ComConsult Research

Der Netzwerk Insider

November 2016

Systematische Weiterbildung für Netzwerk- und IT-Professionals

Schwerpunktthema

SDN in Unternehmensnetzen

von Dipl.-Math. Cornelius Höchel-Winter

SDN weckt immer noch so viele Emotionen wie kaum ein anderes Netzwerkthema in den letzten Jahrzenten. Je nach Sichtweise wird die Technologie zum Heilsbringer, zur Spinnerei technologiegläubiger Akademiker oder gar zum Jobvernichter hochstilisiert

Bei so großen Unterschieden in der Bewertung und Argumentation lohnt es sich in der Regel, mal kurz durchzuatmen, einen Schritt zurückzutreten und mit einem etwas größerem Abstand die Materie zu betrachten. Dies ist das Ziel dieses Artikels.

Was ist SDN?

Getrieben werden die unterschiedlichen Meinung über SDN natürlich nicht zuletzt von der Tatsache, dass SDN eben **kein** standardisiertes Protokoll oder fertiges Produkt eines Herstellers, das man bewerten könnte, ist. Es gibt noch nicht einmal irgendein Dokument, das SDN umfassend und abschließend festschreibt, denn mit SDN wird eher diffus eine Architektur zur zentralisierten Steuerung von Netzen bezeichnet als eine konkrete Technik.

weiter auf Seite 6

Zweitthema

Internet-DMZ in der Cloud

von Dr. Simon Hoff und Dipl.-Math. Simon Oberem

Mit der Verlagerung von Anwendungen und Daten in eine Cloud, müssen auch entsprechende Sicherheitskomponenten in der Cloud zur Verfügung stehen. Wenn beispielsweise Web-Anwendungen und Web-Services in einer Private Cloud, Public Cloud oder Hybrid Cloud realisiert werden, dann müssen hier auch Firewalls, Intrusion-Prevention-Systeme und Web Application Firewalls (WAFs) bzw. Reverse Proxies integriert werden. Damit wandert automatisch ein Teil der Systeme, die in der Vergangenheit im lokalen Rechenzentrum (RZ) im Bereich der Internet-Anbindung aufgebaut wurden, in die Cloud, und dieser Trend zeigt sich inzwischen in praktisch allen Bereichen der Internet-Anbindung.

1. Traditioneller Aufbau von Internet-DMZs

Eine Demilitarized Zone (DMZ) ist ein Zwischennetz, das als Pufferzone den Übergang zwischen Netzen unterschiedlichen Sicherheitsniveaus schafft. Typisches Beispiel ist eine DMZ zwischen dem Internet und dem internen Netz. Ausprägungen und Spielarten von DMZs sind vielfältig und auch am Internet-Übergang gibt es keine Standards, sondern unterschiedliche Best-Practices. Generell kann man Internet-DMZs grob in DMZs klassifizieren, die nur ausgehenden Verkehr, nur eingehenden oder ein- und ausgehenden Verkehr behandeln, wie in Abbildung 1 skizziert. Am Internet-Zugang ist der Aufbau einer zweistufigen Firewall-Architektur gebräuchlich, und die Systeme im DMZ-Bereich, die direkt mit dem Internet und mit internen Systemen kommunizieren (z.B. Proxies, VPN-Gateways und Reverse Proxies), werden typischerweise dual-homed angebunden.

weiter auf Seite 18

Geleit

Funktechnologien: es kommt eine Revolution

auf Seite 2

Standpunkt

Universelle Mobilität – ist das gesund?

auf Seite 14

Aktueller Kongress

UC-Forum 2016

ab Seite 12

Aktuelle Sonderveranstaltungen

Wireless und Mobility Winterschule 2016

ab Seite 3 und ab Seite 15

Geleit

Funktechnologien: es kommt eine Revolution

Funk-Netzwerke oder auf Neudeutsch Wireless-LANs kämpfen seit ihrer Markteinführung mit den Grenzen der Physik: entweder hohe Leistung oder große Entfernungen. Dies ist dann noch zu kombinieren mit den daraus abgeleiteten Zellplanungen und der Integration unterschiedlicher Teilnehmermengen. Denn wir haben nicht nur die Grenzen der Physik, wir haben auch Anforderungen, die verschiedener nicht sein können. Vom Büro über das Hotel bis zur Fertigung. Und natürlich soll es zuverlässig und sicher sein, zwei Attribute, die nun gar nicht zur Funktechnik passen. Damit wären wir wieder bei der Physik.

