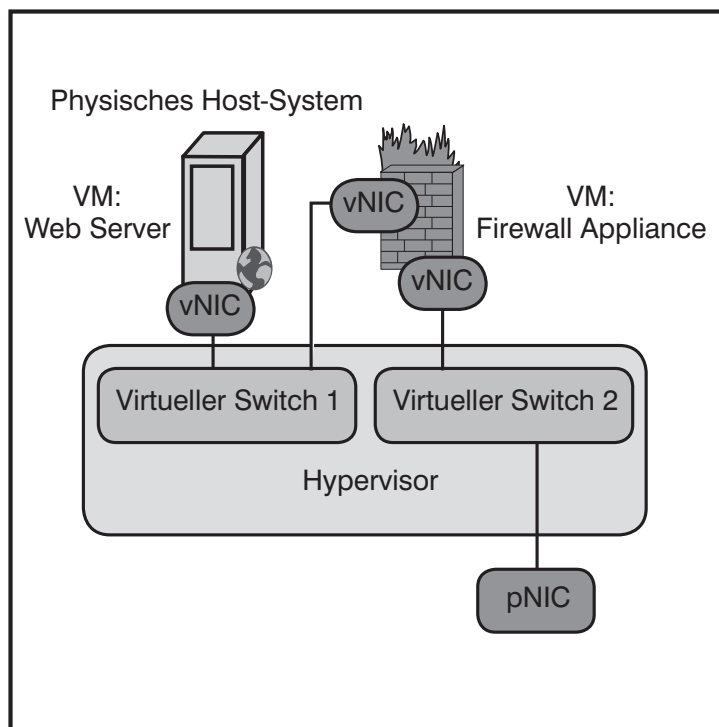


Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

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 Netzwerkmanage-

ments 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.

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 den vergangenen zwei Jahren ausschließlich im Bereich Forschung, Entwicklung und Beratung von WLANs nach IEEE 802.11 tätig. Sein Fokus lag hierbei 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.

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 Sicherheits-

zone zugewiesen, z.B. ein Virtualisierungs-Cluster für die Finanzabteilung, ein Virtualisierungs-Cluster für die Entwicklungsabteilung, etc. Physische Sicher-

heitselemente trennen, wie zuvor ohne Virtualisierung, die verschiedenen Sicherheitszonen voneinander ab (siehe Abbildung 1).

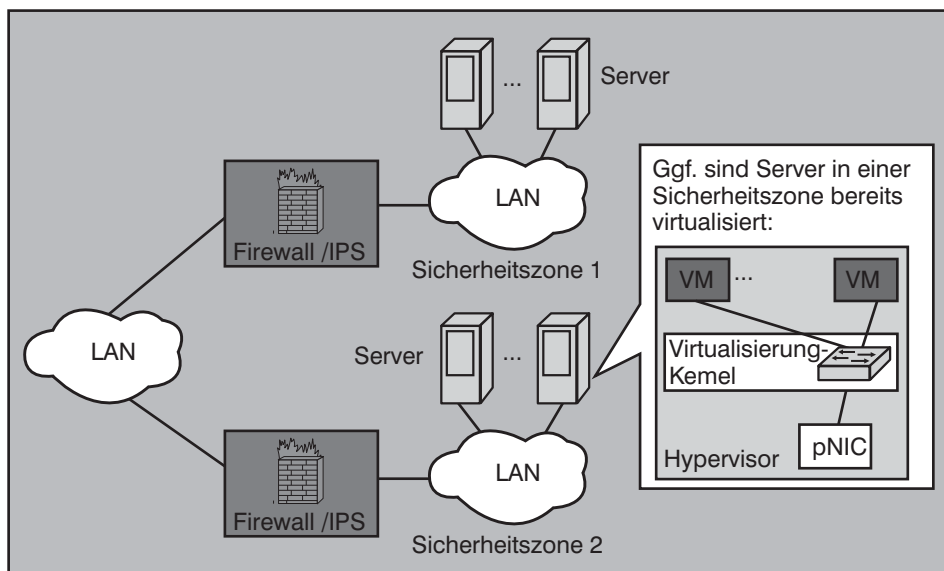


Abbildung 1: Dedizierte physische Server je Sicherheitszone

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

1.2 Szenario 2: Virtuelle Trennung von Sicherheitszonen

Im zweiten Szenario erfolgt die Trennung innerhalb der virtuellen Umgebung mittels virtueller Switches. 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 Leis-

tungsmerkmalen 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 Resource Scheduler (DRS) genannt.

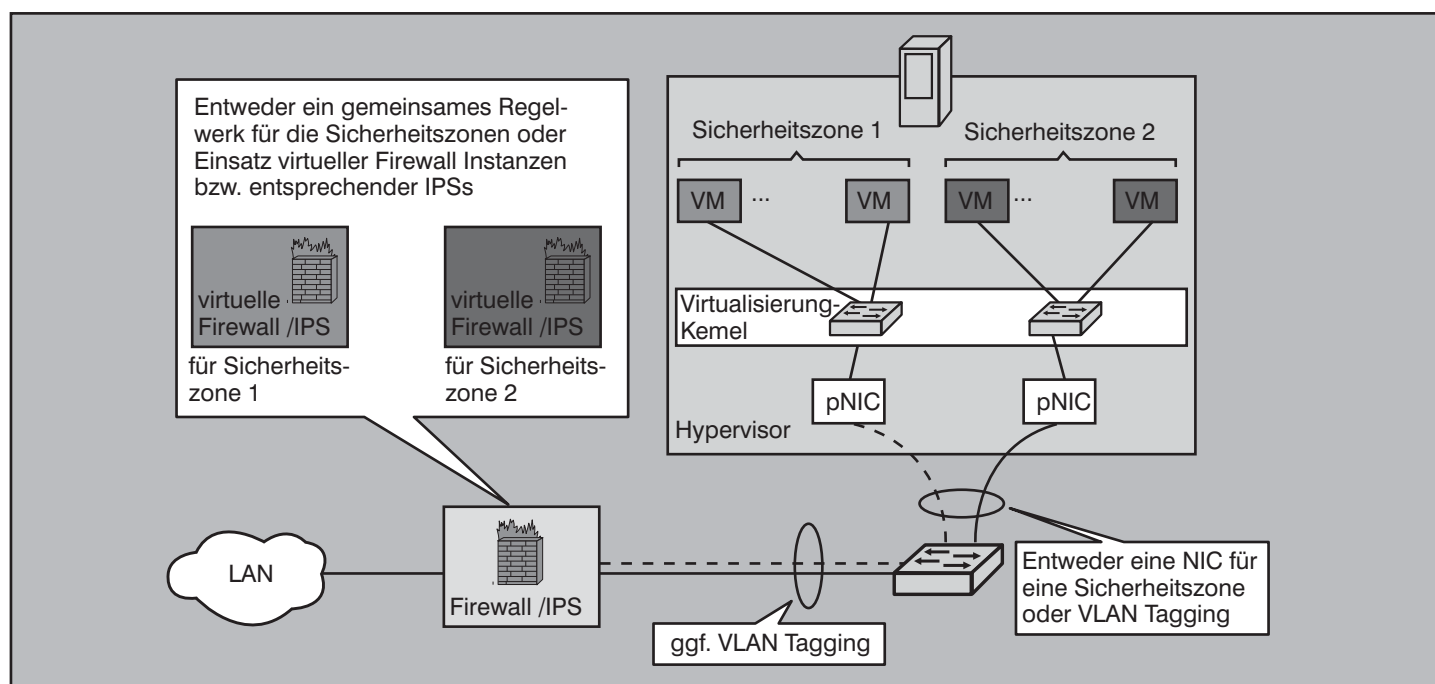


Abbildung 2: Virtuelle Trennung von Sicherheitszonen

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-

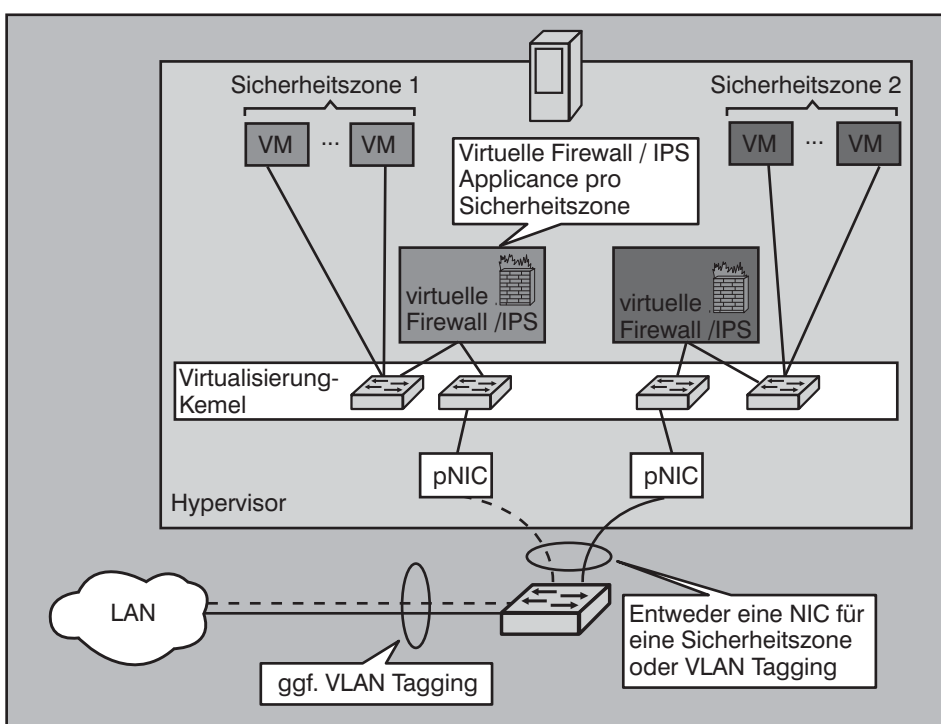


Abbildung 3: Vollständige Virtualisierung von Sicherheitszonen

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

Ein weiterer wichtiger Aspekt im Zusammenhang mit virtuellen Firewalls ist die erforderliche Performance für den Betrieb der virtuellen Sicherheitskomponenten, welche nun logischerweise mit in die Ressourcenplanung bzw. die Dimensionierung der virtuellen Infrastruktur integriert werden müssen. In physischen Firewalls kommt oftmals Spezialhardware zum Einsatz, welche auf die Anforderungen der Paketanalyse optimiert ist. Beispielsweise werden speziell entworfene ASICs zur Paket- und Flussanalyse verwendet. Eine derart optimierte Hardware ist nicht ohne Leistungsverlust zu virtualisieren.

2. Begriffsklärung

Da es – wie im letzten Abschnitt dargestellt – zwei grundlegend unterschiedliche Ansätze gibt, Firewalls zu virtualisieren, ist zunächst eine Begriffsklärung erforderlich, wenn von „virtuellen Firewalls“ die Rede ist. Die folgenden Abschnitte grenzen „virtualisierbare“ von den „virtuellen“ Firewalls ab und zeigen die konzeptionellen Unterschiede beider Varianten auf.

