

Sonderdruck für Network Performance Channel

Netzwerkanalyse und Monitoring

Virtuelle Systeme überwachen

Energieverbrauch bestimmen

Mit Marktübersicht

Monitoring-Tools/Protokollanalyatoren



Datenverkehr in virtuellen Switches analysieren

Sensoren im Unsichtbaren



In diesem Jahr setzen die Betreiber laut einer aktuellen Gartner-Studie zum ersten Mal mehr Server als virtuelle Maschinen auf denn als physische Geräte aus Blech und Silizium. Die Konsolidierung mehrerer Einzelsysteme zu einem zentralen System birgt zwar große Einsparpotenziale, bringt aber auch eine Reihe unerwünschter Nebenwirkungen bei der Analyse mit sich – Stichwort „Invisible Traffic“. Die Folge ist ein erhöhter Aufwand bei der Netzwerksicherheit und bei der Performance-Überwachung.

Virtuelle Umgebungen kommunizieren intern über aus Software gebildete Switches und Netzwerkkarten. Der Netzwerkverkehr darüber ist für herkömmliche Analysewerkzeuge vor dem Virtualisierungs-Host unsichtbar. Einige der Abläufe innerhalb der virtuellen Switches erschweren die Auswertung zusätzlich, selbst wenn man beispielsweise einen Sniffer innerhalb einer virtuellen Maschine (VM) installiert. So ist der Promiscuous-Mode per Default abgeschaltet, das heißt, VMs können keinen Unicast-Traffic zu anderen Nodes im Netz sehen. Virtuelle Switches von VMware sind zudem in der Lage, Netzwerk-Traffic von Knoten zu unterbinden, die vorgeben, von anderen Netzknoten zu kommen (Forged Transmit Blocking). Schwachstellen oder aktive Schadsoftware können dadurch unentdeckt bleiben, und die Fehlersuche ist erschwert. Auch wenn Anwender Statistikdaten zum Netzwerkaufkommen verlangen oder rechtlich sensible Inhalte zu untersuchen sind, verursacht die abgeschlossene Welt der inter-virtuellen Kommunikation Probleme.

Der Hypervisor – Einblick in die virtuelle Schaltzentrale

Längst sind die virtuellen Switches in puncto Funktionsumfang an ihre physischen Vorbilder herangewachsen. Durch ihre Position innerhalb des Hypervisors des Virtualisierungs-Hosts verfügen sie jedoch über erheblich weitreichendere Möglichkeiten, als sie ein „echter“ Switch bieten könnte. Über die direkte Verbindung zum Hypervisor „weiß“ der Switch mehr als ein physisches Gerät. So muss er nicht erst die MAC-Adressen, Unicast-Adresse oder Multicast-Gruppenteilnehmer der VMs lernen. Diese Informationen erhält er direkt vom Hypervisor. Weil Da-

tentransfers im RAM stattfinden, haben Geschwindigkeits- und Duplex-Einstellungen keine „realen“ Auswirkungen. Es gibt daher auch keine Kollisionen und Signalisierungsfehler wie beim physikalischen Ethernet. Wie lässt sich der Datenverkehr innerhalb des Hypervisors dann aber konkret abgreifen? Falls es durch die Richtlinien des Hosts erlaubt ist, kann man einzelne Ports an einem virtuellen Switch in einen Mirror-Modus versetzen. Ebenfalls möglich ist das Kopieren aller Pakete auf einen Mirror-Port, also klassische SPAN-Funktionalität. Allerdings belastet diese Funktion den virtuellen Switch nicht unerheblich und je nach Auslastung der physischen Hardware können Pakete verloren gehen.