Bisher entwickelt sich der Markt zweigeteilt. Auf der einen Seite haben wir den Mobilfunk, auf der anderen die WLANs. Die technischen Konzepte könnten unterschiedlicher nicht sein, auch wenn beide Welten mit der Physik kämpfen und versuchen die Grenzen des Machbaren immer weiter auszudehnen.

Im WLAN-Bereich werden wir in den nächsten Jahren mit der Umsetzung von 11ad und 11ax einen weiteren Leistungsschub erleben. Die ersten neuen Chip-Generationen sind da und von hier an gibt es nur noch einen Weg: noch mehr Leistung mit noch mehr Einschränkungen. Die entsprechenden Produkte sind schon auf dem Markt oder kommen in den nächsten Monaten. Dementsprechend muss die Planung bereits darauf ausgelegt werden. Aber das ist im WLAN nicht neu, aufgrund der permanenten Weiterentwicklung brauchen wir immer schon Planungsansätze, die über den Tellerrand hinaus gehen. Interessanterweise erhalten wir schon bald ein Verkabelungsproblem. Die gerade für den WLAN-Bereich eingeführten Ethernet-Standards mit 2,5 und 5 Gigabit sind aus heutiger Sicht bereits unzureichend und wir werden bald 10 Gigabit brauchen. Natürlich wieder in Abhängigkeit vom Szenario. Aber speziell Industrie 4.0 wird neue Türen öffnen und einen bisher unbekannten Bandbreitenbedarf auch in die Produktion bringen. Dies muss bereits jetzt vorbereitet und durchdacht werden.

Die gleiche Entwicklung erleben wir im Mobilfunk, nur anders. Auch hier haben wir sehr widersprüchliche Szenerien, die sich in sehr verschiedenen Bedarfsgruppen aufgeteilt nach Reichweite, Teilnehmerzahl und Bandbreite einteilen lassen. Und klar ist schon seit längerem, dass LTE dem sich entwickelnden Bedarf nicht gerecht wird. SmartCity und Autonomes Fahren werden Anforderungen generieren, die wir mit keiner aktuellen Funktechnik abdecken können. Wir haben eben zu große Wiedersprüche im Design. Auf der einen Seite die preiswerte Integration von Sensoren und auf der anderen Seite Gigabit über große Entfernungen.

Wohin wird es von hier aus gehen und werden wir vielleicht endlich auch eine bessere Integration von Mobilfunk und WLAN sehen? Die Antwort ist ganz einfach: wir werden in den nächsten fünf Jahren eine Revolution der Funktechnik erleben. Die Kombination aus der Weiterentwicklung von WLAN mit 11ax und Mobilfunk mit 5G wird völlig neue Voraussetzungen schaffen.

Was ist anders? Nun, die Technologie akzeptiert endlich, dass wir sehr verschiedenen Bedarfs-Situationen haben. Und anstelle der Kombination inkompatibler Einzeltechnologien wird es ein Gesamtpaket geben. Dies wird sich aus heutiger Sicht um 5G herum gruppieren.

Diese Entwicklungen sind so brisant, dass wir eine aktuelle Sonderverstaltung zu diesem Thema aufgesetzt haben: Wireless und Mobility. Diese findet am 12. und 13.12. in Köln statt und beleuchtet alle aktuellen Entwicklungen, vom heutigen Bedarf bis hin zu den Extrem-Anforderungen der Zukunft.

Wir sind fest davon überzeugt, dass Funktechnik/Wireless den Netzwerk-Markt stark verändern werden. Diskutieren Sie mit unseren Experten diese aktuelle Entwicklung und die Konsequenzen für Ihre Netzwerke.

