Quelle: archidea – 123RF

Azure mit lokalen Netzwerken verbinden

Cloud dahoam

von Thomas Joos

Azure bietet vielfältige Möglichkeiten, um Ressourcen in der Cloud mit lokalen Netzwerken zu verbinden. Dazu gehören auch Sicherheitsmechanismen und Loadbalancer, die den Datenverkehr zwischen Cloud und lokalem Rechenzentrum nicht nur zur Verfügung stellen, sondern absichern und hochverfügbar konfigurieren. IT-Administrator zeigt die Wege auf, um die Cloudumgebung mit dem lokalen Netzwerk zu verbinden.

Um Serverdienste, Ressourcen oder VMs in Microsoft Azure miteinander zu verbinden, stehen verschiedene Netzwerkfunktionen zur Verfügung. Mit den Netzwerkdiensten lassen sich nicht nur Cloudressourcen in Azure verknüpfen, sondern auch mit dem eigenen Unternehmensnetzwerk verbinden. Das ermöglicht die Kommunikation zwischen der Cloud und lokalen Netzwerken. Hier seien zum Beispiel die virtuellen Netzwerke genannt. Diese sind Basis der Verbindung verschiedener Objekte in Azure und bieten eine Vielzahl an Möglichkeiten zur Kommunikation zwischen Cloudkomponenten und lokalen Servern.

Virtuelle Netzwerke verstehen

Bei der Verwaltung der virtuellen Netzwerke spielen auch die Subnetze eine Rolle, mit denen sich virtuelle Server und andere Dienste in Azure voneinander trennen lassen. Das ist auch bei der Verbindung einzelner Ressourcen in den virtuellen Netzwerken für die Anbindung an Netzwerken im Unternehmen wichtig. Die IP-Adressen in den Subnetzen lassen sich frei definieren.

Die IP-Adressen kommen innerhalb des virtuellen Netzwerks und der in diesem Netzwerk verbundenen Server zum Einsatz. Virtuelle Netzwerke und Subnetze erstellen Sie in der Verwaltungsoberfläche von Azure oder mit Skripten über die PowerShell. Zwischen den Subnetzen eines virtuellen Netzwerks erstellt Azure automatisch Routen. Das heißt, die Server in den verschiedenen Subnetzen können miteinander kommunizieren. Azure verteilt per DHCP automatisch IP-Adressen in den virtuellen Netzwerken. Natürlich lassen sich für einzelne Objekte, zum Beispiel VMs, innerhalb eines virtuellen Netzes auch statische IP-Adressen vergeben.

Subnetze können Sie jederzeit nachträglich zu den virtuellen Netzwerken hinzufügen. In den Einstellungen von virtuellen Netzwerken lässt sich für jedes festlegen, ob es auch mit anderen Netzen kommunizieren oder an Firmennetzwerke angebunden werden soll. Für die Integration in ein lokales Unternehmensnetz kommt das Azure-VPN-Gateway oder ExpressRoute zum Einsatz. Lokal muss daher ein Endgerät positioniert sein, das diese Technologien unterstützt.

Sie können die Einstellungen virtueller Netzwerke jederzeit anpassen. So erstellen Sie zum Beispiel weitere Subnetze, fügen Gateways hinzu, binden lokale Netzwerke an und vieles mehr. Auch die DNS-Server lassen sich jederzeit konfigurieren und erweitern. In den Einstellungen von VMs sind die zugeordneten virtuellen Netzwerke zu sehen. Diese verwalten Sie im Webportal von Azure im Bereich "Virtuelle Netzwerke". Buchen Sie anschließend virtuelle Server oder Clouddienste, können Sie im Assistenten zum Erstellen des neuen Objekts das jeweilige virtuelle Netzwerk auswählen. Verfügt dieses über ein VPN-Gateway oder eine ExpressRoute in das lokale Rechenzentrum, kann auch hier eine Kommunikation erfolgen. Eine neue ExpressRoute-Leitung wird ebenfalls im Webportal erstellt.