Die andere Variante, um Einblick in den Netzwerkverkehr innerhalb des Hypervisors zu erlangen, wäre es, Probes innerhalb jeder VM zu installieren, die ihre Daten an eine zentrale Monitor-Konsole weiterreichen. Dies ist jedoch aus mehreren Gründen problematisch. Zum einen sind in Produktivsystemen keine Änderungen an den VMs erwünscht, die die CPU zusätzlich belasten und Störungen durch zusätzliche Prozesse verursachen könnten. Zudem müssen die Daten aus dem Virtualisierungs-Host zur Monitor-Konsole gelangen. Dies belastet entweder die Bandbreite des Netzwerks oder erfordert weitere virtuelle und physische Netzwerkkarten für ein separates Analysesegment. Des Weiteren sind virtuelle Maschinen keine statischen Objekte wie physische Server. Je nach Anforderungen der Benutzer, Auslastung des Hosts und aktueller Situation lassen sich die VMs zwischen den Hosts verschieben, oft automatisch ohne Zutun des Administrators. In so einem Fall ändern sich die Zuordnungen der virtuellen Ports, was für den

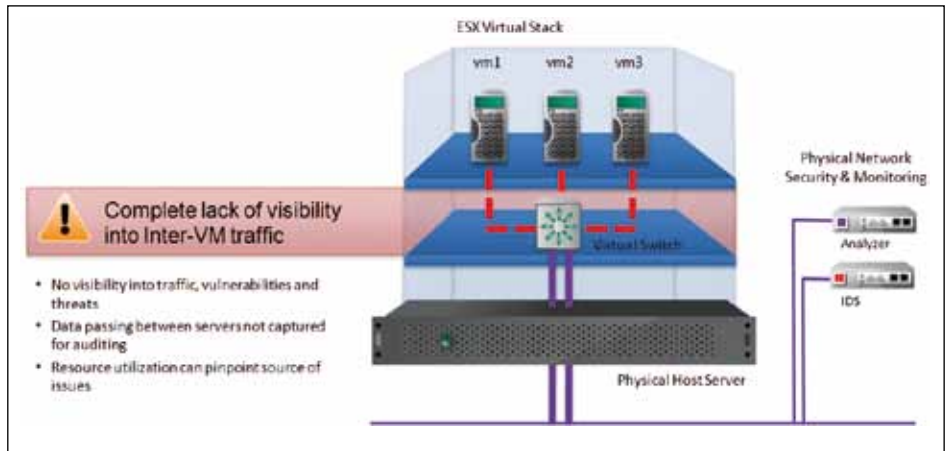


Bild 1. Netzwerkverkehr, der zwischen virtuellen Maschinen abläuft, ist mit herkömmlichen Netzwerkanalyselösungen nicht greifbar.

Hypervisor kein Problem ist, Analyse-Software innerhalb der VM aber durcheinanderbringen würde.

Analog zu Test Access Ports (TAPs) aus der physischen Welt gibt es mittlerweile auch TAP-Software, die innerhalb des Hypervisors arbeitet. Ein TAP ist in die Netzwerkleitung eingeschleift und stellt die durchfließenden Pakete an einem dedizierten Highspeed Port zur Verfügung. Software-TAPs, wie sie beispielsweise Net

Optics mit dem Phantom Monitor für VMware anbietet, sind im Hypervisor unterhalb des virtuellen Switches positioniert. Ein solcher TAP ermöglicht die Replizierung sämtlichen Netzwerkverkehrs innerhalb des virtuellen Switches, erlaubt die Anwendung von Filtern und kann die kopierten Daten auch auf einem dedizierten physischen Netzwerk-Interface ausgeben. Dabei generiert das System auch Netflow-Daten, sodass die Informationen in ein be-