Viel Erfolg dabei

Ihr
Dr. Jürgen Suppan

Schwerpunktthema

SDN in Unternehmens-netzen

Fortsetzung von Seite 1

Dipl.-Math. Cornelius Höchel-Winter ist Leiter des Testlabors der ComConsult Research GmbH. In dem Labor werden regelmäßig Messungen und Evaluierungstests neuester Hard- und Softwareprodukte durchgeführt und ausgewertet. Herr Höchel-Winter besitzt langjährige Erfahrung in der Konzeptionierung, im Aufbau und Betrieb von Windows- und Unixnetzen; so hat er als verantwortlicher Projektmanager die Rechenzentren und Netzwerke auf dem Gelände der EXPO2000 in Hannover aufgebaut und während der Weltausstellung betrieben.

Diese fehlende allgemein anerkannte Definition führt eben auch dazu, dass jeder mit einem zentralen Managementtool dieses Produkt in letzter Zeit gerne mal in der Nähe von SDN positioniert. Aber so einfach ist es nicht.

SDN steht für „Software Defined Networking“, der Begriff reicht bis in die 1990er Jahre zurück. Die Basis dessen, was wir heute unter SDN verstehen, wurde jedoch erst 2007/2008 an den amerikanischen Universitäten Berkeley und Stanford gelegt und ist eng verbunden mit den Namen Martîn Casado, Nick McKeown und Scott Shenker, dem Unternehmen Nicira und dem Protokoll OpenFlow.

OpenFlow ist ein Kommunikationsprotokoll zur Steuerung von Layer-2- und Layer-3-Swiches und Routern im Netzwerk. Das Protokoll wird von der ONF (Open Networking Foundation) entwickelt und ist historisch gesehen im Grunde der Startpunkt der modernen SDN-Entwicklung.

Das Protokoll basiert auf „Anweisungen“ an die Netzwerkkomponenten, wie mit welchen eingehenden Paketen zu verfahren ist. Diese „Anweisungen“ bestehen jeweils aus einer Mustererkennung und einer oder mehreren Aktionen. Die Aktionen werden von der OpenFlow-Komponente durchgeführt, wenn das eintreffende Paket zu dem jeweiligen Muster passt. Als Muster kommen alle Layer-2-, Layer-3- und Layer-4-Headerkomponenten in Frage, insbesondere also die MAC- und IP-Adressen sowie die Portnummern von UDP und TCP, typische Aktionen sind „Paket an Port x weiterleiten“ oder „Paket wegwerfen“, aber auch Änderungen des Pakets selbst wie VLAN-Zuordnung oder QoS-Markierungen sind möglich.
An den Universitäten stand man damals vor der Aufgabe, neue Netzwerkprotokolle und -verfahren testen zu wollen, ohne aufwändige, dedizierte Testumgebungen aufbauen zu müssen. Die Idee war daher, das Produktiv- bzw. Campusnetz (mit) zu nutzen und pro Anwendung zu steuern, wie die jeweiligen Kommunikationsströme im Netz behandelt werden. Schnell waren die wesentlichen Eckpunkte gefunden, wie man so etwas umsetzen könnte. Man nehme:

- OpenFlow,
- einen zentralen Controller, der die Netzwerkströme jetzt via OpenFlow steuert, und
- Netzwerkkomponenten, die die OpenFlow-Anweisungen des Controllers umsetzen und die einzelnen Pakete entsprechend bearbeiten und weiterleiten können.

Eine wichtige Anmerkung vorweg: Wenn an dieser Stelle und auch später im Artikel von „einem“ oder „dem“ Controller die Rede ist, bedeutet das nicht, dass es sich physisch um ein einzelnes System handelt. Vielmehr ist damit eine zentrale Control Plane gemeint, die natürlich sowohl redundant als auch verteilt aufgebaut werden kann.

Damit ist das Grundgerüst von SDN im Wesentlichen skizziert (siehe Abbildung 1).

