LANCOM™ Whitepaper
Netzvirtualisierung

Einleitung

Virtualisierung ist eines der Top-Themen im IT-Markt! Neben schon bekannten Lösungen wie der Server-Virtualisierung wird die Idee der Virtualisierung zunehmend auch für andere Bereiche der Informationstechnologie interessant. Die Gründe für diesen Trend liegen auf der Hand: Experten erwarten eine bessere Ausnutzung der Ressourcen, höhere Flexibilität und Sicherheit sowie reduzierte Kosten für Investitionen und Administration. Dieses Whitepaper zeigt Techniken und Einsatzmöglichkeiten für die Virtualisierung von Netzen und die dazu notwendigen Komponenten.

Ziele der Virtualisierung

Ganz allgemein steht in der Informationstechnologie der Begriff „Virtualisierung“ für die Trennung einer IT-Anwendung von der verwendeten Hardware. Diese Trennung verfolgt unterschiedliche Ziele, u.a.:

- Optimale Ausnutzung der Ressourcen
- Sicherheit
- Kostenreduzierung

Bereits seit einiger Zeit verbreitet ist die Virtualisierung von Servern. Dabei wird die Server-Applikation (z.B. ein File-Server) samt Betriebssystem in eine virtuelle Maschine verlagert. Mehrere virtuelle Server-Prozesse mit unterschiedlichen Betriebssystemen können dabei parallel auf einer physikalischen Maschine realisiert werden und die Ressourcen so optimal ausnutzen. Kommt es zu einer Störung der Hardware, können die Server-Prozesse in einer virtuellen Infrastruktur auf eine andere Hardware übertragen werden und den Betrieb sicherstellen. Die Server können so zentral auf standardisierter Hardware verwaltet werden, was zu einer deutlichen Reduzierung der Betriebskosten bei optimierter Verfügbarkeit der Prozesse führt.

Ähnliche Ziele verfolgt die Virtualisierung auf Client-Seite, bei der die Hardware an den Arbeitsplätzen auf die Ein- und Ausgabegeräte (Bildschirm, Tastatur und Maus) reduziert wird. Jede Arbeitsstationen nutzt eine eigene Instanz des Betriebssystem auf dem Server mit persönlicher Konfiguration für den Anwender. Neben dem reduzierten Aufwand für die Administration und der vereinfachten Datensicherung steigert der Verzicht auf lokale Speichermedien die Sicherheit.

Netzvirtualisierung

Nicht nur Server und Arbeitsplatzrechner werden virtualisiert, auch das Netz als verbindendes Element (LAN, WLAN bzw. kabelgebundenes oder drahtloses WAN) kann virtualisiert werden. Während bei der Virtualisierung von Clients und Servern die zentrale Wartung und Kosteneinsparungen zu den wichtigsten Ziele gehören, eröffnen virtualisierte Netze völlig neue Anwendungen, die „normale“ Netze nicht bieten können. Die bisher eingesetzten Methoden zur Netzvirtualisierung beziehen sich auf den Übertragungsweg:

- VPN nutzt eine WAN-Verbindung wie eine LAN-Verbindung.
- VLAN lässt mehrere abgeschirmte Netzverbindungen auf einem gemeinsam genutzten Übertragungsmedium zu (Shared Medium).
- Access Points können mit einem WLAN-Modul mehrere Funkzellen (SSIDs) aufspannen, die z. B. unterschiedliche Verschlüsselungseinstellungen verwenden (Multi-SSID).