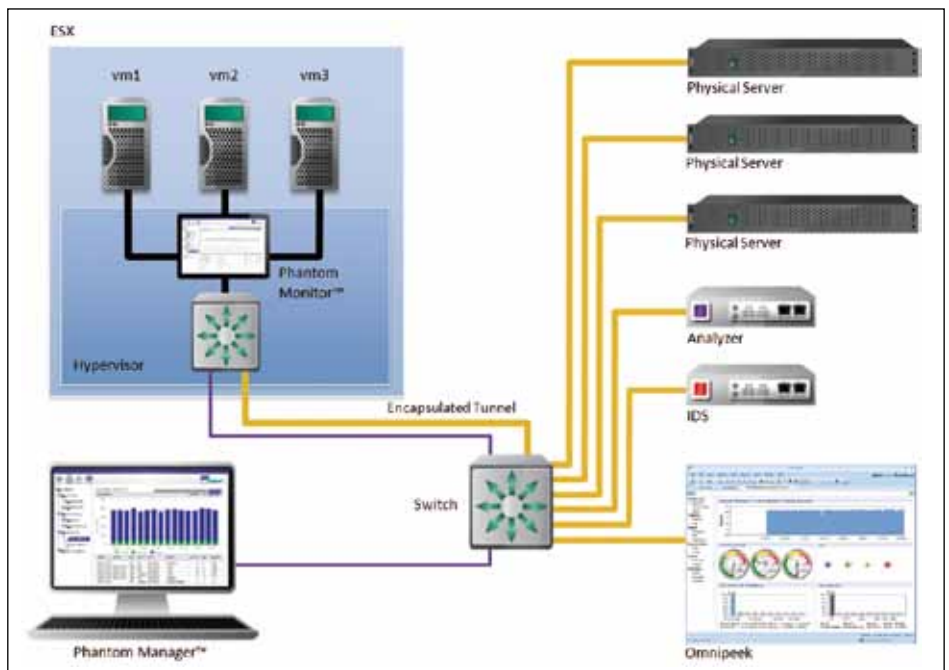


Bild 2. Blick hinter die „virtuellen“ Kulissen.

stehendes Management-Framework integrierbar sind.

Wichtig ist, dass der TAP die VMs eindeutig identifiziert, auch wenn diese beispielsweise mit VMotion zwischen physischen Hosts verschoben werden. Phantom Monitor kann den VMotion-Aktivitäten folgen und liefert auch nach einem Umzug der VM an einen anderen Standort nach wie vor die korrekten Daten. Gerade in größeren Umgebungen mit vielen Hosts ist es

im Netzwerk transportieren. Die Analyse kann dadurch an jedem beliebigen Rechner erfolgen, der dazu vorgesehen ist. Dazu verpackt das virtuelle TAP die Daten in einen GRE-Tunnel und sendet den Traffic über eine physische Netzwerkschnittstelle an die Netzwerkkarte des Analyse-Systems. Den GRE-Tunnel terminiert der Messrechner, und der eingekapselte Datenverkehr ist nach Bedarf analysierbar.

bruch auf dem Client selbst, vor Verlassen des LANs und einmal aus der virtuellen Umgebung auf.

Per Multisegmentanalyse des lokalen Netzwerks lässt sich sehr gut der Datenfluss in der virtuellen Umgebung mit dem Datenfluss in der realen Welt vergleichen (Bild 3). Links ist der Datenfluss vor dem realen Switch, rechts ist der Datenfluss in der virtuellen Welt ersichtlich.

Zur Überraschung aller Beteiligten erstellt der virtuelle Server Jumbo Frames, obwohl er dies gar nicht sollte – und diese sogar bis zu einer Größe von zum Teil über 30.000 Byte. Die Jumbo Frames waren dann beim Austritt in die reale Welt in 1.514 Byte große Datenpakete gestückelt, gelangen in das Internet, und der Client auf der WAN-Seite quittiert stets korrekt. Dies funktioniert solange, bis auf der WAN-Leitung ein Paketverlust auftritt.

Nun ist der virtuelle Server mit der Aufgabe konfrontiert, eine einzelne 1.514 Byte große Sequenz aus einem seiner Jumbo Frames neu zu senden. Anfänglich scheint er damit keine Probleme zu haben, kommt jedoch schnell aus dem Tritt und schickt nun immer wieder das zuvor fehlende Paket mit der Sequenznummer 1924019328, was schließlich zum Abbruch der Kommunikation führt.