1. Paket kommt beim ersten Switch (Ingress-Switch) an.
2. Falls der Switch keine Regel kennt, wie das Paket behandelt werden muss, fragt er beim Controller nach. Hierzu leitet er wahlweise das komplette Paket oder nur Metadaten (Header-Daten) an den Controller weiter.
3. Der Controller entscheidet über Bearbeitungs- und Weiterleitungsregeln und schickt diese Regeln an alle betroffenen Systeme.
4. Das Paket wird entsprechend dieser Regeln bearbeitet und durch das Netzwerk geschleust.

Schon aus diesem recht einfachen Basiskonzept lassen sich wesentliche Merkmale der ursprünglichen Idee ableiten:

1. Das Konzept ist **flowbasierend.**
   Das heißt, der Controller muss Bearbeitungs- und Weiterleitungsregeln nicht für jedes einzelne Paket ableiten und verteilen, sondern nur für ganze Klassen von Verkehrsströmen oder Kommunikationsbeziehungen (sogenannte Flows), die anders behandelt werden müssen als andere. Konkret: die über einen anderen Weg durch das Netz geschleust oder die sonst wie anderes bearbeitet werden sollen.

   Diese Flows werden natürlich durch die Mustererkennung von OpenFlow definiert.
2. Da die OpenFlow-Regeln auch auf nachfolgende Pakete angewendet werden sollen, muss der Switch oder Router diese Regelsätze zwischenspeichern. Das bedeutet einerseits einen völlig neuen Tabellentyp („Flow Table“) für diese Informationen im Speicher der Netzwerkkomponenten, bietet andererseits aber auch die Chance, die unterschiedlichen Forwarding-Tabellen von MAC-Adressen über IPv4- und IPv6-Adressen bis hinzu ACLs, die man heutzutage alle in Switches findet, zu vereinheitlichen und so eine **einheitliche Speicherstruktur** (Data Plane) zu schaffen.

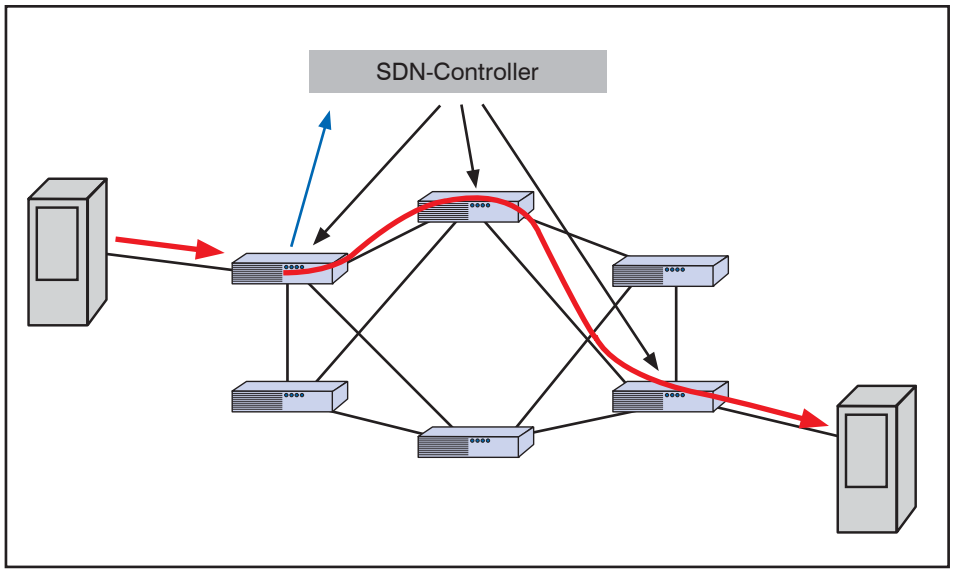

Abbildung 1: Basiskonzept von SDN: zentrale Netzwerksteuerung

3. Aus architektonischer Sichtweise gestattet es OpenFlow von außen die Forwarding Plane von Netzwerkkomponenten zu manipulieren oder gar komplett zu verwalten. Die sogenannte **Control Plane**, die für diese Aufgabe zuständig ist, wird also praktisch auf den Controller **ausgelagert**.

