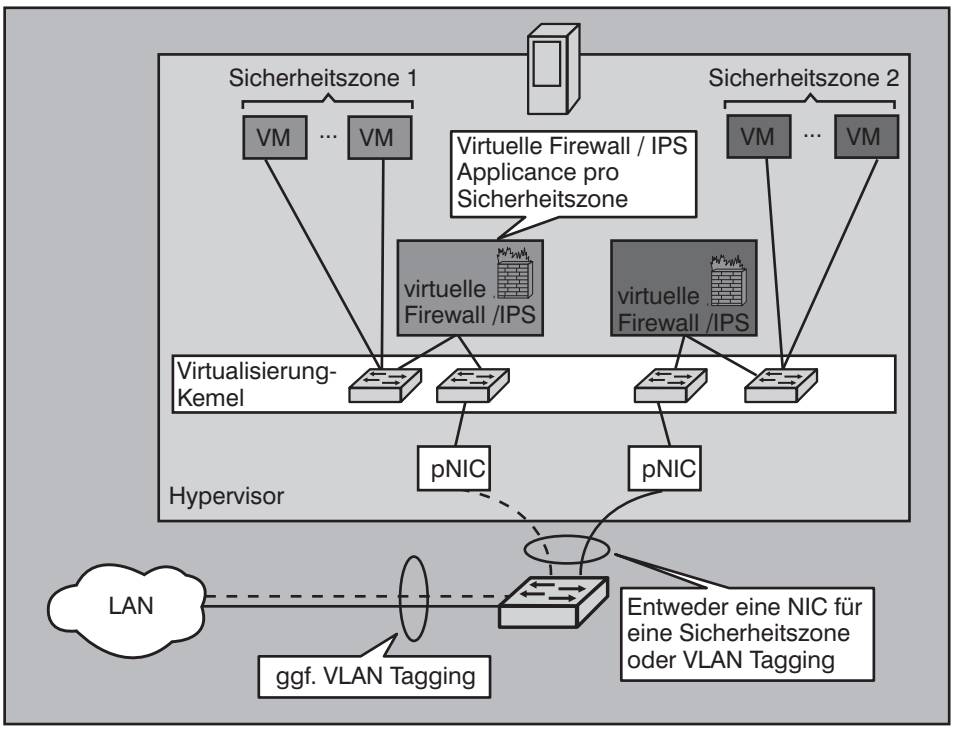


Abbildung 3: Vollständige Virtualisierung von Sicherheitszonen