Maximale VPN Kapazität für Homeoffice in Krisenzeiten

Skalierbares Remote Access VPN via AWS

Hier erfahren Sie...

- ... wie mit AWS ein skalierbares Remote Access VPN erstellt werden kann.
- ... wie Sie Schritt für Schritt die Netzwerkkonfiguration aufbauen.
- ... wie Sie ein skalierbares Remote Access VPN via AWS mit FortiGate und SD-WAN aufbauen.

matrix technology AG
Nymphenburger Str.1, 80335 München
Telefon +49 89589395-600
Telefax +49 89589395-711

Inhaltsverzeichnis

1 Vorwort

März 2020: Aufgrund der Corona-Krise schicken viele Unternehmen ihre Mitarbeiter ins Homeoffice. Sofern auf lokale Unternehmensressourcen zugegriffen werden muss, wird ein Remote Access VPN verwendet. Häufig sind diese Lösungen jedoch nur für einen Bruchteil der Belegschaft dimensioniert, da im Normalbetrieb nur wenige Mitarbeiter gleichzeitig diese Lösung verwenden. In Krisenzeiten kann die massive Nutzung durch das Gros der Belegschaft zu Engpässen und teils massiven Verfügbarkeitsproblemen führen.

Dieses Whitepaper zeigt auf, wie die Public Cloud von Amazon Web Services (kurz: AWS) verwendet werden kann, um einen deutlich skalierbareren Zugang zu erstellen, der gleichzeitig aus wirtschaftlicher Sicht nur so lange bezahlt wird, wie er auch genutzt wird. Da im Prinzip keine neue Hardware notwendig ist und damit nicht auf Lieferungen gewartet werden muss, können die Maßnahmen zeitnah umgesetzt werden.

Im ersten Teil dieses Whitepapers soll die einfachere und preisgünstigere Lösung vorgestellt werden, die aber mit weniger Sicherheitsfeatures agiert. Im zweiten Teil des Whitepapers wird eine Lösung mit deutlich höherer Funktionalität und mehr Sicherheitsfeatures vorgestellt, die außerdem SD-WAN Technologie nutzt, um die Last des VPN-Verkehrs auf mehrere Internetanschlüsse einer Firma zu verteilen.

2 Technische Problembeschreibung

Der erste Gedanke, der sich in der Kombination der Begriffe “Performance Problem” und “VPN” auftut, ist meist die eigentliche Verschlüsselung – welcher Algorithmus „frisst“ wieviel CPU und wie schnell ist die darunterliegende Leitung. Erfahrene Netzwerkadministratoren betrachten dann zudem noch Paketlaufzeiten und Paketgrößen (Stichwort: MTU-Problematik).

Bei Site2Site-Verbindungen, die beispielsweise zwei Unternehmensstandorte vernetzen, sind diese meist über IPSEC-VPNs realisiert und terminieren häufig auf den Firewalls oder Routern. Sind diese Geräte dedizierte Netzwerk Hardware, so besitzen sie häufig spezielle ASICs, die dafür sorgen, dass die mathematisch aufwendigen Operationen des Verschlüsselns in Hardware umgesetzt werden. Eine für die Betrachtung in diesem Whitepaper aber wesentliche Eigenschaft ist, dass diese VPNs sehr statisch sind. Sie haben in der Regel wohldefinierte Endpunkte und sind meist ständig in Betrieb.

Im Unterschied hierzu sind Remote Access VPNs sehr viel dynamischer. Sie werden ständig auf- und abgebaut. Die Endpunkte sind dynamisch, da der von Zuhause arbeitende Mitarbeiter hinter privaten Anschlüssen ohne feste Adressen sitzen. Dazu kommt, dass es (vor allem in Krisenzeiten) viele parallele Verbindungen sind, die mit individuellen Parametern bedient und verwaltet werden müssen. Darüber hinaus – und das ist je nach Hersteller der Remote Access-Lösung unterschiedlich – verwenden die Verbindungen häufig statt IPSEC- sogenannte SSL-VPN-Technologien, bei denen der Verkehr mittels derselben Protokolle verschlüsselt wird, wie beim Zugriff auf Webseiten. Dies ist aber wiederum je nach Hersteller nicht mehr Hardware-optimiert, so dass die gewöhnliche CPU der Appliance verwendet wird, die bei einem Massenansturm auch in die Knie geht.

Abschließend greift beim Remote Access noch ein weiterer Aspekt, der ebenfalls häufig zum Engpass wird: Die Lösung ist benutzerorientiert, das heißt, dass in den meisten Fällen eine Anmeldung am intern führenden System stattfindet. Häufig bedeutet dies eine Kopplung mit Microsofts Active Directory Service. Je nach Effizienz dieser Kopplung, scheitert der Betrieb der Lösungen häufig daran, dass diese Kopplung überlastet ist, oder, was noch schlimmer wäre, die AD Server mit zu vielen Anfragen überlastet werden.