Hier deutet sich bereits an, dass dieses Konzept einige Freiheitsgrade besitzt, die gerne übersehen werden. Stellt man insbesondere den Controller ins Zentrum des Konzepts, wird schnell klar, dass OpenFlow nur eine mögliche Ausprägung der Schnittstelle zu den Hardware-Geräten ist. Wählt oder entwickelt man eine andere Schnittstelle, kann man sich zum Beispiel von OpenFlow-spezifischen Einschränkungen befreien, insbesondere von der Beschränkung auf Layer-2- bis Layer-4-Merkmale:

- Theoretisch lassen sich nämlich alle klassischen Netzwerkgeräte vom Switch und Router bis hin zu Firewall und Loadbalancer steuern bzw. deren Regelwerk bedarfsgerecht anpassen.

- Das Konzept (auch mit OpenFlow) erzwingt keineswegs, dass jeglicher Datenverkehr vom Controller gesteuert werden muss. Wir werden diesen Aspekt weiter unten noch diskutieren.

- Und das Konzept erzwingt keineswegs, dass es nur einen Controller gibt. Es gibt tatsächlich Lösungen mit spezialisierten Controllern für bestimmte Gerätetypen oder Protokolle. Auch diesen Punkt werden wir unten etwas genauer beleuchten.

Was hierbei auf den ersten Blick komplex aussieht, ist das genaue Gegenteil. Es macht überhaupt keinen Sinn Firewalling-Funktionalität in eine Lösung zu bringen, die im Kern die Wegewahl durch das Netzwerk regeln soll. Andererseits wäre es schade, Firewalls prinzipiell auszuschließen.

Die spannende Frage ist also, wie dieses Grundgerüst in der Praxis umgesetzt wird. Tatsächlich gibt es eine breite Palette von Möglichkeiten, die die Bandbreite von SDN aufzeigen, aber gerade auf Grund dieser Bandbreite auch für viel Verwirrung und Unsicherheit im Markt sorgen.

Die Vision: SDN überall

Den Entwicklern von SDN schwebte schon früh die Vision vor, den beschriebene Entwurf auf der Basis von OpenFlow flächendeckend für gesamte Unternehmens- oder Campusnetze einzusetzen und alle Netzwerkkomponenten über einen zentralen Controller zu steuern.

Nick McKeown, einer der Gründungsväter, hatte in seinen Präsentationen folgende Definition von SDN:

> A network in which the control plane is physically separate from the forwarding plane.
>
> and
>
> A single control plane controls several forwarding devices.
>
> (That's it)

Mit anderen Worten: „Dumme" Netzwerkkomponenten, die nur das reine Packet Forwarding umsetzen, werden von einer zentralen Controller-Instanz gesteuert, wo die komplette Netzwerkintelligenz und alle Statusinformationen des Netzes zusammengeführt werden.

Die Erwartungen an dieses allumfassende und sehr strikte Modell waren sehr groß und wurden mit entsprechend markigen Worten vorgetragen:

- Ablösung der statischen und dezentralen Netzwerkkonzepte aus den 50er- und 60er-Jahren durch dynamische, zentral gesteuerte Strukturen,

- Ablösung der „Mainframe-artigen", proprietären und komplexen Netzwerkkomponenten durch einfache und günstige „Forwarding Devices", möglichst auf Basis von i386-Standardkomponenten,

- Ablösung von standardsbasierenden Netzwerkprotokollen mit Innovationszyklen in der Größenordnung von Jahrzehnten (Was ja mit Blick auf die IEEE und IETF durchaus realistisch ist!) durch moderne, schnellentwickelte Softwaremodule im Controller, möglichst auf Open-Source-Basis.

Kurz: Alles wird einfacher und alles wird billiger.

Was bedeutet ein solches Modell für das Netzwerk?

Bleiben wir hierzu kurz noch bei der Vorstellung, dass alle mit der Bearbeitung und Weiterleitung von Netzwerkverkehr beschäftigten Geräte in eine gemeinsame SDN-Architektur eingebunden sind und von einer einzigen übergeordneten Controller-Instanz gesteuert werden.