Aber nicht nur beim Erstellen von virtuellen Servern steht das virtuelle Netzwerk in Azure zur Verfügung, auch in den Assistenten zum Anlegen von Clouddiensten. So besteht zum Beispiel die Möglichkeit, einen Hadoop-Cluster auf Basis von Azure HDInsight in einem gemeinsamen virtuellen Netzwerk mit verschiedenen anderen Windows- oder Linux-Servern zu betreiben. Verfügt das virtuelle Netz über ein Azure-VPN-Gateway oder eine ExpressRoute, wird auch hier die Kommunikation weitergeleitet.

Virtuelle Netzwerke erstellen

Über den Menüpunkt "Virtuelle Netzwerke" legen Sie wie erwähnt mithilfe eines Assistenten ein neues Netzwerk an. Dabei geben Sie auch die IP-Adresse des DNS-

Servers im virtuellen Netzwerk an und bauen eine Verbindung zum Unternehmensnetzwerk auf, zum Beispiel über ein VPN. Als DNS-Server lassen sich an dieser Stelle auch welche aus dem Internet oder aus dem Unternehmensnetzwerk hinterlegen, wenn eine Anbindung an das Firmennetzwerk per VPN konfiguriert ist. Durch diese Verbindung lassen sich in dem Fall Daten zwischen Azure und dem lokalen Unternehmensnetzwerk austauschen. Die Anbindung an das Unternehmensnetzwerk erfolgt auf Basis eines IPSec-VPNs.

Sobald das Unternehmensnetz mit dem virtuellen Azure-Netzwerk verbunden ist, können die Clouddienste auf Ressourcen im Unternehmen zugreifen und Anwender und Serverdienste sind in der Lage, im lokalen Netzwerk auf die Clouddienste und virtuellen Computer in Azure zuzugreifen. Sie können beim Erzeugen eines neuen virtuellen Netzwerks auch Adressräume darin erstellen. Azure routet automatisch alle Subnetze und Adressräume, die Sie anlegen. Erzeugen Sie neue Subnetze, werden diese automatisch geroutet. Sie können für Subnetze auch benutzerdefinierte Namen festlegen. Diese finden Sie dann in den verschiedenen Assistenten zum Erstellen neuer Ressourcen, zum Beispiel virtueller Server, sodass sich Subnetze leichter zuordnen lassen. Klicken Sie auf "Erstellen", um das virtuelle Netzwerk mit den Einstellungen zu konfigurieren, die Sie im Assistenten festgelegt haben. Den Fortschritt des Vorgangs sehen Sie im Nachrichtenbereich von Azure.

Alle virtuellen Netzwerke, die in einem Azure-Abonnement vorhanden sind, lassen sich im Webportal über den Bereich "Virtuelle Netzwerke" auch nachträglich anpassen. Dazu klicken Sie auf das entsprechende Netzwerk und im sich öffnenden Fenster können Sie anschließend VPNs konfigurieren, DNS-Server für das Netzwerk festlegen sowie weitere Subnetze anlegen und vieles mehr. Im Dashboard des virtuellen Netzwerks sind die Ressourcen zu sehen, die das virtuelle Netzwerk nutzen. Bei der Planung des Adressraums von IP-Adressen müssen Sie darauf achten, dass sich die IP-Adressen nicht mit anderen überschneiden, auch nicht mit den IP-Adressen im Unternehmen, wenn