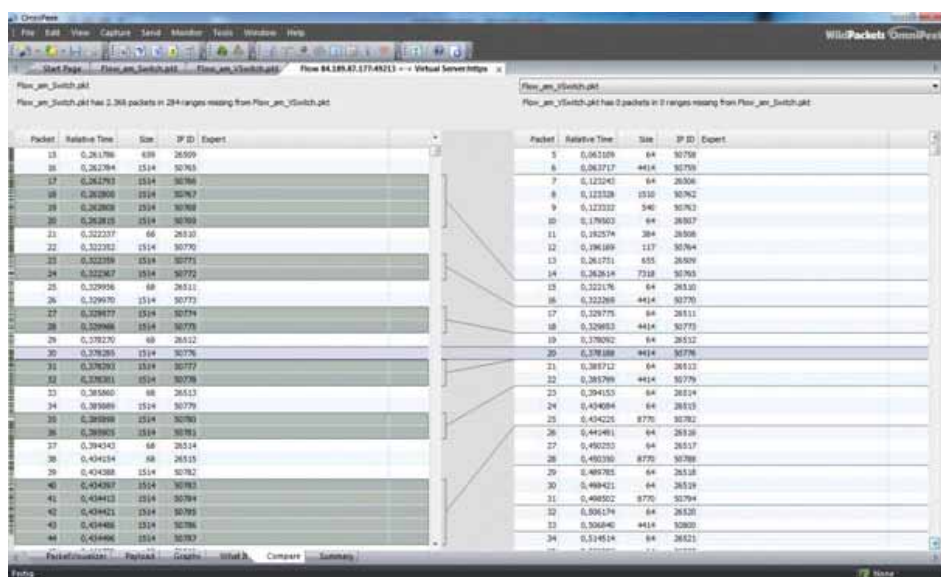


Bild 3. Blau unterlegt Paket mit IP 50776 links auf der WAN-Seite und rechts das Original aus der VM.

erforderlich, die einzelnen TAP-Instanzen auch zu sammeln und an einer zentralen Konsole zu bündeln, andersfalls geht der Überblick über die Datenströme verloren. Dass ein virtueller TAP extrem hohe Ansprüche in Sachen Stabilität erfüllen muss, versteht sich von selbst. Er arbeitet schließlich direkt im Allerheiligsten des Virtualisierungs-Hosts, dem Hypervisor. Darum ist beim Einsatz eines solchen Software-TAPs in einer Produktivumgebung unbedingt auf eine passende Zertifizierung des Hypervisor-Herstellers zu achten. Zudem muss sich die Software mit minimalen Ressourcen zufriedengeben. Schließlich geht jedes Prozent Rechenleistung zu Lasten der VMs und ihrer Anwendungen. Mithilfe von Generic Routing Encapsulation (GRE) lassen sich die Analysedaten in einem abgeschlossenen Tunnel aus dem Host hinaus zu einer anderen IP-Adresse

Anwendungsbeispiel Multisegmentanalyse

Ein international tätiges Wissenschaftsinstitut stellt Forschern und Entwicklern Dateien weltweit zur Verfügung. Die engagierten Wissenschaftler klagten jedoch immer wieder über Verbindungsabbrüche, die oft nutzlos, da nur halb fertige Downloads trotz nicht geringer Wartezeit als Resultat hinterließen. Die Dateien selbst waren im Rechenzentrum auf einem virtuellen Server bereitgestellt und aus der Sicht der Server-Verantwortlichen funktionierte dort alles. Das Netzwerk war augenscheinlich in Ordnung, und so sollte einem Download über das Internet eigentlich nichts im Wege stehen. In so einem Fall kommt zweckmäßigerweise ein Analysewerkzeug zum Einsatz. In einer Drei-Punkt-Messung zeichnete das System die gleiche TCP-Kommunikation inklusive Verbindungsab-

Fazit

Die Analyse von virtuellem Datenverkehr unterscheidet sich nur marginal von der Analyse in der realen Welt. Sicher sind einschlägige Spezifika von virtuellen Umgebungen zu berücksichtigen, das Prinzip bleibt jedoch aus Sicht des Analytikers gleich: Ist für eine korrekte Datenaufnahme gesorgt, steht einer schnellen Problemlösung nichts im Wege.

Timur Özcan, Matthias Lichtenegger
und Stefan Haberland/jos

Timur Özcan ist Channel & Business Development Manager EMEA bei Network Performance Channel, Matthias Lichtenegger ist Country Manager D-A-CH/CEE bei Wildpackets, und Stefan Haberland ist Sales Engineer NGN Technologien bei Brainworks Computer Technologie.

Info: Network Performance Channel GmbH
Tel.: +49 6103 906751
Web: www.np-channel.de