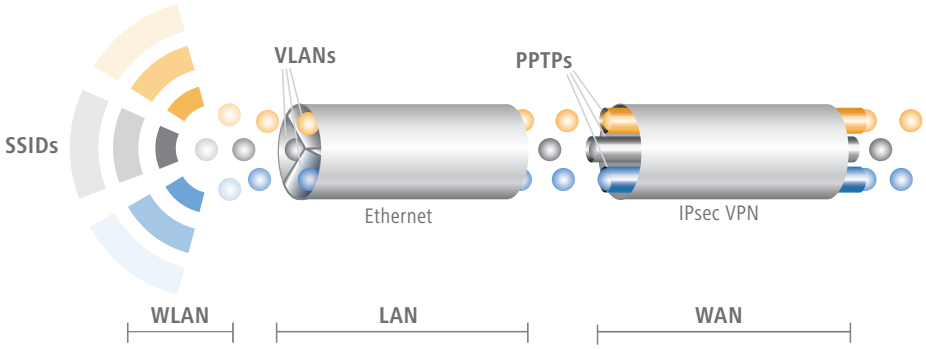
Alle drei Techniken können auf bestimmten Übertragungswegen (IPsec VPN für WAN, VLAN für Ethernet-Verkabelung, Multi-SSID für WLAN) vollständig separierte Netze parallel betreiben. Die Leistungsfähigkeit der eben benannten drei Techniken ist jedoch begrenzt, weil sie in der Regel auf einen Übertragungsweg beschränkt sind. Für eine ökonomische Virtualisierung von Ende zu Ende ist eine logische Verknüpfung dieser Techniken erforderlich. Außerdem werden VPN

LANCOM™ Whitepaper
Netzvirtualisierung

und VLAN üblicherweise zur Erweiterung der internen Netzstruktur eingesetzt. Demgegenüber steht eine immer stärkere Verbindung von ganz unterschiedlichen externen Teilnehmern: die IP-basierte Zusammenarbeit orientiert sich immer mehr an den Aufgaben der Mitarbeiter und macht nicht an den Grenzen einer Organisation halt. Der einfachste Fall ist dabei der Netzzugang für Gäste in den eigenen Räumen, in komplexen Szenarien erhalten externe Dienstleister über das Internet Zugriff auf bestimmte Anwendungen im lokalen Netz. Der nächste Schritt ist daher die Virtualisierung von ganzen Netzen vollständig auf logischer Ebene, unabhängig von bestimmten Zugangspunkten: dazu müssen die vereinzelten Virtualisierungstechnologien für Übertragungswege durch ein ebenso virtualisiertes Routing zwischen diesen verknüpft werden. Ähnlich wie bei der Virtualisierung von Servern wird dabei eine Hardware (Router) genutzt, um mehrere virtuelle Router einzurichten, wobei jeder virtuelle Router speziell für sein Netz konfiguriert werden kann. Mit einer solchen höheren Ebene der Virtualisierung können auf vorhandenen Infrastrukturen parallel völlig unterschiedliche Anwendungen mit dedizierten Einstellungen für das Routing und die Zugriffsberechtigungen realisiert werden.

Multi-VPN: Tunnel im Tunnel

IPsec hat sich als Industrie-Standard für hoch-sichere Verbindungen über WAN-Strecken durchgesetzt. Professionelle Router mit VPN-Gateway bieten verschiedene Möglichkeiten, sich sicher zu authentifizieren und Daten mit hoher Verschlüsselung zu übertragen. Bei Authentifizierung auf Basis von Zertifikaten, kann sich kein fremdes Gerät als vermeintliche Gegenstelle ausgeben und eine Verbindung zum zentralen VPN-Gateway aufbauen. Mit AES-Verschlüsselung können die übertragenen Informationen von niemandem eingesehen werden. Somit eignet sich IPsec-VPN als sichere Methode, den Übertragungsweg zwischen Standorten über das Internet zu virtualisieren. Der Nachteil von IPsec ist jedoch, dass die Übertragung auf die TCP/IP-Ebene (Layer 3 im OSI-Referenzmodell) beschränkt und starr im Bezug auf die Netzdefinition ist, z. B. sind keine zwei separaten Netze mit überschneidendem IP-Adresskreis möglich. Speziell die Netze sollen bei der Virtualisierung sehr flexibel den Erfordernissen angepasst werden. Damit echte Ende-zu-Ende-Netzvirtualisierung möglich wird, müssen zwischen den Gateways Tunnel innerhalb eines IPsec-Tunnels etabliert werden, die völlig unabhängig vom IP-Adressraum der zu vebindenden Netze sind. Mit dem PPTP-Protokoll bietet sich eine Technik an, die schon lange für verschiedenste Internet-Einwahl-Anschlüsse verwendet wird. Ähnlich wie bei VLAN im LAN wird pro virtuellem Netz ein PPTP-Tunnel aufgebaut, der die korrespondierenden VLANs der Standorte durch IPsec hindurch zu einem einheitlichen Netz verbindet. Mit diesem neuartigen Tunnelkonzept können sogar Pro-