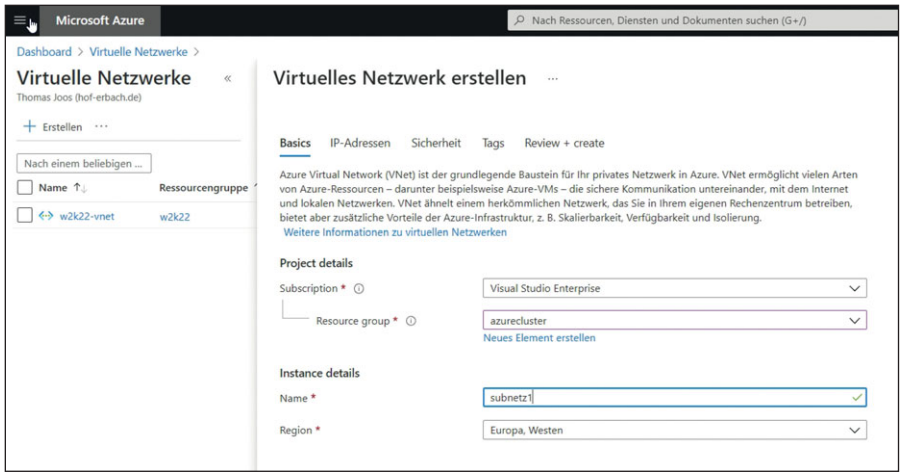

Bild 1: Virtuelle Netzwerke lassen sich flexibel in Azure erstellen

das virtuelle Netzwerk an das Unternehmensnetzwerk angebunden werden soll.

Connection Broker anbinden

Lokale Netzwerke können auch direkt über das Internet auf Dienste in Azure zugreifen, etwa für hochverfügbare IT-Umgebungen. Dazu sind weder virtuelle Netzwerke noch VPNs notwendig. Remotedesktop-Sitzungshosts nutzen zum Beispiel für Hochverfügbarkeit den Connection Broker. Um diesen aus dem lokalen Netzwerk an Azure anzubinden, müssen Sie den nativen SQL-Client installieren [1]. Dieser wird auch benötigt, wenn Sie einen eigenen Datenbankserver für die Hochverfügbarkeit mit RDS aufspielen. Anschließend konfigurieren Sie im Server-Manager über das Kontextmenü des Connection Brokers die Hochverfügbarkeit der RDS-Umgebung. Bei der Einrichtung hilft ein Assistent. Wählen Sie als Option "Freigegebener Datenbankserver" aus. Anschließend geben Sie den DNS-Namen zu Ihrer Datenbank in Azure ein und die kopierte Verbindungszeichenfolge inklusive der angepassten Daten zur Anmeldung.

Nun erfolgt die Anbindung. Ist diese erfolgreich abgeschlossen, wird die Azure-SQL-Datenbank verwendet. Binden Sie weitere Connection Broker an, lassen sich diese auf dem gleichen Weg verbinden. Dadurch erreichen Sie eine Hochverfügbarkeit für den Connection Broker über Azure. Sie können also virtuelle Netzwerke mit lokalen vermischen und Serverdienste von Windows Server ab Version 2016 zusammen mit Azure und virtuellen Netzwerken betreiben. Serverdienste wie