Ein solches Netz hat beeindruckende neue Eigenschaften: Es gibt im Grunde keine Layer-2- oder Layer-3-Domänen mehr!

Der Controller definiert nämlich für jede Kommunikationsbeziehung, zum Beispiel für eine Datenbankverbindung zwischen zwei Servern oder für eine Anwendung zwischen Server und Client, je einen Pfad von Endpunkt zu Endpunkt quer durch das Netzwerk und verteilt die dazugehörenden Weiterleitungsregeln entlang dieses Wegs.

Und da er das für alle Datenverbindungen macht, heißt das, unser Netzwerk besteht nur noch aus bedarfsgerecht, dynamisch aufgebauten Punkt-zu-Punkt-Verbindungen (gegebenenfalls auch Punkt-zu-Mehrpunkt-Verbindungen): kein Spanning Tree, keine Routing Protokolle, kein Shortest-Path-Bridging und ähnliches, keine VLANs

Zweitthema

Internet-DMZ in der Cloud

Fortsetzung von Seite 1

Dr. Hoff ist technischer Direktor der ComConsult Beratung und Planung GmbH und blickt auf jahrelange Projekterfahrung in Forschung, Standardisierung, Entwicklung, Planung und Betrieb in den Bereichen IT-Sicherheit, lokale Netze und mobile Kommunikationssysteme zurück.

Dipl.-Math. Simon Oberem ist als Berater bei der ComConsult Beratung und Planung GmbH in dem Bereich IT-Sicherheit tätig. Im Projektgeschäft befasst er sich maßgeblich mit den Aspekten von ISMS nach ISO 27001, auch auf Basis BSI-Grundschutz sowie deren praxistauglicher Umsetzung.

Dieser bewährte Aufbau beginnt sich nun signifikant zur verändern. Zum einen machen Virtualisierung und RZ-Automatisierung auch vor Internet-DMZs nicht halt. Dies ist speziell im der Bereich von Web-Anwendungen und Web-Services der Fall. Zum anderen ist es vom Hosting der Internet-DMZs samt externer Firewall in einem Provider-RZ zu einer Private Cloud bei einem Cloud Provider nicht weit.

2. Cloud Computing und Informationssicherheit

Cloud Computing umfasst als Oberbegriff gemäß einer Definition des BSI (siehe BSI Cloud Computing Eckpunktepapier) „das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle.“ Die Dienstleistungen umfassen dabei neben Infrastructure as a Service (IaaS), Platform as a Service (PaaS) insbesondere auch Software as a Service (SaaS).

Im Rahmen des Cloud Computing haben sich außerdem unterschiedliche Betreibermodelle etabliert:

- Public Cloud: Hier werden durch einen entsprechenden Anbieter über das Internet Cloud-Ressourcen und Dienste der Allgemeinheit zur Verfügung gestellt.
- Private Cloud: Hierbei wird die Cloud-Infrastruktur dezidiert für eine Organisation betrieben. Sie kann von der Organisation selbst oder einem Dritten organisiert und geführt werden und kann dabei im RZ der eigenen Organisation oder eines Cloud-Dienstleisters stehen.
- Virtual Private Cloud: In einer Public Cloud kann auf Basis der gemeinsam genutzten Infrastruktur mit den Mitteln der Mandantentrennung einem Kunden eine dedizierte virtuelle Landschaft bereitgestellt werden.
- Hybrid Cloud: Diese Cloud-Infrastruktur ist eine Zusammensetzung aus verschiedenen Cloud-Infrastrukturen (Public Cloud oder Private Cloud), die jeweils für sich eigenständig sind und deren Daten bzw. Anwendungen über standardisierte oder proprietäre Technologien gekoppelt werden.

Ein fundamentales Problem des Cloud Computing liegt damit auf der Hand. Außer bei einer Private Cloud im eigenen RZ gilt: Daten verlassen die Institution und neben der Absicherung der Daten beim Transport ist die Kernfrage, wie die Daten beim Cloud Provider abgesichert werden.