2.1 Virtualisierbare Firewalls – Appliances, die in logische Firewall-Instanzen untergliedert werden können

Die meisten am Markt etablierten Hersteller von Appliance-basierten Firewalls- also Firewalls, die als physische Komponente in das Datennetz integriert werden - bieten bereits seit geraumer Zeit das Leistungsmerkmal, ihre Komponenten in logische Firewall-Instanzen zu segmentieren. Jede Teileinheit stellt sich nach Außen als eigene Firewall dar, die unabhängig von benachbarten Teileinheiten ein eigenes Regelwerk, eigene Administrationsrechte, eigene IP-Adressstrukturen und ggf. eigene Routing-Tabellen besitzt.

Innerhalb von mandantenfähigen Firewall-Managementsystemen können diese Firewall-Instanzen wie ihre physischen Pendanten überwacht und administriert werden. Dem Firewall-Manager einer einzelnen Instanz können granular Rechte vergeben werden, die es ihm in einem bestimmten Umfang erlauben, seine Instanz zu verwalten. Ein übergeordnetes Basisregelwerk, Netzwerkeinstellungen sowie bestimmte Objekte können beim Anlegen der Instanz vordefiniert und gleichzeitig für die jeweilige Instanz vor Änderung geschützt werden. Damit bieten virtualisierbare Firewalls die Möglichkeit, Mandanten einfach und kostengünstig eine vollwertige Firewall zur Verfügung zu stellen, ohne auf eine übergeordnete Basiskontrolle verzichten zu müssen.

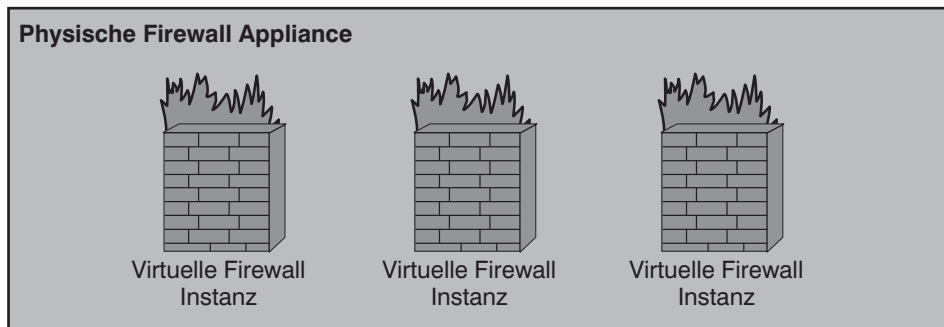


Abbildung 4: Physische Firewall mit drei virtuellen Firewall Instanzen

Eine solche physische Sicherheitskomponente soll im Folgenden als „virtualisierbare Firewall“ bezeichnet werden, während die darin konfigurierten einzelnen logischen Firewalls „virtuelle Firewall Instanzen“ darstellen.

Die einzelnen am Markt befindlichen Produkte dieser Kategorie unterscheiden sich hinsichtlich der Frage, welche der genannten Leistungsmerkmale zu welchem Grad unabhängig von benachbarten virtuellen Firewall Instanzen verfügbar sind. Beispiele für diese Architektur sind Ciscos „Virtual Firewall Context“, Junipers „Virtual System“ und Nokias „Multiple Domain Security“.

Abbildung 4 zeigt eine physische Firewall Appliance, in der drei logische Firewalls in Form von virtuellen Firewall Instanzen konfiguriert sind.

2.2 Virtuelle Firewalls – Firewalls als virtuelle Maschine innerhalb einer Server-Virtualisierungslösung

Mit der Marktreife von Technologien zur Server-Virtualisierung hält nun auch eine weitere Form von Firewalls Einzug in das Portfolio der Anbieter von Sicherheitskomponenten: Firewalls, die als virtuelle Maschine innerhalb einer Virtualisierungsumgebung betrieben werden. Mit derartigen Produkten sind insbesondere diejenigen Hersteller am Markt zu finden, deren Firewalls auch ohne den Virtualisierungsgedanken als reine Software-Lösung erhältlich sind bzw. für Standard-(Linux-)Betriebssystem-Umgebungen entwickelt wurden. Als Beispiele derartiger Anbieter sind Checkpoint mit der VPN-1 VE „Virtual Edition“ und Astaro mit der „Security Gateway Virtual Appliance“ zu nennen.

Der Leistungsumfang dieser Komponenten geht dabei über den eines dynamischen Paketfilters deutlich hinaus: VPN-Gateway, Intrusion Prevention, E-Mail-Sicherheit bis hin zu Hochverfügbarkeit im Active/Active- und Active/Standby-Modus gehören zum Funktionsumfang der genannten Produk-

te. Dabei werden jedoch seitens der Hersteller keine Angaben zur Leistung in diesen Kategorien gemacht. Dies ist insofern verständlich, als die Leistung von den verfügbaren Ressourcen des Host-Systems abhängt. Hier sollte ein ausgiebiger Test mit realistischen Kommunikationsdaten in einem nicht-produktiven Umfeld der weiteren Einsatzplanung vorausgehen. Schließlich wird eine solche Sicherheitskomponente schnell zum Flaschenhals, wenn sie sämtlichen Netzverkehr auf mehreren Schichten des OSI-Modells untersuchen soll. Und nicht umsonst wurde auf Seiten der physischen Sicherheits-Appliances Spezialhardware entwickelt, die nur auf Basis von dedizierten ASICs hohe Durchsatzraten erzielen kann.

Die Produktion einer virtuellen Appliance ist bei Vorliegen einer reinen Software-Lösung aus Herstellersicht denkbar einfach: Innerhalb einer Virtualisierungsumgebung wie beispielsweise Citrix XenServer, Microsoft Hyper-V oder VMware Virtual Infrastructure wird eine neue virtuelle Maschine angelegt, die das erforderliche Betriebssystem aufweist und über die nötigen I/O-Ressourcen zur Kommunikation der VM mit der Außenwelt verfügt. Diese virtuelle Maschine erhält Zugriff auf die Firewall-Software z.B. in Form eines ISO-Images der Installations-CD-ROM, die mit einem virtuellen CD-ROM-Laufwerk verknüpft ist. Die Software wird nun von diesem Image auf die virtuelle Maschine installiert. Nachdem der Installationsvorgang abgeschlossen ist, liegt die virtuelle Appliance in Form des Festplatten-Images der virtuellen Maschine vor.

Ist dieses Festplatten-Image in einem offenen Format spezifiziert, wie etwa Microsofts „Virtual Harddisk“ (.vhd) oder dem „Open Virtual File Format“ (.ovf), ist diese virtuelle Maschine theoretisch mit jeder Server-Virtualisierungslösung zu betreiben, die dieses Format unterstützt. In der Praxis ist es gegenwärtig so, dass die meisten Hersteller derartiger virtueller

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

Firewalls das VMware-proprietäre „Virtual Machine Disk Format“ (.vmdk) nutzen. Der Hintergrund dafür ist, dass VMware ein eigenes Zertifizierungsprogramm aufgelegt hat, das ein Produkt als „VMware Certified Virtual Appliance“ ausweist, sofern es im Wesentlichen die folgenden Aspekte liefert:

- fertige Konfektion der Software als virtuelle Maschine für die Virtualisierungslösung von VMware
- Support des Herstellers für den Betrieb der Software als virtuelle Maschine in der VMware-Umgebung
- Lizenzgebühren des Herstellers an VMware

Mindestanforderungen hinsichtlich Funktionalität, Funktionstests oder Leistungsfähigkeit bestehen hingegen nicht.

Theoretisch ist also der Betrieb der virtuellen Appliance auch im Citrix XenServer und Microsoft Hyper-V Umfeld denkbar, nachdem das Dateiformat in die dort lesbare „.vhd“-Form konvertiert wurde. Allerdings würde dann der Hersteller-Support für diese Lösung nicht mehr gelten, weswegen diese Möglichkeit in Produktivumgebungen ausscheidet.

Das Management dieser virtuellen Firewalls unterscheidet sich nicht von ihren physischen Ausführungen. Beide werden über das gleiche zentrale Management verwaltet. Die Virtualisierung bleibt somit hinsichtlich des Managements transparent für den Firewallbetrieb.

Die folgenden Abschnitte beleuchten Integrationsaspekte sowie Hochverfügbarkeitsmechanismen derartiger virtueller Firewalls.

3. Integration in die virtuelle Infrastruktur / das Datennetz

Die marktgängigen Server-Virtualisierungslösungen vom Typ 1 Virtual Maschine Monitor arbeiten nach dem Prinzip, dass auf einer geeigneten Serverhardware eine Virtualisierungslösung installiert wird – der sog. Hypervisor – auf dem dann die virtualisierten Server in Form von virtuellen Maschinen (VMs) laufen. Um den virtuellen Maschinen eine Netzwerkverbindung sowohl untereinander, als auch mit der Außenwelt zu ermöglichen, werden virtuelle Netzwerke (Citrix) bzw. virtuelle Switches (VMware) innerhalb des Hypervisors realisiert.

Während sich die Bezeichnung dieses

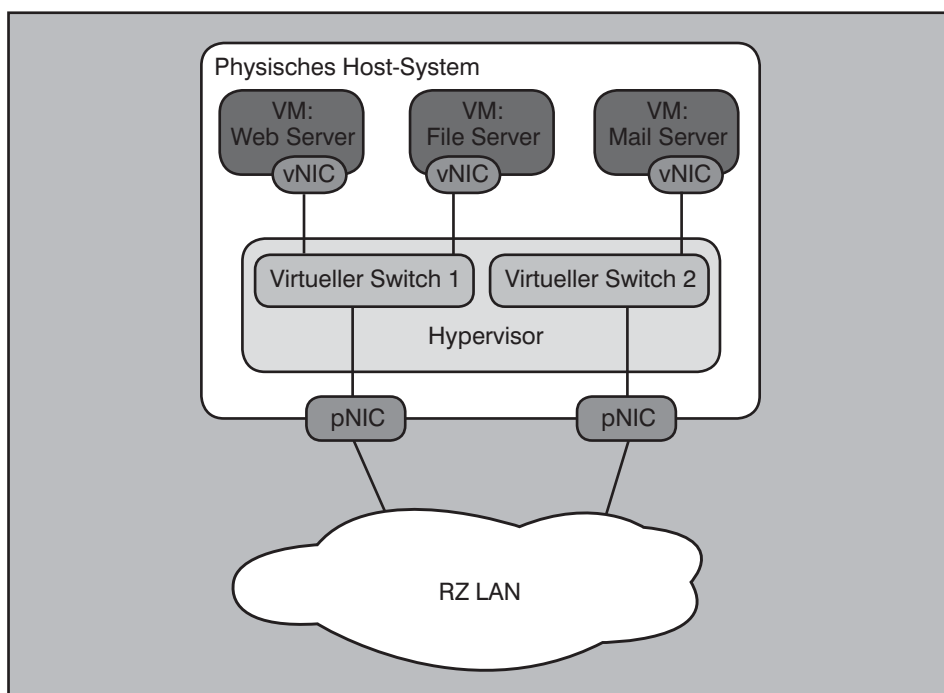


Abbildung 5: Verbindung der virtuellen Maschinen untereinander und mit dem physischen Netz (RZ LAN) über virtuelle Switches innerhalb des Hypervisors. Physische Netzwerkschnittstellen (pNIC) verbinden das Host-System mit dem Rechenzentrumsnetz, virtuelle Netzwerkschnittstellen (vNIC) verbinden die virtuellen Maschinen mit den virtuellen Switches.