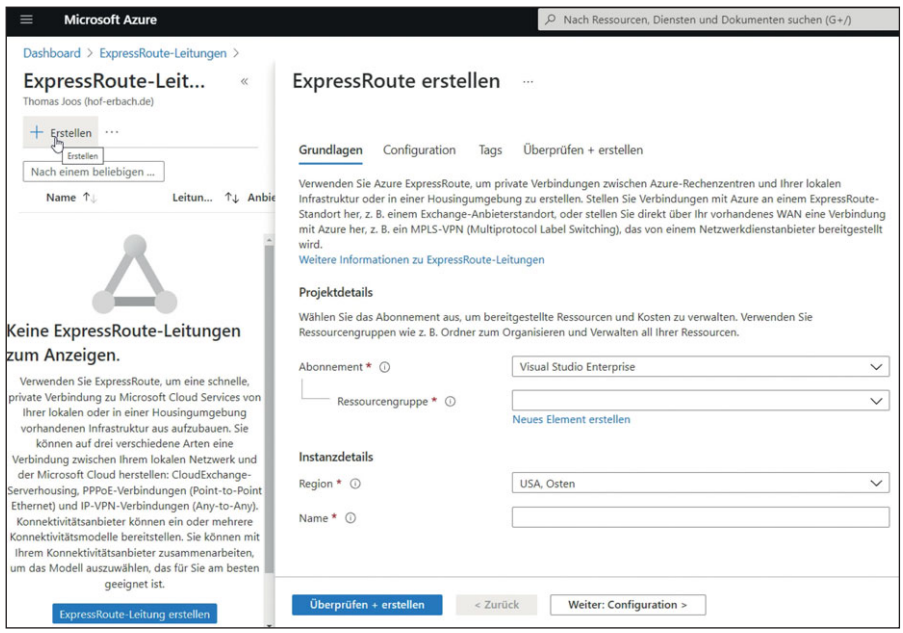

Bild 2: Neue ExpressRoute-Leitungen werden ebenfalls im Webportal erzeugt.

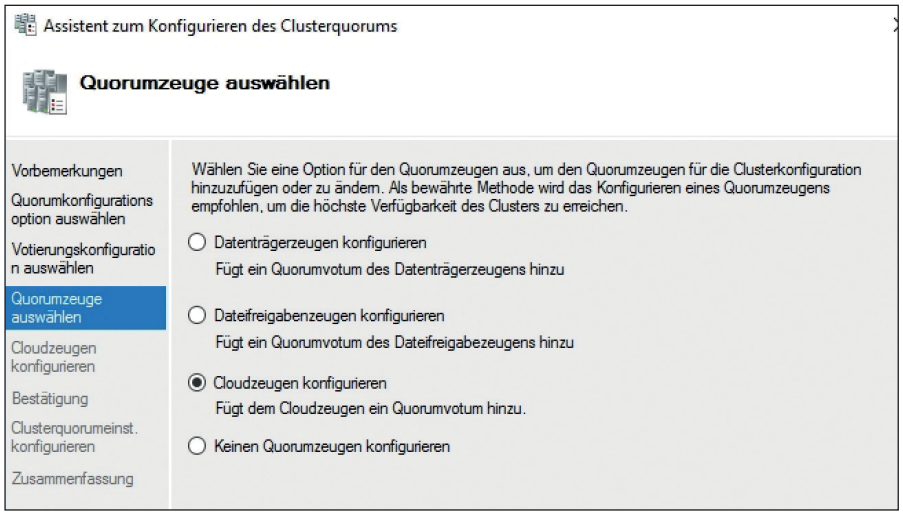

Bild 3: Die Anbindung an Azure als Cloudzeuge erfolgt zum Beispiel im Failovercluster-Manager von Windows Server oder im Windows Admin Center.

Azure SQL können die virtuellen Netzwerke ebenfalls nutzen, um sich mit anderen Azure-Diensten oder Diensten in lokalen Netzwerken zu verbinden.

Cloud Witness mit Azure

Mit Windows Server ab 2016 und Azure lagern Sie bei Bedarf die Zeugenfunktion eines Clusters in die Cloud aus. Dadurch erhalten Sie eine effektive Überwachung des Quorums eines Clusters. Für global verteilte Cluster verbessern Sie so deren Effizienz erheblich und erleichtern die Verwaltung. Grundlage für Cloud Witness in einem Cluster mit Windows Server und Azure Stack HCI ist die Vorbereitung des passenden Azure-Storage-Accounts (Speicherkonto). In diesem lagert das Blob-File, in dem die Zeugen Daten für den Cluster speichern. Dazu fügen Sie im Azure-Portal mit "Speicherkonten" ein neues Speicherkonto hinzu. Sie finden den Menüpunkt am schnellsten über die Suche im Azure-Portal. Wählen Sie im Bereich "Replikation" die Option "Lokal redundanter Speicher (LRS)" aus.