LANCOM Systems

LANCOM™ Whitepaper
Netzvirtualisierung

tokolle zur dynamischen Steuerung des IP-Routings innerhalb eines virtuellen Netzes, wie z. B. RIP, sicher zwischen Standorten übertragen werden. Ein weiterer Vorteil dieses Konzepts gegenüber separaten Tunneln mit Authentifizierung und Verschlüsselung pro Netz liegt in der Beschränkung der Authentifizierung und Verschlüsselung auf einen umhüllenden IPsec-Tunnel. Bei gleicher Sicherheit wie mit separaten IPsec-Tunneln werden rechenintensive Authentifizierungs- und Rekeying-Prozesse (zyklischer Wechsel der zur Verschlüsselung verwendeten Schlüssel) eingespart. Somit werden hinsichtlich Transparenz und Routing ähnliche Eigenschaften wie bei MPLS-VPN erzielt, jedoch mit höherer Sicherheit und dem Vorteil, dass das VPN nicht in der Hand des Internet-Providers sondern in der des Anwender-Unternehmens liegt. Der Verwendung verschiedenster Übertragungstechniken wie ADSL, SHDSL, Glasfaser oder UMTS auch als Backupverbindung für denselben Standort steht nichts im Wege. Durch die Unabhängigkeit vom Anschlussbetreiber besteht die Möglichkeit, Netzvirtualisierung über Ländergrenzen hinweg mit verschiedensten Netzzugängen einzusetzen.

Advanced Routing and Forwarding (ARF)

Wie aber können die vorhandenen, physikalischen Netze für die Anforderungen der modernen Kommunikation und Zusammenarbeit genutzt werden? Moderne Netzvirtualisierungen gehen über die statische Konfiguration von VPNs und VLANs hinaus und nutzen Funktionen wie das „Advanced Routing and Forwarding“. Der Kernpunkt dieser Technologie ist die Möglichkeit, für jede Nutzung ein eigenes IP-Netz auf dem zentralen physikalischen Router einzurichten (z. B. ein Netz für die Mitarbeiter mit Ihren Arbeitsplatz-PCs oder mobilen Notebooks, eines für Gäste im WLAN, eines für den Dienstleister der Alarmanlage). Für jedes dieser Netze können grundlegende Dienste wie z. B. der DHCP-Server separat konfiguriert werden.

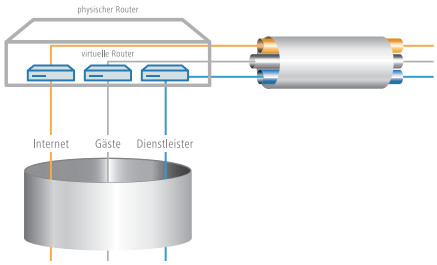
Datenpakete, die am physikalischen Router eintreffen, werden nun anhand verschiedener, vordefinierter oder automatisch gelernter Kriterien einem der Netze zugeordnet. Wie und wohin diese Datenpakete geroutet werden, wird anhand der Regeln für das virtuelle Netz entschieden. Insgesamt verhalten sich die Netze mit ihren eigenen Definitionen, Kriterien für zuzuordnende Datenpakete, Eigenschaften und Dienste wie eine Reihe eigenständiger virtueller Router. Kriterien und Eigenschaften für solche virtuellen Netze können sein:

- Zugang über einen definierten Netzwerkport eines Switches – ggf. mit Authentifizierung – und Aufnahme ins VLAN für Mitarbeiter im LAN. Anhand des VLANs gelangen die Pakete ins Netz für Mitarbeiter. Der Anwender hat damit Zugriff auf alle Anwendungen und Ressourcen, die für Mitarbeiter zur Verfügung stehen.
- Zugang über einen VPN-Client auf einem Mobilrechner von unterwegs mit Authentifizierung und Verschlüsselung. Anhand des VPNs wird der Anwender dem Netz für Mitarbeiter mit allen Ressourcen und Anwendungen zugeordnet.
- Zugang über das WLAN mit der SSID für Mitarbeiter. Für diese SSID wird Authentifizierung und hohe Verschlüsselung gefordert. Nach Anmeldung befindet sich der Anwender im Netz für Mitarbeiter.
- Zugang über das WLAN mit der SSID für Gäste. Es wird z. B. keine Authentifizierung gefordert und nur mäßige Verschlüsselung. Der Anwender gelangt