Ansatzes zwischen den Herstellern der Virtualisierungslösungen unterscheidet, ist die damit verbundene Funktionalität die gleiche: mit Hilfe der Administrationsoberfläche oder Kommandozeile wird für jede physische und virtuelle Netzwerkschnittstelle definiert, welchem Netzwerk diese zugeordnet wird, welche VLAN ID sie ggf. bekommt und welche Konnektivität sich daraus mit anderen Netzwerkschnittstellen ergibt. Auf diese Weise können unterschiedliche Topologien realisiert werden: Testumgebungen ohne Verbindung zur Außenwelt oder dem Produktivnetz, Demilitarisierte Zonen (DMZ) innerhalb der Virtualisierungsumgebung und Servernetze mit Verbindung zum physischen LAN.

Abbildung 5 zeigt die Verbindung von virtuellen Maschinen untereinander und mit dem physischen Netz (RZ LAN) über virtuelle Switches innerhalb des Hypervisors.

Die von VMware gewählte Bezeichnung „virtueller Switch“ mag dabei zur Veranschaulichung der Funktionalität dieser Komponente dienlich sein. Andererseits ist sie insofern irreführend, als dem virtuellen Switch einige wesentliche Merkmale fehlen, die der Netzwerker mit einer solchen Komponente assoziiert. So besitzt der virtuelle Switch zwar ebenfalls eine MAC-Tabelle, in der er die Zuordnung von Layer-2-Adressen und seinen einzelnen Ports speichert. Diese MAC-Tabelle wird jedoch

nicht dynamisch auf Basis des beobachteten Datenverkehrs erlernt, sondern mittels der oben beschriebenen statisch konfigurierten Konnektivität definiert. Ein Ethernet-Frame mit einer unbekanntenen Ziel-MAC-Adresse führt also nicht zu einem Layer-2-Broadcast an alle Switch-Ports, sondern wird schlicht verworfen.

Aus einer Sicherheitsperspektive betrachtet bringt dieses Verhalten des virtuellen Switches jedoch auch Vorteile mit sich: konstruktionsbedingt ist diese Komponente unempfindlich gegenüber Layer-2-Angriffen wie beispielsweise MAC-Flooding. Beim MAC-Flooding wird durch eine große Zahl von Ethernet-Frames mit unterschiedlicher Source-MAC-Adresse versucht, die MAC-Tabelle des Switches zum Überlaufen zu bringen und ihn dadurch zu kompromittieren. Da der virtuelle Switch neue MAC-Adressen nicht dynamisch lernt, kann seine MAC-Tabelle auch nicht überlaufen.

Ein weiterer wesentlicher Unterschied zu physischen Switches ist, dass virtuelle Switches innerhalb eines Hypervisors nicht untereinander verbunden werden können. Es können also keine hierarchischen oder redundanten Netztopologien innerhalb des Hypervisors aufgebaut werden, wie sie aus physischen Netzumgebungen bekannt sind. Dieser Umstand bringt den Vorteil mit sich, dass mittels virtueller Switches keine Schleifentopologien konfiguriert

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

werden können. Damit müssen Mechanismen zur Schleifenunterdrückung wie beispielsweise das Spanning Tree Protocol (STP) von diesen Komponenten nicht unterstützt werden. Auch zwischen zwei physischen Netzwerkschnittstellen, die mit dem gleichen virtuellen Switch verbunden sind und im „NIC-Teaming“-Modus betrieben werden, erfolgt kein Switching.

Ein weiterer Vorteil der Tatsache, dass die Bezeichnung „virtuelles Netzwerk“ von Citrix in Anbetracht der realisierten Funktionalität treffender ist als „virtueller Switch“ von VMware, ist der damit ausbleibende Einfluss auf die physische Netztopologie. Durch die virtuellen Switches wird eben keine weitere Ebene in die Netzwerkhierarchie eingebracht. Bei Inbetriebnahme einer der heutigen Server-Virtualisierungslösungen muss das Netzdesign nicht angepasst werden. Spanning-Tree-Domänen dehnen sich genauso wenig in die virtuelle Infrastruktur aus wie Routing-Bereiche.

Dies mag sich in dem Moment ändern, wo ein tatsächlich vollwertiger virtueller Switch in die Virtualisierungsumgebung eingebracht wird, wie beispielsweise der Cisco Nexus 1000v. Hier gilt es genau zu analysieren, ob ein physischer Switch mit allen Leistungsmerkmalen aber auch Einflüssen auf die Netztopologie virtualisiert wurde, oder ob das oben beschriebene Konzept der virtuellen Switches um zusätzliche Funktionalitäten wie erweiterte Port Security und Quality of Service ergänzt werden.

Virtuelle Firewall-Appliances sind aus Sicht des Host-Systems eine virtuelle Maschine wie jede andere auch und werden insofern in gleicher Weise mit dem Netzwerk verbunden. Abbildung 6 zeigt die Realisierung einer DMZ mittels virtueller Switches und einer virtuellen Firewall in einer virtuellen Umgebung.

4. Hochverfügbarkeit von virtuellen Firewalls

Die Anforderungen an die Verfügbarkeit von Netzkomponenten und Servern sind in virtuellen Umgebungen nicht anders als in physischen Netzen. Dies gilt insbesondere auch für Sicherheitskomponenten, von deren Verfügbarkeit in der Regel die Erreichbarkeit ganzer Netzbereiche abhängt.

Beim Einsatz physischer Appliances in herkömmlichen, nicht-virtualisierten Server-Umgebungen wird üblicherweise ein Active/Standby-Betrieb der Appliances favorisiert, da hier eine vollwertige Redundanz und ein deterministischer Kommunikationspfad vorliegt. Bei Interface-Problemen oder Ausfall der aktiven

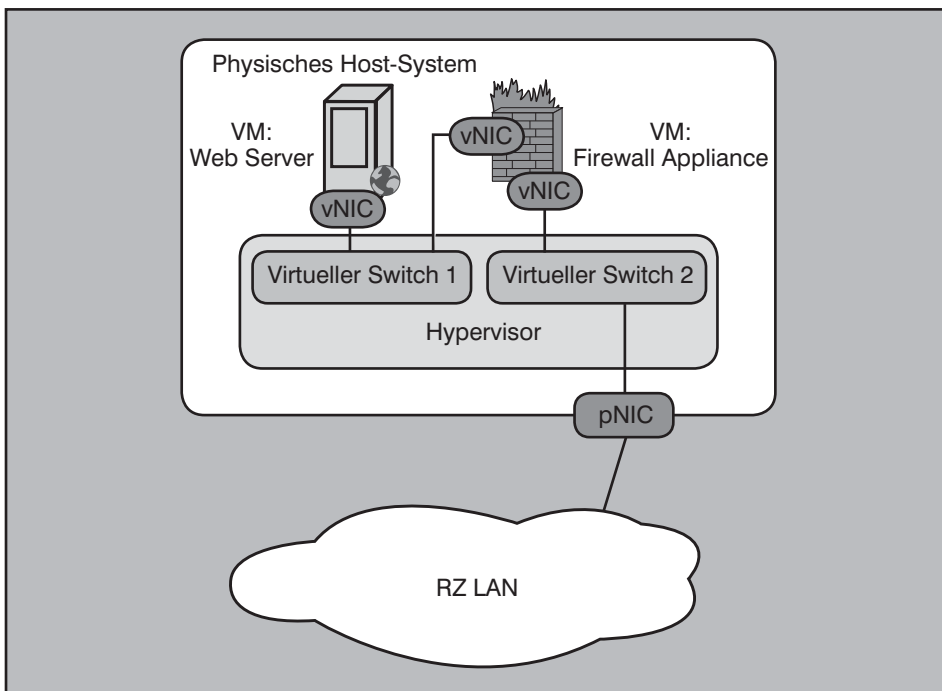


Abbildung 6: Realisierung einer DMZ mittels virtueller Switches und einer virtuellen Firewall in einer virtuellen Umgebung

Firewall übernimmt die Standby-Firewall und wechselt in den aktiven Status. Die Auswirkungen auf die Verkehrsflüsse innerhalb der Schutzzone sind marginal. Da im Layer-3-Modus betriebene Firewall-Cluster über virtuelle IPs verfügen, welche dynamisch der aktiven Firewall zugeordnet werden, muss es bei einem Schwenk lediglich zu einem Update der MAC-Tabellen auf den mit dem Cluster verbundenen

Layer-2-Komponenten kommen. Damit besteht der Unterschied bei einem Schwenk im Wesentlichen aus einem neuen Pfad, den die Pakete durch das Netzwerk nehmen. Aus logischer Sicht hingegen ändert sich nichts.

Ein solcher Hochverfügbarkeitsmechanismus muss auch von virtuellen Firewalls unterstützt werden. Auch virtuelle Fire-

Jetzt Leser werden



Der Netzwerk Insider

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat werden zwei Themen gewählt, über die in ausführlicher Form topaktuelle Insider-Informationen gegeben werden. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:

<http://www.comconsult-akademie.de/de/Registrierung.php>

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

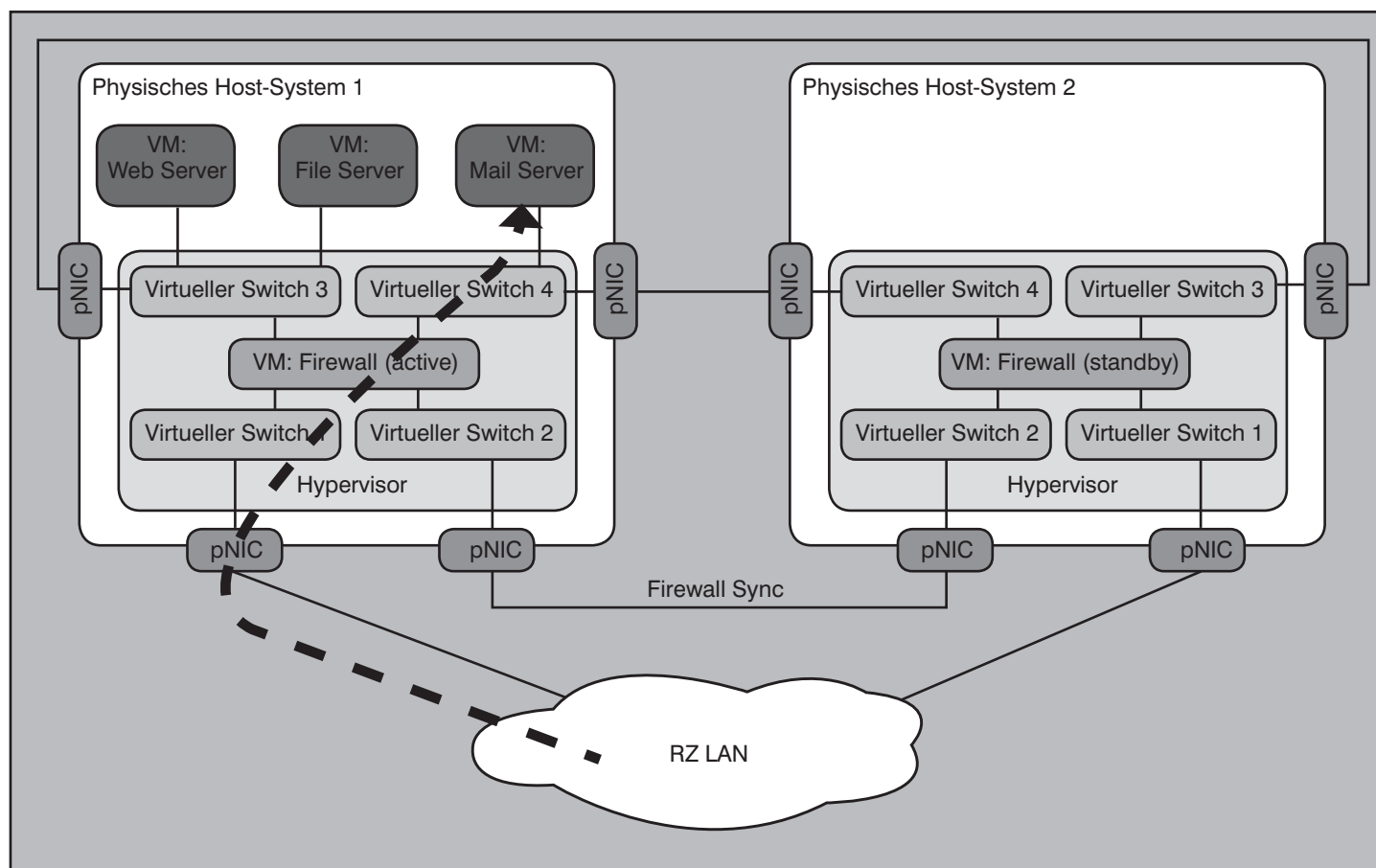


Abbildung 7: Aufbau eines redundanten Host-Systems mit redundanten virtuellen Firewalls und drei virtuellen Servern. Die virtuellen Switches 3 und 4 bilden virtuelle „Server Switches“. Die gestrichelte Linie zeigt den Kommunikationspfad zum Mail Server im Normalbetrieb.

walls müssen entweder im Active/Active- oder im Active/Standby-Modus redundant ausgeführt und auf unterschiedlichen physischen Host-Systemen zum Einsatz gebracht werden können.

Bei der Integration einer redundant ausgeführten virtuellen Firewall in die virtuelle Netzumgebung der Virtualisierungslösung ergeben sich jedoch einige Besonderheiten, die bei der Planung des physischen Netzes und der Dimensionierung der Host-Systeme zu berücksichtigen sind.

Wie in einer physischen Umgebung auch, müssen die redundanten Firewalls Statusinformationen synchronisieren und Heartbeat-Signale austauschen. Hierfür sind eine dedizierte Netzverbindung und jeweils ein virtueller Switch erforderlich. Die Außenanbindung über die physische Netzwerkschnittstelle, die mit dem Rechenzentrumsnetz verbunden ist, wird ebenfalls über einen eigenen virtuellen Switch realisiert. Die virtuellen Server werden über eigene virtuelle Switches angebunden, die sich logisch hinter der Firewall befinden. Abbildung 7 zeigt diesen Aufbau, bei dem drei virtuelle Maschinen (Web Ser-

ver, File Server und Mail Server) in zwei unterschiedlichen Servernetzen (virtueller Switch 3 und 4) durch eine virtuelle Firewall geschützt werden.

4.1 Verschiebung einzelner virtueller Maschinen

Der zweite physische Host, auf dem die redundante virtuelle Firewall installiert ist, muss mit den gleichen Netzen konfiguriert sein wie der erste Host, damit er im Fehlerfall dessen Aufgaben übernehmen kann. Genau hier liegt eines der Interferenzpotentiale mit den Eigenschaften der Virtualisierungslösung: Im Fall von VMware Virtual Infrastructure führt der HA-Cluster-Betrieb der ESX-Hosts im Fehlerfall dazu, dass sämtliche virtuelle Maschinen auf dem verbleibenden Host neu gestartet werden. Demnach würde auch die aktive virtuelle Firewall auf dem zweiten Host gestartet, obwohl dort zwischenzeitlich die redundante Firewall ihre Aufgabe übernommen hat. Dies führt nicht zwangsläufig zu einem Konflikt, wenn die neu gestartete Firewall aufgrund des Heartbeats der redundanten Firewall im Standby-Modus läuft. Dennoch ist diese HA-Eigenschaft in der Regel nicht erwünscht.

Um dieses Verhalten auf einem Zwei-Knoten-Cluster zu vermeiden, sind Priorisierungsmöglichkeiten erforderlich, wie sie etwa die Citrix XenServer Virtualisierungslösung bietet, mit der die HA-Eigenschaft je virtueller Maschine definiert und bis auf 0 reduziert werden kann. Auch unter Microsoft Hyper-V käme es nicht zu diesem Konflikt, da einzelne virtuelle Maschinen – und so auch die virtuelle Firewall – entweder als geclusterter oder nicht-redundanter Dienst eingerichtet werden können.

Ebenso müssen für virtuelle Firewalls dynamische Mechanismen zur Lastverteilung deaktiviert werden, wie z.B. VMwares Distributed Resource Scheduler (DRS). Würde aufgrund einer vorliegenden Lastsituation die virtuelle Firewall im laufenden Betrieb auf ein anderes Host-System migriert, erhielte das Rechenzentrumsnetz keine Kenntnis von der damit einhergehenden Veränderung in der netzwerkseitigen Erreichbarkeit der von der Firewall geschützten virtuellen Maschinen. Neben der zwar kurzen aber dennoch registrierbaren Downtime, die die Migration der virtuellen Firewall mit sich bringt, müssen die MAC-Tabellen der physischen RZ-Switches der

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

neuen Situation angepasst werden. Wird dies nicht durch proaktives Verhalten der verschobenen Firewall (z.B. in Form von Gratuitous ARPs) unterstützt, kommt es zu längeren Ausfällen.

Auf Cluster-Systemen mit mehr als zwei Knoten kann diesem Problem durch Konfiguration einer negativen Affinität für beide virtuelle Firewalls begegnet werden. Im Fall eines erforderlichen Umzugs bzw. Neustarts der ersten, ursprünglich aktiven Firewall sorgt dieser Mechanismus dafür, dass diese Firewall nicht auf dem gleichen Host-System gestartet wird, auf dem die redundante Firewall läuft.

Wie in Abbildung 7 dargestellt, müssen die virtuellen „Server Switches“ 3 und 4 über eine dedizierte Verbindung mit ihrem Pendant auf Seiten des zweiten Host-Systems verbunden werden. Dies hängt damit zusammen, dass neben dem betrachteten Totalausfallszenario eines Host-Systems auch der Umzug einzelner virtueller Maschinen im laufenden Betrieb möglich ist. Dieses in Abhängigkeit der Virtualisierungslösung mit „XenMotion“, „VMotion“ oder „LiveMigration“ bezeichnete Verfah-

ren führt dazu, dass der aktiv genutzte Hauptspeicherbereich einer virtuellen Maschine auf eine Nachbarmaschine umkopiert wird. Ist dieser Vorgang vollständig abgeschlossen, wird der Verweis auf den Festplattenspeicher dieser virtuellen Maschine auf diese neue Instanz umgelenkt und die Maschine läuft auf dem zweiten System weiter, während es von dem ursprünglichen Host-System entfernt werden kann. Dieser Vorgang ist nur möglich, wenn auf dem zweiten Host-System das gleiche virtuelle Netz bzw. der gleiche virtuelle Switch verfügbar ist.

Üblicherweise macht sich eine im laufenden Betrieb verschobene virtuelle Maschine nach Abschluss dieses Vorgangs in Form eines Gratuitous ARPs gegenüber der physischen Infrastruktur bemerkbar. Die physischen Switches passen daraufhin ihre MAC-Tabellen entsprechend an und die virtuelle Maschine ist fortlaufend über den neuen physischen Host erreichbar.

Da im oben beschriebenen Szenario jedoch nur die virtuelle Maschine umgezogen ist, die virtuelle Firewall sich jedoch noch auf dem ursprünglichen Host be-

findet, ist die Erreichbarkeit des virtuellen Servers immer noch nur durch das erste Host-System möglich. Die virtuelle Firewall auf dem zweiten Host-System läuft weiterhin im Standby-Modus und erlaubt insofern keinen Netzzugriff auf die umgezogene virtuelle Maschine. Wie in Abbildung 8 gezeigt, erfordert dies, dass der Zugriff über die Querverbindung der virtuellen Server Switches 4 beider Host-Systeme erfolgt. Dieser Umstand ist bei der Dimensionierung der physischen Netzwerkschnittstellen zu berücksichtigen. De facto führt er zu der Verdoppelung des Bedarfs an Netzwerkschnittstellen für die Produktivdaten: die gleiche Anzahl und Bandbreite physischer Netzwerkschnittstellen in Richtung Rechenzentrumsnetz (RZ LAN) ist auch noch einmal für diese Querverbindung der virtuellen Server Switches einzuplanen.

Daran ändert auch die logische Segmentierung einer physischen Netzwerkschnittstelle durch Nutzung von VLANs nichts, da dies nur dann ohne Performanceverlust möglich ist, wenn auch in Richtung RZ LAN die gemeinsame Nutzung der Schnittstelle durch VLAN-Bildung nicht als