Das Erstellen eines Speicherkontos dauert eine gewisse Zeit. Wichtig zur Anbindung Ihrer Clusterknoten sind die Zugriffsschlüssel des Speicherkontos. Diese müssen Sie im Azure-Portal abrufen, damit Sie diese auf den Clusterknoten verwenden können. Die beiden Schlüssel sind über den Menüpunkt "Zugriffsschlüssel" in der Verwaltung des Speicherkontos zu finden. Mit dem Speicherkonto erstellt Azure auch eine URL, über die das Speicherkonto von extern erreichbar ist. Diese hat das Format "https://<Storage Account Name>.<Storage Type>.<Endpoint>", zum Beispiel: https://cloudwitnessjoos.blob.core.windows.net.

Sobald das Speicherkonto angelegt ist, können Sie das Quorum des Clusters anpassen. Am schnellsten geht das, wenn Sie im Failovercluster-Manager im Kontextmenü des Clusters die Option "Weitere Aktionen / Clusterquorumeinstellungen konfigurieren" nutzen. Hier können Sie über einen Assistenten die Quorum-Konfiguration anpassen. Für die Anbindung an Azure verwenden Sie "Erweiterte Quorumkonfiguration" und klicken auf "Weiter", bis Sie auf der Seite "Quorumzeuge auswählen" sind. Hier wählen Sie die Option "Cloudzeugen konfigurieren".

Im nächsten Fenster geben Sie den Namen des Speicherkontos ein, das als Cloudzeuge verwendet werden soll, und tragen den Zugriffsschlüssel ein. Danach schließt der Assistent die Anbindung an Azure ab. Sie können die erfolgreiche Anbindung im Azure-Portal überprüfen. Klicken Sie auf das Speicherkonto und dann auf "Blobs", sehen Sie den neuen Container "msft-cloud-witness". Dabei handelt es sich um den Container für die Blob-Datei für den Cluster. Klicken Sie auf den Container, sehen Sie die Zeugendatei. Der Name der Datei entspricht der GUID des Clusters. Im Failovercluster-Manager klicken Sie auf den Cluster und sehen dann in der Mitte des Fensters bei "Hauptressourcen des Clusters" den Cloudzeugen – dieser muss "aktiv" geschaltet sein. Per Doppelklick auf die Ressourcen rufen Sie deren Eigenschaften auf. Hier muss der "Status" die Option "Online" anzeigen.

Virtuelle Firewalls hochziehen

Im Bereich der Kommunikation von Ressourcen in Azure und virtuellen Netzwerken, die wiederum eine Verbindung mit lokalen Netzwerken aufbauen können, spielen auch die Netzwerksicherheitsgruppen (Network Security Groups, NSG) eine wichtige Rolle. NSGs arbeiten mit Richtlinien, um Datenverkehr über verschiedene Netzwerke oder Subnetze hinweg zu sichern. Wenn Sie Objekte, die in Azure mit dem Netzwerk kommunizieren, an eine NSG anbinden, werden die Sicherheitsrichtlinien sofort angewendet. Dabei kann es sich um Subnetze, ganze virtuelle Netzwerke oder VMs handeln. NSGs sind im Grunde genommen also flexible virtuelle Firewalls in Azure, die sich an verschiedene Objekte in der Cloud binden lassen. Dadurch wird auch der Datenverkehr in lokale Unternehmensnetzwerke beeinflusst.

Die Richtlinien einer NSG blockieren standardmäßig den kompletten Datenverkehr. Administratoren müssen festlegen, welche Datenströme sie zulassen wollen. Der erlaubte Verkehr wird in den Richtlinien definiert. NSGs müssen Sie aber nicht an komplette virtuelle Netzwerke oder an Subnetze koppeln, auch die Anbindung an einzelne VMs ist möglich.