Aus dem Blickwinkel der Informationssicherheit handelt es sich beim Cloud Computing tatsächlich zunächst um eine spezielle Form des Outsourcings, d.h. wesentliche Sicherheitsmaßnahmen, wie z.B. Vorgaben an die Verschlüsselung von Daten, können nur noch vertraglich geregelt werden. Die Informationssicherheit und der Datenschutz finden je nach Service-Model (IaaS, PaaS oder SaaS) in einem erheblichen Umfang beim Cloud Provider statt. Im Extremfall ist bei SaaS für die nachhaltige und nachweisliche Absicherung von Anwendungen, Plattformen und Infrastruktur der Cloud Provider zuständig und der Cloud-Nutzer muss sich „nur“ noch um die sichere Nutzung der Cloud-Anwendungen kümmern.

Für die sichere Nutzung und den sicheren Betrieb von Clouds gibt es inzwischen spezifische Anforderungskataloge aus unterschiedlichen Quellen, z.B.:

- NIST, „Guidelines on Security and Privacy in Public Cloud Computing”, 2011
- ISO 27017, “Code of practice for information security controls based on ISO/IEC 27002 for cloud services”, 2015
- BSI, „Anforderungskatalog Cloud Computing - Kriterien zur Beurteilung der Informationssicherheit von Cloud-Diensten“, Februar 2016

Außerdem gibt es auch Möglichkeiten, dass ein Cloud-Provider durch ein spezifisches Zertifikat einen Qualitätsnachweis für die Informationssicherheit liefert (z.B. neben einer generischen Zertifizierung nach ISO 27001 auch eine Cloud-spezifische Zertifizierung nach ISO 27017, nach EuroCloud oder nach der Cloud Security Alliance).