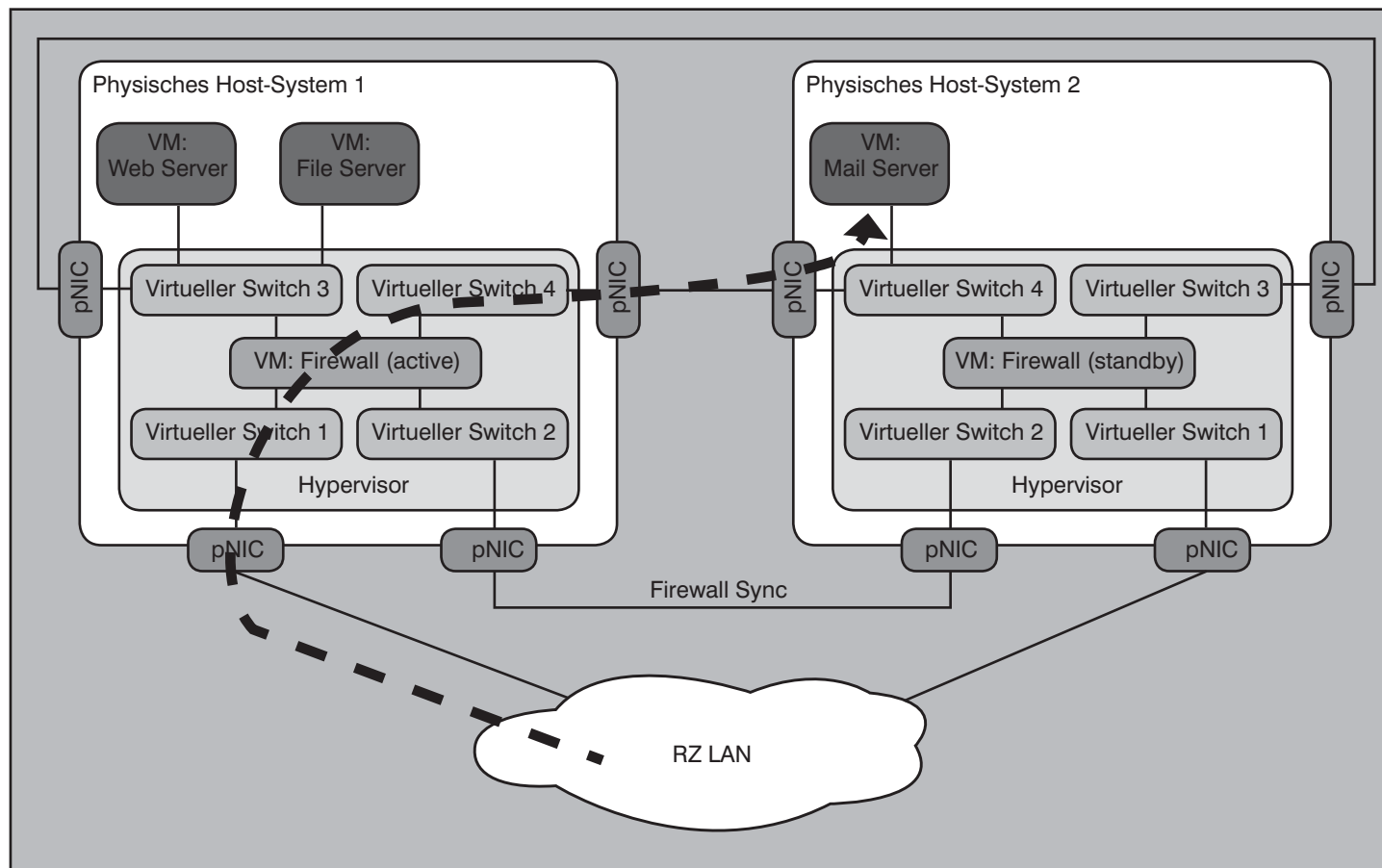


Abbildung 8: Wurde der virtuelle Mail Server im laufenden Betrieb auf den zweiten physischen Host verschoben, bleibt er aufgrund der weiterhin aktiven Firewall über den ersten Host mit dem RZ LAN verbunden. Der Verkehrsfluss wird über eine entsprechende Querverbindung seiner beiden virtuellen Server Switches 4 gelenkt.

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

„Durchsatzbremse“ betrachtet wird.

Die Anzahl physischer Netzwerkschnittstellen ist jedoch auch ohne diese Betrachtungen bereits ein kritischer Faktor bei der Planung von Server-Virtualisierungsumgebungen. So gilt die Einrichtung folgender dedizierter Netzwerkschnittstellen als „best-practice“:

- 2x Management
- 1x XenMotion / VMotion / LiveMigration
- 1x HA Cluster Heartbeat
- 1x iSCSI (sofern keine Storage-Anbindung per dediziertem HBA)
- 1x Datennetz pro Serverbereich

Da gängige rackmounted Server mit nur bis zu 8 physischen Schnittstellen ausgestattet werden können und man bei Blade-Systemen üblicherweise schon mit 6 physischen Schnittstellen an die Midplane die Grenzen der Realisierbarkeit erreicht, gilt es hier im Zuge der Planung einen geeigneten Kompromiss zu finden.

Doch auch bei geeigneter Wahl und Dimensionierung der Schnittstellen führt die wenig intuitive Änderung der Verkehrsflüsse

se nach einem Fail-Over oder dem Umzug einer virtuellen Maschine dazu, dass das Troubleshooting deutlich erschwert wird. Dies ist auch dann der Fall, wenn – wie im folgenden Abschnitt näher dargestellt – nur die virtuelle Firewall ausfällt und es zu einem Fail-Over auf die redundante virtuelle Firewall kommt.

4.2 Failover der virtuellen Firewall

Kommt es zu einer Störung innerhalb der aktiven virtuellen Firewall auf dem ersten physischen Server, erhält die redundante Firewall auf dem zweiten Host-System über die Firewall-Sync-Verbindung hier von Kenntnis und schaltet in aktiven Betrieb. Hierdurch ändert sich wie in Abbildung 9 dargestellt die Netzwerktopologie. Um eine möglichst unterbrechungsfreie Erreichbarkeit der virtuellen Maschinen zu gewährleisten, muss die virtuelle Firewall das Rechenzentrumsnetz proaktiv über diese geänderte Topologie informieren.

4.3 Virtuelle Firewalls im Active/Active-Modus

Zur Philosophie der Server-Virtualisierung gehört eine möglichst gleichmäßige Auslastung aller beteiligten Systeme. Diesem

Gedanken widerspricht der Betrieb von zwei Firewalls im Active/Standby-Modus. Dennoch ist auch in virtualisierten Umgebungen ein Active/Active-Betrieb von Sicherheitskomponenten kritisch zu hinterfragen.

Werden die virtuellen Firewalls wie oben beschrieben im Active/Standby-Modus betrieben, ergeben sich die Leistungsanforderungen aus folgenden Aspekten, damit es zu keiner Flaschenhalsituation kommt:

- Die aktive Firewall muss genügend Rechenleistung besitzen, um den Netzverkehr mit der durch die Server-Kommunikation vorgegebenen Datenrate inspizieren zu können.
- Die Netzanbindung der Firewall in Richtung Rechenzentrumsnetz muss so dimensioniert sein, dass die Bandbreite zur Kommunikation mit allen hinter der Firewall liegenden Servern ausreicht.
- Die Querverbindungen zwischen den virtuellen Server Switches müssen ebenfalls so dimensioniert sein, dass die zur Verfügung stehende Bandbreite

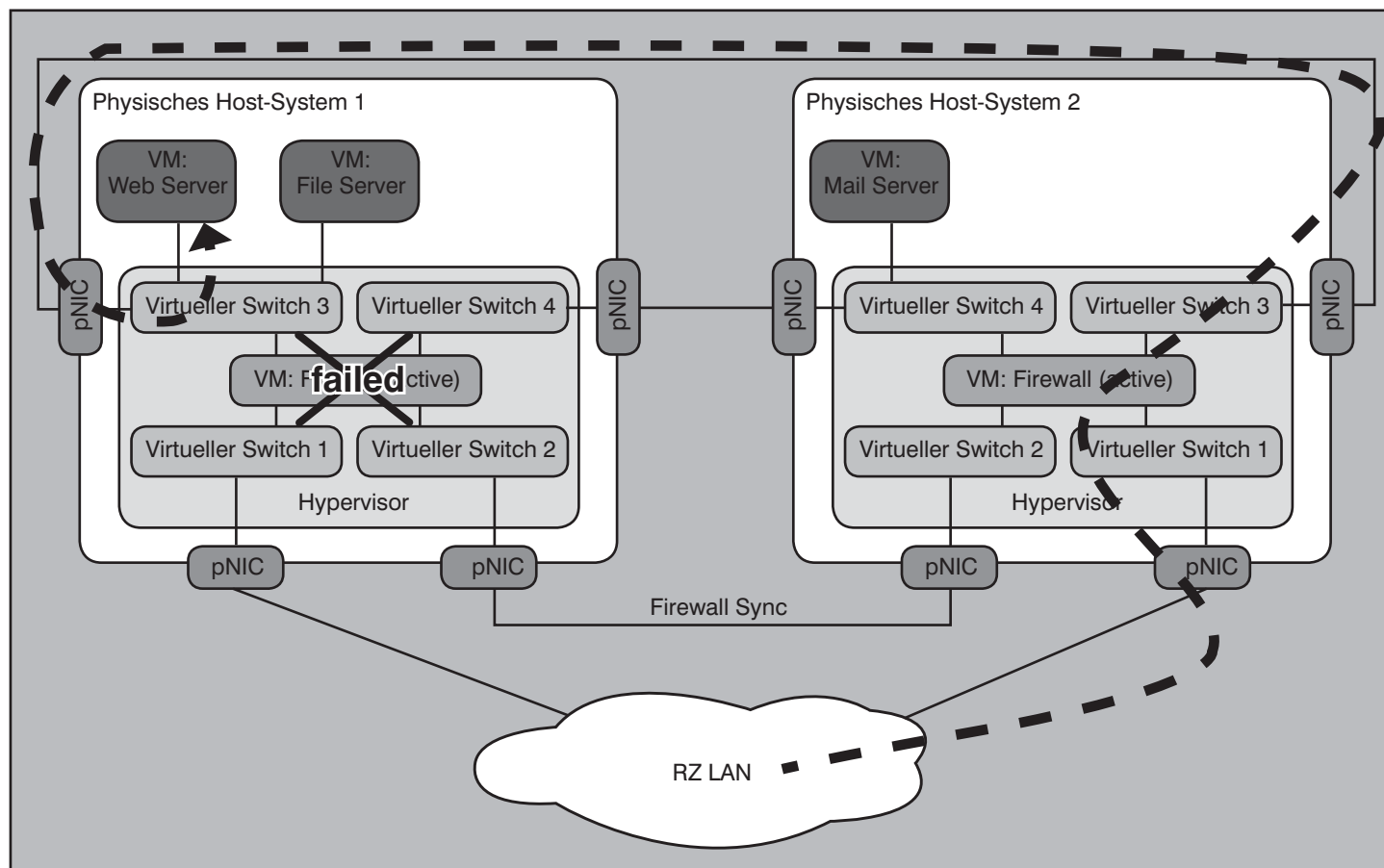


Abbildung 9: Fällt die aktive virtuelle Firewall aus, übernimmt die redundante Firewall auf dem zweiten Host-System und die Verkehrsflüsse in Richtung der virtuellen Server müssen sich entsprechend anpassen.

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

te eine ungehinderte Kommunikation zu allen Servern dieses Netzbereichs gestattet, da aufgrund der Dynamik der virtuellen Umgebung die Position einer virtuellen Maschine sich wie oben dargestellt ändern kann.

Der Active/Active-Betrieb von zwei virtuellen Firewalls ergibt für das Gesamtsystem keine Leistungsvorteile:

- Auch wenn im Normalbetrieb jede aktive Firewall nur 50% Last gegenüber dem Active/Standby-Normalbetrieb aufweist, muss das Host-System genügend Ressourcen reservieren, damit im Fehlerfall die verbliebene aktive Firewall die Rolle der ausgefallenen Firewall vollständig übernehmen kann.
- Gleiches gilt für die Dimensionierung der Schnittstellen in Richtung Rechenzentrumsnetz sowie zwischen den virtuellen Server Switches: würde sich aufgrund einer geeigneten Lastverteilung der Netzverkehr zu gleichen Anteilen auf beide Firewalls aufteilen, müssten die Schnittstellen dennoch für den Fehlerfall so dimensioniert werden, dass sie auch den gesamten Netzverkehr alleine übertragen können.