NSGs können alle Daten filtern, die angebundene Objekte in den Rest des Netzwerks schicken, inklusive des Unternehmensnetzwerks. Die Konfiguration des erlaubten Datenverkehrs nehmen Sie über Eingangs- und Ausgangssicherheitsregeln vor. NSGs ermöglichen das Filtern per Netzwerkprotokoll, den Quell-IP-Adressbereich, den Quellportbereich, den Ziel-IP-Adressbereich und den Zielportbereich. Es lassen sich also durchaus flexible Regeln erstellen, die den Datenverkehr in alle Richtungen steuern. NSGs können Sie problemlos mehreren Objekten in Azure zuordnen, allerdings kann jedes Objekt in Azure nur eine NSG nutzen.

Sicherheitsregeln lassen sich zudem priorisieren. Existieren mehrere Regeln für eine NSG, wertet diese die einzelnen Richtlinien in der entsprechenden Reihenfolge aus. Die Regeln für ein- und ausgehenden Datenverkehr sind über eigene Menüpunkte definierbar, damit jederzeit genau zu erkennen ist, welche Regeln existieren. Für ein- und ausgehende Regeln lassen sich jeweils eigene Prioritäten festlegen. Für die Bereitstellung von NSGs kommen auch Automatisierungsskripte infrage. Bei "Zugriffsteuerung (IAM)" steuern Sie, welche Azure-Benutzer das Recht erhalten, die Regeln der NSG sowie die komplette NSG zu verwalten.

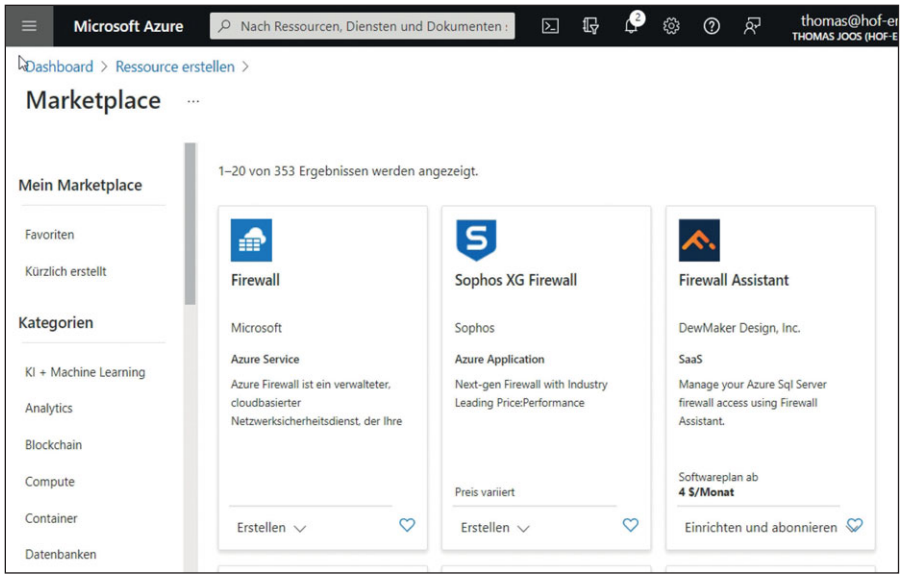

Bild 4: Der Azure-Marketplace bietet zahlreiche virtuelle Appliances für den Netzwerkbereich.

Virtuelle Firewalls von Drittanbietern nutzen

Unternehmen, denen die Standard-Sicherheitsfunktionen in Azure nicht ausreichen, können über den Azure Marketplace virtuelle Appliances lizenzieren, die die Sicherheit im virtuellen Cloudnetzwerk verbessern und flexibler steuerbar machen. Die Aufgabe von virtuellen Firewalls besteht auch darin, die Netzwerkverbindungen in hybriden Netzwerken abzusichern. So lässt sich der Datenverkehr zwischen verschiedenen lokalen Rechenzentren und der Cloud absichern. Solche Appliances sind allerdings keine Dienste in Azure, sondern kommen normalerweise als VM daher.