LANCOM™ Whitepaper
Netzvirtualisierung

aufgrund der SSID ins Netz für Gäste und erhält nur Zugriff auf das Internet und bestimmte Drucker. Tatsächlich sind die anderen Ressourcen nicht gesperrt, IP-technisch existieren alle anderen Netze, Dienste und Ressourcen nicht.

- Zugang über VPN mit Authentifizierung als Dienstleister und verschlüsselter Übertragung. Aufgrund der VPN-Zuordnung wird der Anwender dem Netz für Dienstleister zugeordnet und kann nur die Geräte im Netz erreichen, welche zum Arlamierungssystem gehören, alle anderen Ressourcen existieren in diesem Netz nicht.



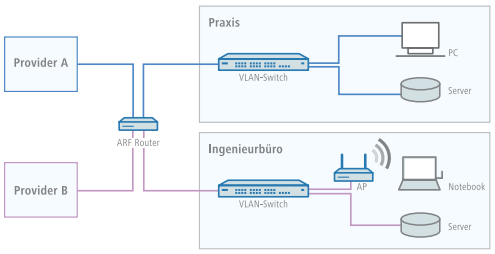
Anforderungen an die Hardware

Um diese Form der Virtualisierung zu erreichen, müssen die verwendeten Router Advanced Routing and Forwarding beherrschen, also mehrere IP-Netze völlig unabhängig voneinander verwalten und Dienste zur Verfügung stellen können. Außerdem müssen die Router die Zuordnung der IP-Netze zu Schnittstellen, VLANs, SSIDs, Gegenstellen, WAN-Verbindungen oder auch per Firewall ermittelten Paket-Eigenschaften unterstützen. Damit die virtuellen Netze auch über strukturierte Verkabelung in Hierarchien und im WLAN durchgesetzt werden können, müssen auch die Switches und Access Points VLAN-fähig sein.

Beispiel: Büro- oder Praxisgemeinschaft

Virtualisierte Netzstrukturen bieten schon für kleine Unternehmen deutliche Vorteile. Auch Arztpraxen, Steuerkanzleien oder Ingenieur-Büros können heute nicht mehr auf die Vernetzung mit Geschäftspartnern verzichten. In vielen Gebäuden reicht die vorhandene Verkabelung aber nicht aus, um für jeden Mieter ein komplett eigenes Netz einzurichten.

In diesem Fall kann für z.B. für die Arztpraxis und das Ingenieur-Büro jeweils ein separates virtuelles IP-Netz eingerichtet werden. Beide Netze sind intern völlig voneinander getrennt, so dass kein unbefugter Zugriff auf Patientendaten oder Konstruktionspläne möglich ist. Das Ingenieur-Büro kann zusätzlich noch einen WLAN-Zugang für Gäste einrichten, die nur Zugriff auf das Internet haben.