- Des Weiteren kann keinesfalls garantiert werden, dass die jeweilige aktive Firewall nur die Server schützt, die sich auf dem gleichen Host-System befinden. Die virtuellen Maschinen des geschützten Netzbereichs befinden sich im gleichen Servernetz und ihre physische Lokation unterliegt weiterhin den genannten dynamischen Prozessen.

- Besteht das Host-System aus mehr als 2 Cluster-Knoten und erstreckt sich der von den virtuellen Firewalls geschützte Server-Bereich ebenfalls über mehr als 2 Knoten, kommt es zwangsläufig zu Host-System-übergreifender Netzkomunikation über die Querverbindungen der virtuellen Server Switches.

Der Active/Active-Betrieb der virtuellen Firewalls bringt dem gegenüber die gleichen Nachteile mit sich, wie sie auch von physischen Firewalls her bekannt sind: die Komplexität steigt dadurch, dass sitzungsspezifische Informationen wechselseitig ausgetauscht werden müssen. Die Kommunikationswege sind nicht mehr deterministisch und der Antwortweg einer Sitzung kann sich vom Pfad der Anfrage unterscheiden. Insofern wird auch im virtuellen Umfeld ein Active/Active-Betrieb von Firewalls nicht empfohlen.

4.4 Virtuelle Firewalls auf Host-System-Clustern aus mehr als 2 Knoten

Besteht die physische Server-Umgebung aus mehr als zwei Host-Systemen ist nicht nur die Konfiguration der virtuellen Switches überall einheitlich vorzunehmen, sondern auch überall eine Verbindung der virtuellen Switches erforderlich, die zum gleichen VM-Servernetz gehören. Dies mag den Einsatz zusätzlicher physischer Switches erforderlich machen, die diese Verbindungen pro virtuellem Server-Switch-Typ aufnehmen. Wie aus Abbildung 10 hervorgeht, wird die Netztopologie durch diese Firewall-Architektur und die ggf. zusätzlichen Layer-2-Switches deutlich verkompliziert.

5. Management der virtualisierten Umgebung

An dieser Stelle kommt eine weitere Herausforderung ins Spiel: das Management dieser virtualisierten Umgebung. Während das Managementsystem für die virtuellen Firewalls identisch mit demjenigen für physische Firewalls ist und für die virtuellen Maschinen ebenfalls leistungsfähige Managementsysteme als Teil der Virtualisierungslösung erhältlich sind, gibt es derzeit kein Werkzeug, mit dem das entstandene Datennetz einheitlich und über-

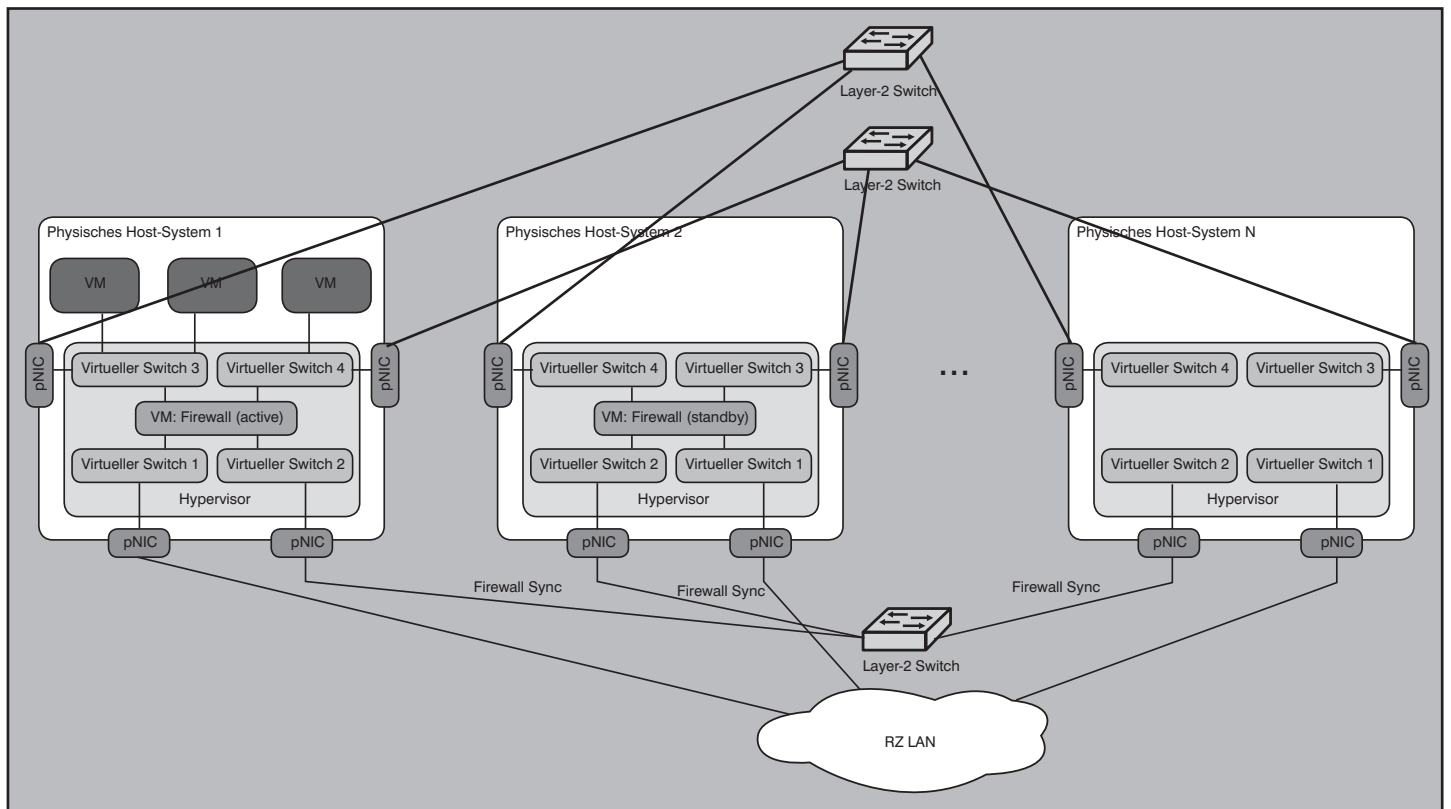


Abbildung 10: Bei mehr als 2 physischen Host-Systemen werden zusätzliche Layer-2 Switches erforderlich, die die zusammengehörenden virtuellen Server Switches sowie die Switches für den Firewall Sync mit einander verbinden.

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

sichtlich administriert werden könnte.

Abbildung 11 stellt das Beispiel einer logischen Darstellung der Netzwerktopologie innerhalb eines Host-Systems inkl. virtueller Firewall ihrer Repräsentation im VMware Managementsystem „Virtual Center“ gegenüber. Weder der Zusammenhang zwischen den virtuellen Switches noch die Tatsache, dass es sich jeweils um die gleiche virtuelle Firewall an den virtuellen Switches handelt, wird deutlich. Hier ist dringend eine übergreifende Managementlösung gefragt, die sowohl das physische als auch das virtuelle Netzwerk inkl. virtueller Netzkomponenten einheitlich darstellt.

Da die Virtualisierung von Servern als ein wesentliches Ziel die optimierte Ausnutzung von physikalischen Ressourcen hat, gehören Mechanismen zu der Virtualisierungslösung, die die Verlagerung einzelner virtueller Maschinen auf andere Server im laufenden Betrieb ermöglichen. Schon bei Verwendung von getrennt betriebenen Sicherheitskomponenten stellt dieses Verhalten eine Herausforderung für die Sicherheit dar. Bei jeder Bewe-

gung der virtuellen Maschinen von einem physischen Server zum nächsten muss sichergestellt sein, dass die virtuelle Maschine nach Umzug wieder im gleichen Sicherheitskontext zu finden ist. Dies ist jedoch weniger eine technische, als vielmehr eine menschliche Herausforderung, da hier die Auswirkungen von versehentlich falscher Konfiguration den Server in das falsche VLAN und damit auch in den falschen Sicherheitskontext setzen kann. Auch an dieser Stelle ist also eine ganzheitliche, übersichtliche Managementumgebung gefragt.

6. Verteilte virtuelle Switches

Im vorangehenden Abschnitt wurde dargestellt, dass für Umzüge von virtuellen Maschinen im laufenden Betrieb und für eine konsistente Integration redundanter virtueller Firewalls die gleiche Netztopologie in den Host-Systemen vorliegen muss. Da die Managementsysteme der gängigen Virtualisierungslösungen in dieser Hinsicht wenig Transparenz bieten, ist der manuelle Weg dieser Konfiguration bei zahlreichen Hosts nicht nur sehr aufwendig, sondern auch äußerst fehl-

erträchtig. Abhilfe schaffen kann hierbei z.B. eine Skript-gesteuerte Konfiguration der virtuellen Switches.

VMware bietet mit dem unter dem Namen „vSphere 4“ erschienenen neuen Release seiner Virtualisierungslösung sogenannte „Distributed Virtual Switches“ an, um diesem Problem zu begegnen. Die Idee hierbei ist, dass nicht mehr einzelne virtuelle Switches je Host-System konfiguriert werden müssen, sondern dass sich die virtuellen Switches über den gesamten Host-System-Cluster erstrecken. Abbildung 12 zeigt, wie sich zumindest die logische Darstellung dieser Architektur inkl. virtueller Firewalls dadurch vereinfacht. Es bleibt jedoch fraglich, ob diese verteilten virtuellen Switches aus mehr als einem Perl-Skript bestehen, die deren Konfiguration auf allen Host-Systemen vereinheitlichen. So ist z.B. unklar, ob in diesem Konzept die Kommunikation zwischen den einzelnen virtuellen Switch-Segmenten, die sich auf unterschiedlichen Hosts befinden, aber dem gleichen verteilten virtuellen Switch zugeordnet sind, vorgesehen ist und über welche physischen Verbindungen dieser Da-