Eine bekannte virtuelle Firewall in diesem Bereich ist die Next-Generation-Firewall (NGFW) von Barracuda. Diese steht für lokale Netzwerke zur Verfügung und bietet in Azure den gleichen Funktionsumfang. Barracuda stellt zudem eine Appliance bereit, die mehrere virtuelle Firewalls zentral verwaltet. Sie können mit der Appliance also nicht nur die Firewalls in Azure managen, sondern auch die Firewalls zu anderen Clouddiensten wie AWS sowie die lokalen Firewalls und die Kommunikation zwischen diesen Firewalls. Die Next-Generation-Firewall von Barracuda unterstützt auch die Azure-ExpressRoute-Verbindungen, die Sie im Netzwerkbereich des Webportals erstellen. Dabei handelt es sich um direkte Verknüpfungen von Azure mit lokalen Unternehmensnetzwerken. Auf Wunsch lassen sich auch andere Clouddienste von Microsoft anbinden, zum Beispiel Microsoft 365. Weitere prominente Vertreter von Firewalls im Azure-Marketplace stammen etwa von Sophos, VT Air Next Generation Enterprise Firewall und SonicWall NSv.

Multi-Site-VPNs

Betreiben Unternehmen mehrere Niederlassungen, die per VPN miteinander verbunden sind, können in Azure Multi-Site-VPNs zum Einsatz kommen. Dabei werden virtuelle Netzwerke in Azure mit verschiedenen lokalen Standorten des Unternehmens per VPN verbunden. Die Verbindungen zwischen den virtuellen Netzwerken können darüber hinaus mit den bereits erwähnten Netzwerksicherheitsgruppen oder durch Appliances von Drittanbietern abgesichert werden. Dadurch vernetzen Unternehmen ihre Netzwerke und Clients weltweit über Azure miteinander. Verschiedene Azure-Abonnements lassen sich dadurch ebenfalls miteinander verbinden, auch mit lokalen Netzwerken.

Damit Sie Multi-Site-VPNs einsetzen können, muss das entsprechende Endgerät im lokalen Rechenzentrum kompatibel mit Azure und den Netzwerkfunktionen des Clouddienstes sein. Das VPN-Gerät muss dynamisches Routing unterstützen, damit eine Verbindung zu virtuellen Netzwerken in Azure hergestellt werden kann. Beim Einsatz einer Firewall in Azure müssen Sie sicherstellen, dass die Firewall die Funktion ebenfalls unterstützt.

ExpressRoute-Verbindungen sind derweil besonders wichtig, wenn Sie Ihr lokales Netzwerk mit Azure verbinden. Drittherstellter-Appliances unterstützen diese Funktionen, um virtuelle Azure-Netzwerke mit lokalen Netzwerken oder anderen Clouddiensten zu vernetzen. Firewalls, wie die bereits erwähnte Next Generation Firewall von Barracuda, können den Datenverkehr von ExpressRoute-Verbindungen zusätzlich verschlüsseln und nach unerwünschtem Datenverkehr oder Malware durchsuchen.

Fazit

Azure bietet verschiedene Möglichkeiten, um Ressourcen in der Cloud miteinander zu vernetzen, aber auch lokale Rechenzentren anzubinden. Der beste Weg dahin besteht zunächst darin, dass das Endgerät im Unternehmensnetzwerk kompatibel mit Azure ist und die einzelnen Dienste wie Virtual Networks, Multi-Site-VPNs und ExpressRoutes unterstützt. Erstellen Sie die Netzwerkverbindungen im Webportal, können Sie den Datenverkehr testen. Kompatible Firewalls im lokalen Netzwerk können auf diese virtuellen Objekte zugreifen und den Datenverkehr zwischen Azure und lokalem Rechenzentrum effektiv verwalten und absichern. *(jp)*

Link-Codes

[1] **Microsoft ODBC-Treiber für SQL Server**
h1z32