Internet-DMZ in der Cloud

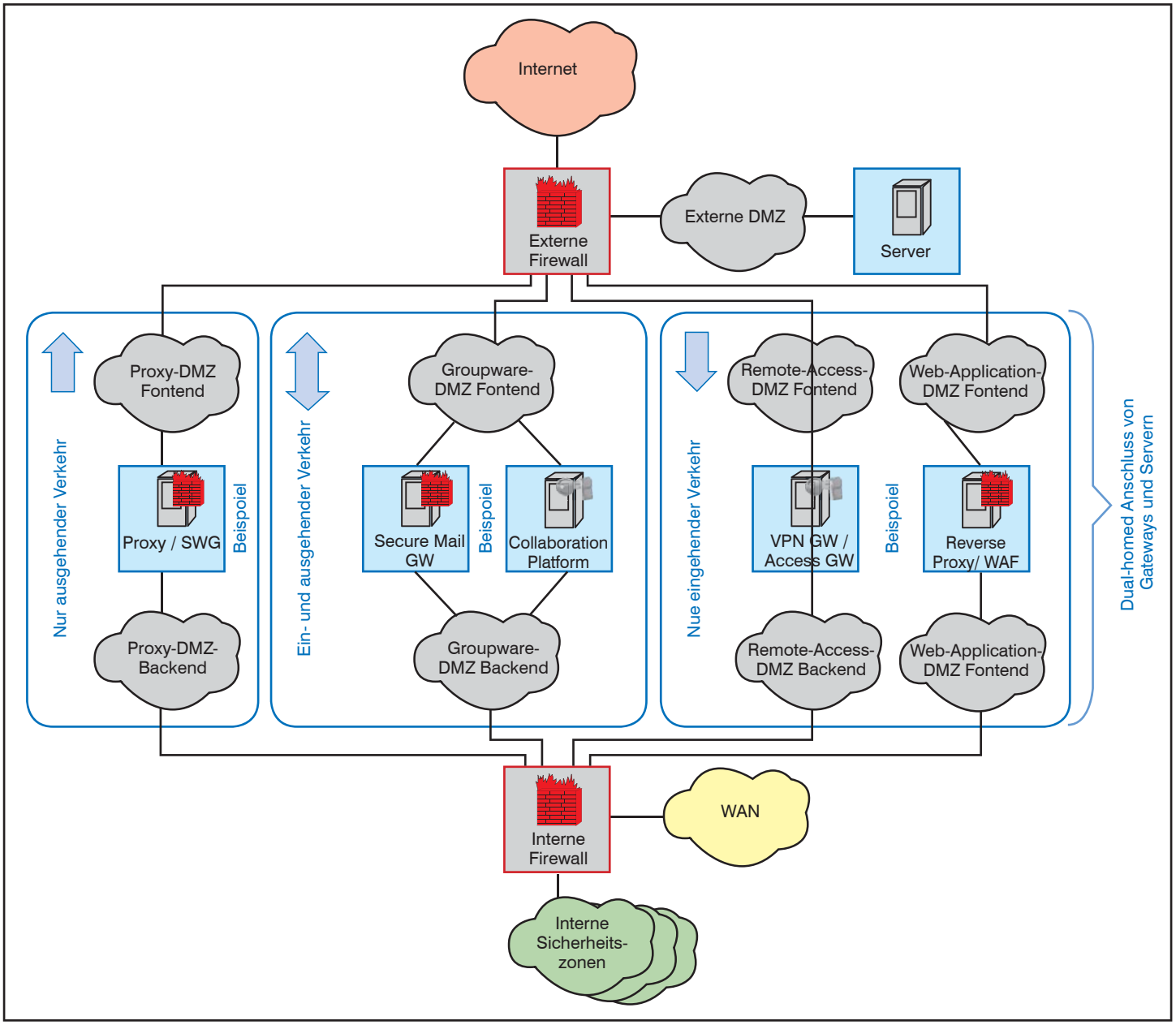

Abbildung 1: Beispiel einer zweistufigen Firewall-Architektur für den Internet-Zugang mit DMZ-Bereich

3. Notwendigkeit von Sicherheitskomponenten in der Cloud

Werden Anwendungen bzw. Anwendungskomponenten in die Cloud verlagert, müssen sich die Maßnahmen der Informationssicherheit automatisch ebenfalls auf die Cloud erstrecken.

Nehmen wir beispielsweise an, dass eine Web-Anwendung in einer Cloud auf Basis von PaaS realisiert werden soll. Der Cloud Provider betreibt die Plattform bestehend aus Web-Servern, Web-Anwendungsservern und Datenbankservern. Hinzu kommen Load Balancer, die ebenfalls Plattformbestandteil sind. Auf diese Plattform wird die Web-Anwendung, inklusive Anwendungs-Code und Datenbankschema auf der Plattform durch den Nutzer über einen gesicherten Kommunikationskanal geladen und eine sichere Mandantentrennung sorgt dafür, dass die Bestandteile der Web-Anwendung und die zugehörigen Daten vor den anderen Nutzern der Systeme geschützt werden. Bei einer 3-Tier-Webanwendung liegt oft vor jedem Tier eine Firewall (ggf. ergänzt um Intrusion-Prevention-Funktionen), welche die Kommunikation filtert. Diese Firewalls müssten dann idealerweise Bestandteil der Gesamtplattform beim Cloud Provider sein. Ähnliches gilt für den Einsatz einer WAF. Für eine Web-Anwendung sind meist auch Authentisierungsdienste erforderlich und selbstverständlich müssen Daten nicht nur beim Transport, sondern auch bei der Ablage geschützt werden. Als Folge ist PaaS ohne Security as a Service in vielen Fällen nur schwer denkbar.

Automatisierung ist ein wesentlicher Kernbestandteil der Cloud-Idee (und moderner Rechenzentren). Die physikalische Infrastruktur muss hierzu von Diensten, Applikationen und damit den logischen Strukturen so weit entkoppelt werden, dass die Einrichtung (das „Provisioning“) von Diensten und Applikationen in der Regel ausschließlich auf der logischen Ebene erfolgt. Dies bedeutet konsequente Virtualisierung auf allen Ebenen der Infrastruktur. Hierzu wird mit Overlay-Techniken gearbeitet, die von der zugrundeliegenden