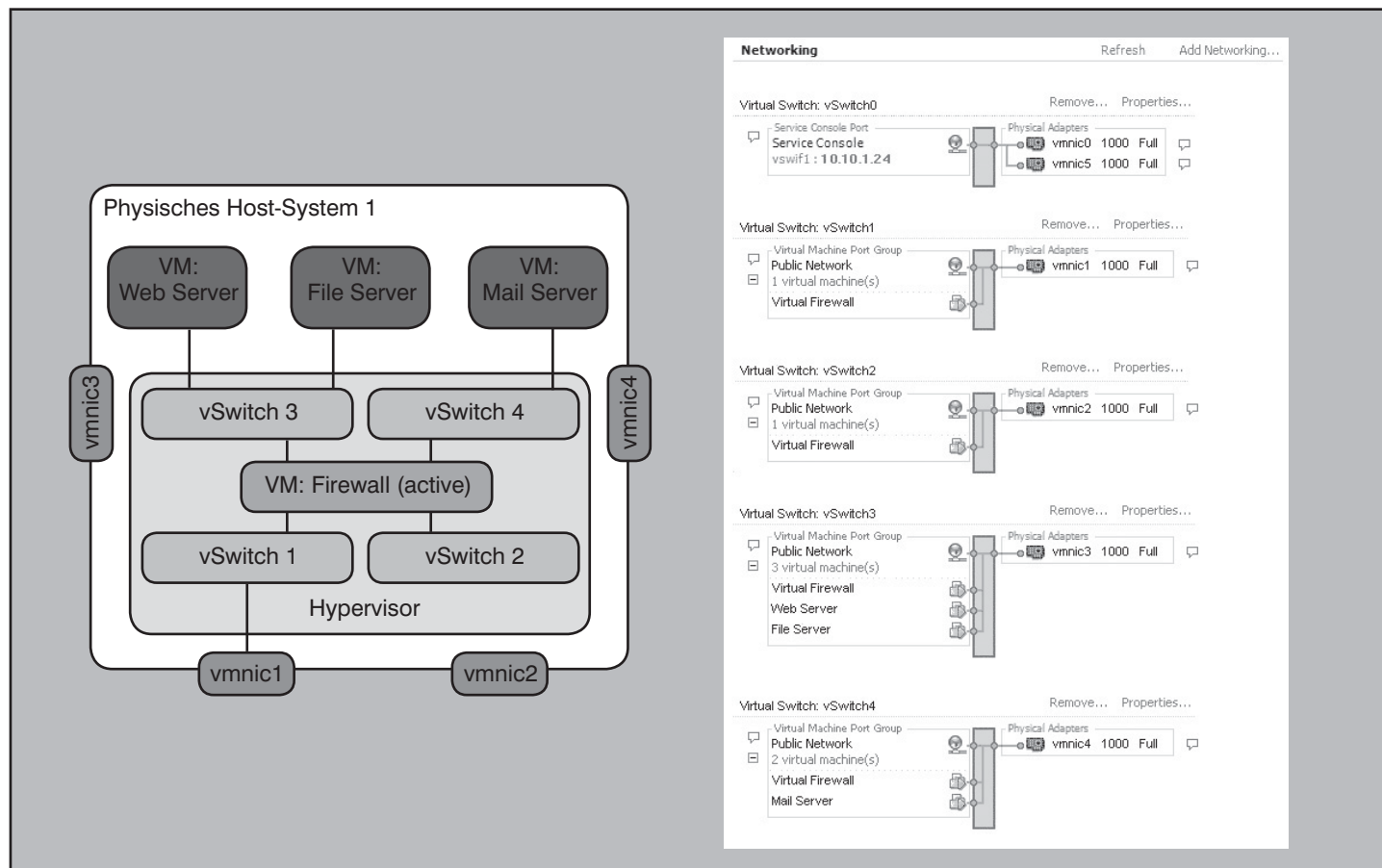


Abbildung 11: Logische Darstellung der virtuellen Netzwerktopologie eines Host-Systems inkl. virtueller Firewall (links) und die Darstellung in der VMware Managementumgebung Virtual Center (rechts).

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

tenverkehr dann stattfindet (vgl. z.B. die dedizierte Verbindungen zwischen den virtuellen Switches 4 beider Hosts in Abbildung 7). Gerade im Failover-Fall der virtuellen Firewall oder beim Verschieben von virtuellen Maschinen kommt der Beantwortung dieser Frage auch in dieser Architektur eine hohe Bedeutung zu.

7. Technische Einschränkungen beim Einsatz von virtuellen Firewalls

Betrachtet man die Umstände, die mit der Virtualisierung von Firewalls einhergehen, genauer, zeigen sich auch technische Einschränkungen, die mit diesem Ansatz einhergehen. Zunächst sei herausgestellt, dass einer virtuellen Firewall in der Regel nicht dediziert die Gesamtleistung des Host-Systems zur Verfügung steht, wie es bei einer physischen Appliance der Fall ist. Die Firewall muss sich die verfügbare Hardware-Leistung wie beispielsweise CPU, RAM und Netzwerkdurchsatz mit den anderen virtuellen Maschinen teilen. Damit ist klar, dass eine virtuelle Firewall nur dann die gleiche Leistung bringen kann wie die gleiche Software auf einer Appliance, wenn – neben der identischen Hardware-Ba-

sis – bis zu 100% der Ressourcen von der Firewall beansprucht werden dürfen.

Ab einer gewissen zu erwartenden Durchschnittslast, die von der virtuellen Firewall verursacht wird, widerspricht es allerdings dem ursprünglichen Virtualisierungsgedanken – nämlich eine möglichst hohe Konsolidierungsrate zu erzielen –, wenn virtuelle Firewall und virtuelle Server auf dem gleichen Host-System betrieben werden. Müssen z.B. 50% der Host-Ressourcen der virtuellen Firewall zur Verfügung stehen, können nur noch halb so viele virtuelle Server auf diesem Host betrieben werden, als wenn man die Firewall als dedizierte physische Appliance realisiert hätte.

Abhängig von den weiteren virtuellen Maschinen, die auf dem physischen System betrieben werden, ergeben sich außerdem schwer vorhersehbare Lastprofile für die Performance. Dies führt zu einer weiteren Beschränkung des Einsatzbereiches einer virtuellen Firewall gegenüber ihrem physischen Pendant. So wird klar, dass eine Virtualisierung der Firewall umso weniger erstrebenswert ist, je größer ihre eigenen Leistungsanforderungen sind.

Die Virtualisierung setzt letztlich auf einem Stück Software, dem Hypervisor, auf. Sicherheitsschwächen im Hypervisor betreffen somit auch unweigerlich alle virtuellen Systeme und daher ebenso die virtuelle Firewall. Gerade an Sicherheitskomponenten bestehen in der Regel besondere Anforderungen hinsichtlich ihres Betriebs in einer gehärteten Umgebung. Diese Tatsache ist daher in die Entscheidung für oder gegen eine virtuelle Firewall mit einzubeziehen.

Um einem virtuellen Gesamtsystem umfassenden Schutz zu geben, reicht daher eine virtuelle Firewall, die wie ein weiterer virtueller Server einfach an den virtuellen Switch gebunden wird, oftmals nicht aus. Vielmehr muss es einen Schutzmechanismus geben, der tiefer in die virtuelle Infrastruktur eingreift.

7.1 VMsafe

Der Hersteller VMware hat die genannten Grenzen von virtuellen Firewalls zum Anlass genommen, die Thematik der Bildung von Sicherheitszonen zu überarbeiten. Mit der aktuellen Version vSphere 4.0 als Nachfolger von Virtual Infrastructure 3 ste-

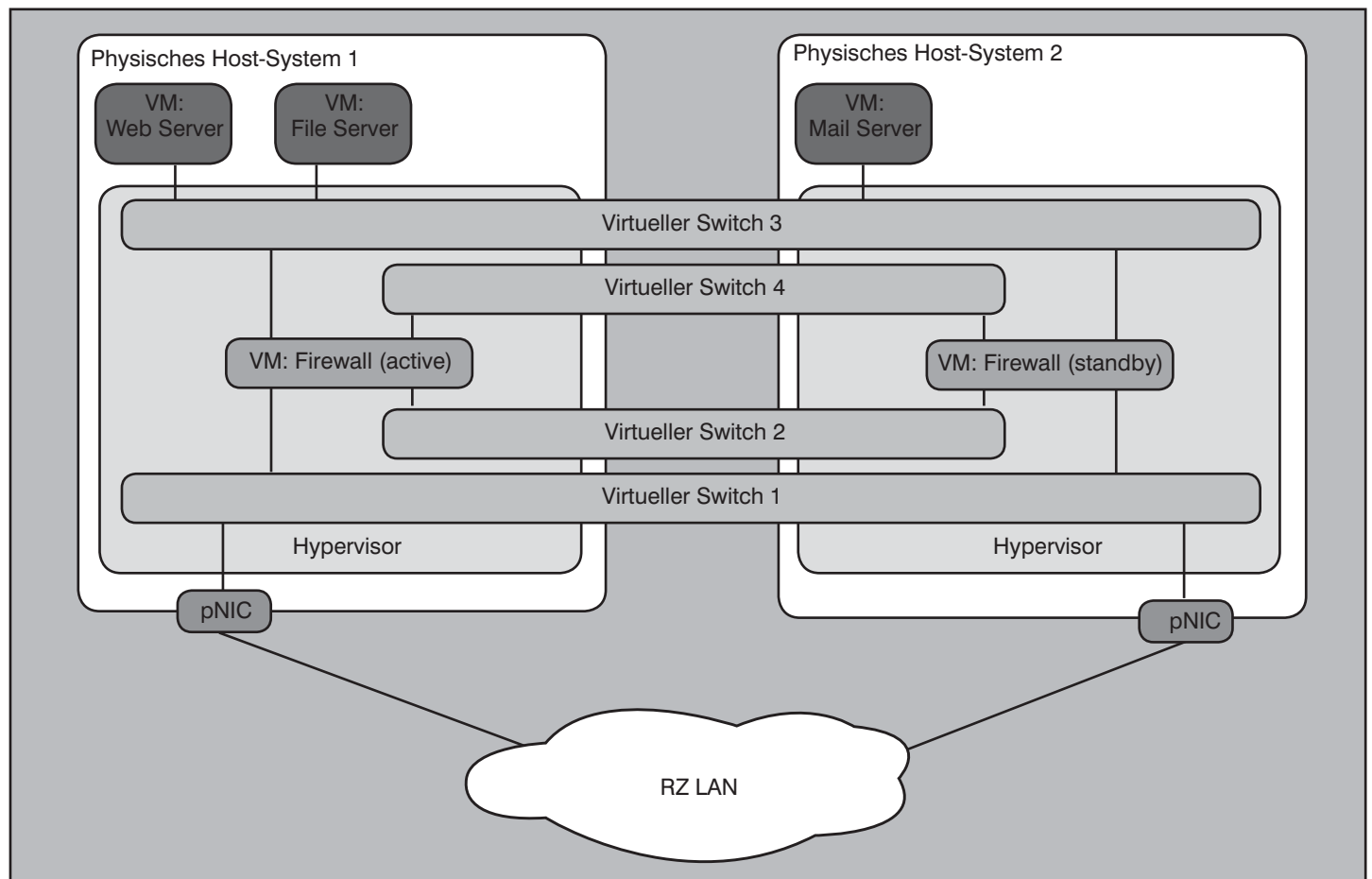


Abbildung 12: Logische Netztopologie von zwei Host-Systemen mit virtuellen Firewalls bei Einsatz von verteilten virtuellen Switches

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

hen zwei Neuerungen an, welche insbesondere in Hinblick auf virtuelle Firewalls relevant sind: VMware vShield Zones und VMware VMsafe.

VMware VMsafe stellt eine Schnittstelle innerhalb des VMware Hypervisors dar, über welche der Zugriff auf CPU, Arbeitsspeicher, Massenspeicher und Netzwerk der virtuellen Maschinen erfolgen kann. Im Gegensatz zu bisherigen virtuellen Firewall-Produkten, welche in der Regel nur aus der Firewall-Software in einer virtuellen Maschine anstatt auf physischer Hardware bestehen, berücksichtigt diese Schnittstelle Spezifika der Virtualisierung. Der Zugriff der VMsafe-kompatiblen Systeme (z.B. einer virtuellen Firewall) erfolgt vollkommen transparent, d.h. eine Änderung der virtuellen Netztopologie ist nicht erforderlich.