Beispiel: Vernetzte Handelsfiliale

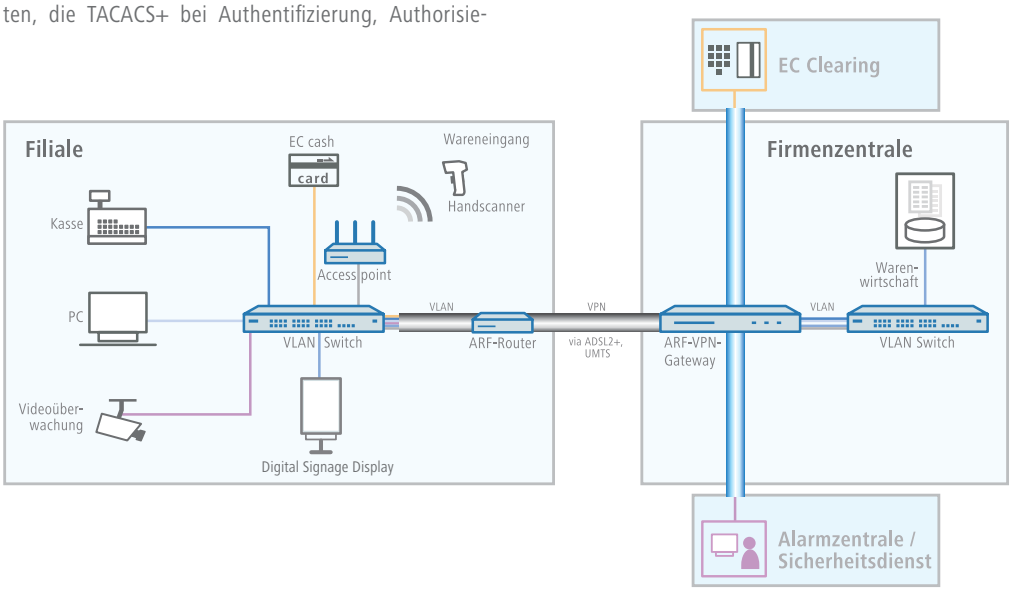
In dem ersten Beispiel geht es vor allem um die Trennung von internen Datenströmen. Ein entscheidender Vorteil der virtuellen Netzstruktur ist jedoch, auch Anwendungen mit externen Teilnehmern sauber in das eigene Netz zu integrieren. Das Beispiel einer vollständig vernetzten Filiale (z.B. in einem Supermarkt) zeigt die weiten Möglichkeiten, die ARF in Verbindung mit VLAN realisieren kann. Neben den PCs der Filialleitung, die über VPN mit der Zentrale verbunden sind (hier

LANCOM™ Whitepaper
Netzvirtualisierung

blau dargestellt), können auch die Barcode-Scanner am Wareneingang (drahtlos angebunden über einen Access Point) jederzeit Daten mit dem ERP-System austauschen. Außerdem sind verschiedene externe Dienstleister in das Netz eingebunden: eine Großbäckerei steuert den Backautomaten und ruft Informationen über dessen Zustand ab (hellblau), der Sicherheitsdienst kann die Bilder der Überwachungskameras der Filialen rund um die Uhr beobachten (violett) und die EC-Terminals an den Kassen sind direkt mit dem Clearing verbunden (gelb). Für jede Anwendung wird dabei ein eigenes virtuelles IP-Netz eingerichtet, für das ein spezieller IP-Adresskreis und separate Routing-Einstellungen definiert werden. Der Netzabschnitt für die EC-Abrechnung kann so z.B. an die IP-Adressen angepasst werden, welche die Clearing-Stelle in ihrer VPN-Struktur verwendet. Im internen LAN werden die IP-Netze zusätzlich über entsprechende VLANs markiert, die über einen VLAN-fähigen Switch getrennt werden – andere Teilnehmer können nicht auf dieses Netz zugreifen. Mit dem Einsatz von Netzkomponenten, die TACACS+ bei Authentifizierung, Autorisierung und Accounting unterstützen, kann gleichzeitig eine wichtige Anforderung der Payment Card Industry erfüllt werden (PCI-Compliance).

Fazit

Mit bewährten Virtualisierungstechnologien wie VPN, VLAN und MultiSSID wird die Ausnutzung der vorhandenen Übertragungswege (Internetanschluss, Netzwerkverkabelung, WLAN) in Netzwerken deutlich verbessert. Advanced Routing and Forwarding ermöglicht die flexible Verknüpfung der verschiedenen Virtualisierungstechnologien für Übertragungswege und virtualisiert gleichzeitig die Routerfunktionen. Damit lassen sich sicher getrennte IP-Netze über räumliche Netzgrenzen hinweg parallel auf denselben Infrastruktur-Komponenten betreiben. Netzvirtualisierung, die nur durch das Zusammenspiel von aufeinander abgestimmten Routern mit ARF, VLAN-fähigen Switches und Access Points mit Multi-SSID erzielt wird, eröffnet völlig neue Anwendungen auf Basis einer einzigen Infrastruktur – bei gleichzeitig reduzierten Kosten.



LANCOM Systems GmbH I Adenauerstr. 20/B2 I 52146 Würselen I Deutschland I E-Mail info@lancom.de

LANCOM Systems