Dies erlaubt u.a. folgende Einsatzmöglichkeiten:

- Erkennung von schadenstiftender Software ohne Installation eines separaten Agenten.

Hierdurch ist z.B. eine zentrale Anti-Virus-Erkennung mittels einer VMsafe-kompatiblen VM anstatt der Installation eines Agenten in jeder VM möglich. Dies schont zum einen die Ressourcen, zum anderen kann auf diese Weise keine Schadsoftware den Agenten innerhalb der VM deaktivieren.

- Kontrolle des ein- und ausgehenden Netzwerkverkehrs mittels Paketfilter/ IDS/ IPS

Auf Basis eines dynamischen Paketfilters kann ein- und ausgehender Verkehr virtueller Maschinen kontrolliert werden. Aber auch eine Spiegelung des Verkehrs einzelner TCP/IP-Ports auf ein externes System ist möglich. Ein Beispiel ist die Spiegelung von HTTP-Verkehr auf ein IDS-System zur weiteren Analyse. Die Regeln können dabei auf verschiedenen Ebenen greifen. Auf Basis einer VM, einer Gruppe von VMs oder global. So könnte beispielsweise eine globale Standardregel für alle VMs lauten, dass eingehender Verkehr blockiert wird. Ebenso lassen sich IDS/IPS-Systeme transparent in die virtuelle Infrastruktur einbinden.

Auf der anderen Seite gibt es auch Kritikpunkte bezüglich VMsafe:

- Der Zugriff auf die Schnittstelle wird von VMware kontrolliert. Im Rahmen eines Review-Prozesses muss der potentielle Partner Details zur Verwendung und seine Absichten darlegen. Letztend-

lich entscheidet VMware, ob dieser zur Nutzung berechtigt ist. Dem gegenüber bieten offene Schnittstellen wie etwa unter XenServer deutliche Vorteile.

- Die Integration zusätzlicher Funktionalität in den Hypervisor erhöht das Risiko von Softwarefehlern und damit die Gefahr von Schwachstellen. Die erfolgreiche Kompromittierung der VMsafe-Schnittstelle entspricht prinzipiell der Kompromittierung des Gesamtsystems.

Generell erfordert die VMsafe API jedoch entsprechende Neuentwicklungen von Produkten, damit diese die neuen Funktionen auch nutzen können.

7.2 VMware vShield Zones

Eine weitere Option für Kunden und Hersteller ist die Nutzung von VMware vShield Zones.

Mittels der Software-Option VMware vShield Zones (ab vSphere Advanced Edition) ist es innerhalb der virtuellen Umgebung möglich, verschiedene Sicherheitszonen zu bilden. Die Grundlage hierfür bildete das Produkt VirtualShield der Firma Blue Lane, welche VMware 2008 übernommen hat. Über eine separate VM (vShield Zones VA) je physischem Server und eine Management-VM (vShield Zones Manager) können verschiedene Sicherheitszonen auf Basis einer gemeinsamen physischen Infrastruktur gebildet werden. Dies ermöglicht beispielsweise das Erstellen von Firewall-Regeln je VM, Switch oder Cluster. Ebenso wird der Sicherheitskontext einer VM bei Nutzung von z.B. vMotion beibehalten. Die Konfiguration und das Management sind hierbei in die VMware-

Management-Werkzeuge (vCenter Server) integriert. Derzeit befinden sich die vShield Zones noch in einer privaten Beta-phase, so dass derzeit keine detaillierten Infos oder Erfahrungswerte diesbezüglich vorliegen.

8. Tests

Wie für die gesamte Virtualisierungstechnologie gilt auch und gerade für den Sicherheitsbereich, dass ausgiebige Tests unerlässlich sind. Während virtualisierte Firewalls bereits vielfältig erfolgreich genutzt werden und ihr Einsatz nur geringen Einfluss auf die Kommunikationsflüsse hat, müssen beim Einsatz von virtuellen Firewalls die dynamischen Prozesse der virtuellen Umgebung ausgiebig untersucht werden.

Des Weiteren ist das Lastverhalten der virtuellen Firewall in einer Testumgebung mit möglichst realistischen Datenaufkommen zu analysieren. Anhand der von der Firewall angeforderten Systemressourcen ist zu entscheiden, ob eine virtuelle Lösung dienlich ist.

9. Fazit und Ausblick

Die Verwendung von virtuellen Firewalls hat insbesondere beim redundanten Einsatz enormen Einfluss auf die logische Netztopologie und die Verkehrsflüsse innerhalb einer virtualisierten Umgebung. Die marktgängigen Managementlösungen bieten derzeit noch keine ausreichende Unterstützung, um das physische und virtuelle Netzwerk sowie die darin befindlichen virtuellen Sicherheitskomponenten ganzheitlich zu überwachen und somit für

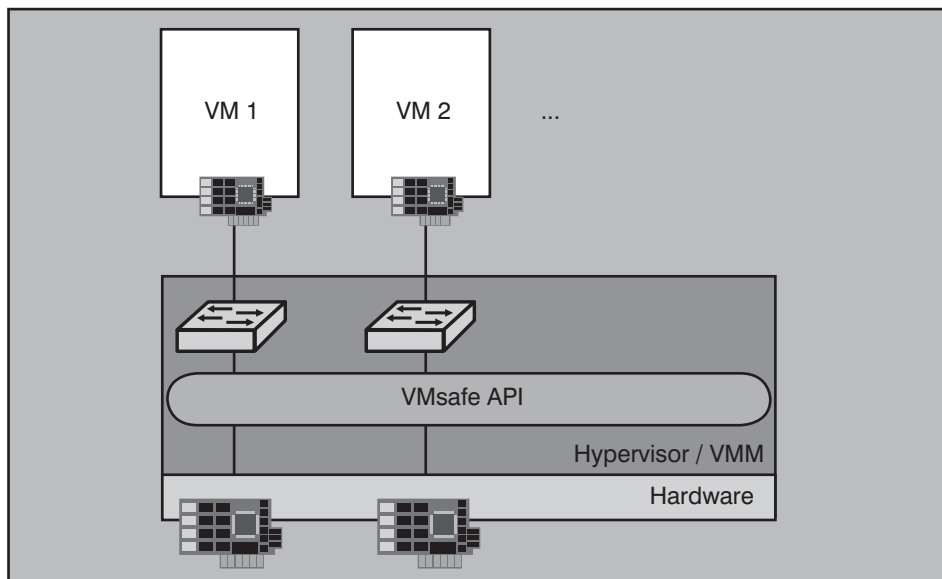


Abbildung 13: VMsafe API innerhalb des VMware Hypervisors

Virtualisierung: Mehr Sicherheit durch virtuelle Firewalls?

das erforderliche Sicherheitsniveau des Gesamtsystems zu sorgen.

Insofern ist die Eignung virtueller Firewalls für die Segmentierung eines Rechenzentrumsnetzes in unterschiedliche Sicherheitszonen als fraglich zu betrachten. Ihr Einsatz ist eher prädestiniert, um einzelnen Serversystemen, die nur eine eingeschränkte Dynamik besitzen, einen zusätzlichen Schutz zu bieten.

Für darüber hinaus gehende Anforderungen sind neue Konzepte gefragt. Ob diese in Form von VMwares VMsafe API und den vShield Zones realisiert werden, bleibt bei Verfügbarkeit dieser Produktmerkmale näher zu untersuchen.

10. Abkürzungen

API	Application Programming Interface	OVF	Open Virtual File Format
ARP	Address Resolution Protocol	pNIC	physical NIC
ASIC	Application Specific Integrated Circuit	QoS	Quality of Service
CPU	Central Processing Unit	RAM	Random Access Memory
DMZ	Demilitarized Zone, Demilitarisierte Zone	RZ	Rechenzentrum
DRS	Distributed Resource Scheduler	STP	Spanning Tree Protocol
HA	High Availability	TCP	Transmission Control Protocol
HBA	Host Bus Adapter	UTM	Unified Threat Management
HTTP	Hypertext Transfer Protocol	VHD	Virtual Hard Disk
IDS	Intrusion Detection System	VLAN	Virtual LAN
I/O	Input / Output	vNIC	virtual NIC
IP	Internet Protocol	VM	Virtual Machine, Virtuelle Maschine
IPS	Intrusion Prevention System	VMDK	Virtual Machine Disk Format
iSCSI	internet Small Computer System Interface	VPN	Virtual Private Network
LAN	Local Area Network		
MAC	Media Access Control		
NIC	Network Interface Card		
OSI	Open Systems Interconnection		

Jetzt Leser werden



Der Netzwerk Insider

In Zusammenarbeit zwischen ComConsult Technology Information Ltd und der ComConsult Technologie Information GmbH wird monatlich „Der Netzwerk Insider“ veröffentlicht, der sich mittlerweile mit über 15.000 eingetragenen Lesern zu einem der führenden deutschen Technologie-Magazine entwickelt hat. Der Netzwerk-Insider vertritt die Sichtweise von Technologie-Anwendern und bewertet Produkte und Technologien im Sinne der wirtschaftlichen und erfolgreichen Umsetzbarkeit in der täglichen Praxis. Durch seine strenge wirtschaftliche Unabhängigkeit (keine Hersteller-Anzeigen) kann er es sich leisten, Schwachstellen und Nachteile offen anzusprechen. Der Netzwerk-Insider ist bekannt für seine kritische, herstellerneutrale und fundierte Technologie-Bewertung.

Der Netzwerk Insider erscheint 12 Mal im Jahr im PDF-Format und informiert Sie per eMail über die Hintergründe aktueller Netzwerk-Technologien. Jeden Monat wird ein Schwerpunkt-Thema gewählt, über das in ausführlicher Form topaktuelle Insider-Informationen gegeben wird.

Der Netzwerk Insider liefert Ihnen:

- herstellerneutrale und kritische Informationen zu Netzwerk-Technologien aus dem Blickwinkel des Anwenders. Wir wollen klarstellen, ob eine neue Technik für den Anwender wirklich mit Vorteilen verbunden ist und ob sich der Einsatz lohnt.
- Bewertung der entstehenden Betriebsaufwände neuer Technologien. Wir wollen weg von der Anbetung von Technologie-Götzen hin zu einer Kosten-Nutzen-orientierten Betrachtungsweise, die auch den Betrieb einer Technik einbezieht.
- Informationen auf dem neuesten Stand der Technik sobald sie für den Anwender relevant sind mit dem Insider-Wissen führender Netzwerk-Spezialisten. Zum richtigen Zeitpunkt in die richtige Netzwerk-Technik investieren, Fehlentwicklungen vermeiden.
- Konzentration auf technische Schwerpunkt-Themen, um neue Entwicklungen ausführlich und tiefgehend beschreiben zu können.
- Ergebnisse von Produkt- und Praxistests durch ComConsult Research

Hier können Sie sich zum Netzwerk Insider kostenlos und ohne jede Verpflichtung registrieren lassen:
<http://www.comconsult-akademie.de/de/Registrierung.php>