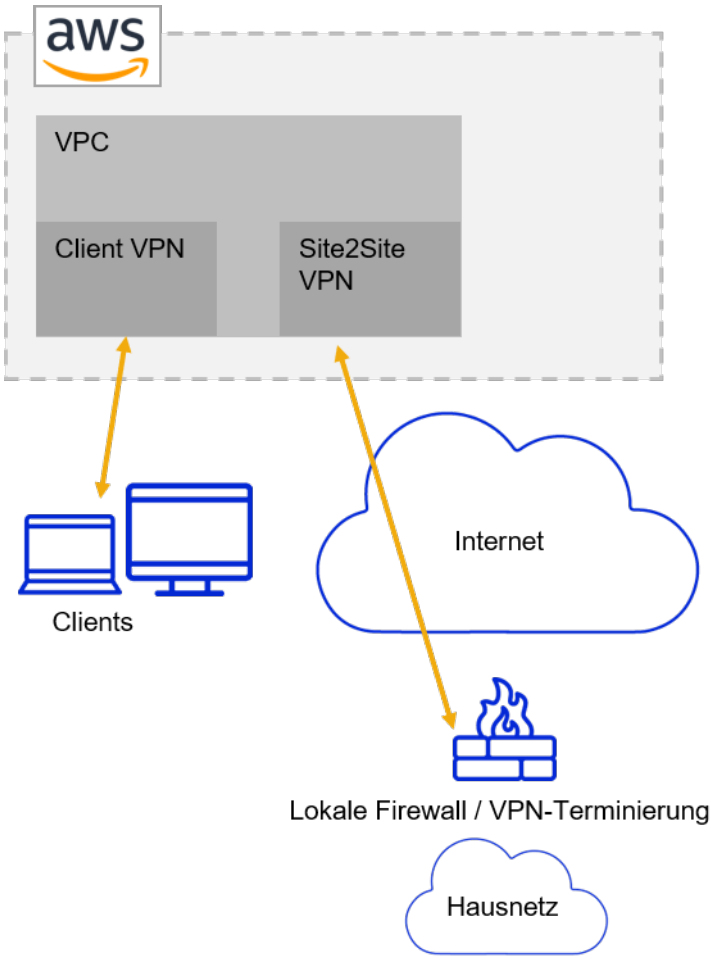
Der finale Flaschenhals ist die Internetanbindung. Viele Unternehmen haben eine Anbindung, die zwar für den normalen Betrieb reicht, aber eben nicht dafür, dass alle Mitarbeiter darüber ihren normalen Bürotätigkeiten nachgehen. Hierzu wird im zweiten Teil des Whitepapers gezeigt, wie die Last mit günstigeren Consumer-Leitungen und SD WAN-Technologie abgefedert werden kann.

3 Skalierbares Remote Access VPN via AWS

AWS bietet seinen Kunden zwei VPN-Technologien, die eigentlich dafür gedacht sind, gesicherten Zugriff auf Ressourcen in AWS zuzulassen, die nicht frei über das Internet erreichbar sind. Hier gibt es zum einen einen Site2Site VPN-Service auf IPSEC-Basis und zum anderen ein Remote Access VPN auf Basis der weit verbreiteten Software Open VPN. Beide Funktionen gibt es als SaaS-Angebot. Das bedeutet, dass keine virtuellen Maschinen installiert und betrieben werden müssen, sondern die Funktion einfach gekauft werden kann. Für die ausreichende Skalierung sorgt AWS dabei im Hintergrund.

Beide VPN-Technologien dienen zum Zugriff auf eine Virtual Private Cloud (kurz: VPC) in AWS. Dies ist ein geschlossener Netzwerkbereich mit eigenen privaten IP-Adressen, der so aus dem Internet nicht erreichbar ist. Eine geeignete Netzwerkkonfiguration kann aber dazu verwendet werden, den Verkehr aus dem Remote Access VPN über das Site2Site VPN wieder in das Firmennetzwerk zu leiten. Abbildung 1 verdeutlicht schematisch wie der Verkehrsfluss abläuft.

Abb. 1: Verkehrsfluss VPN / Site2Site VPN



3.1 Aufbau der Netzwerkkonfiguration

Für den Aufbau sind einige Arbeitsschritte notwendig, die auch von den vorhandenen Gegebenheiten abhängen. In diesem Beispiel gibt es im eigenen Rechenzentrum eine Firewall der Firma Fortinet, diese kann aber auch von einem der anderen gängigen Hersteller am Markt sein. Selbst eine Linux- oder Windows-Instanz, die beide IPSEC-VPNs beherrschen, könnte diese Aufgabe übernehmen.

Step 1: VPC

Im ersten Schritt wird ein dedizierter VPC in der AWS Region der Wahl (für den deutschen Markt in der Regel Frankfurt) angelegt. Bei Anlage des VPCs muss der Administrator ein IPv4-Netz angeben, welches als Hauptnetz für diese virtuelle Private Cloud gilt. Daher sollte dieses Netz nicht zu klein sein, und sich auch nicht mit den internen Netzen überschneiden. Allerdings werden aus diesem Netz lediglich zwei kleine Subnetze als Transfernetze benötigt, so dass ein /27er Netzblock ausreicht.

Step 2: Subnetze

Im zweiten Schritt werden zwei Subnetze innerhalb dieses VPCs angelegt. Hier sollte im Dialog darauf geachtet werden, dass die beiden Subnetze in zwei verschiedenen Availability Zones liegen, um Redundanz zu gewährleisten.

Step 3: Internet Gateway

Nun muss ein Internet Gateway angelegt werden, damit die VPN-Zugänge, die später dazu konfiguriert werden, auch eine Verbindung zum Internet haben.

Step 4: Site2Site VPN

Dieser Arbeitsschritt umfasst mehrere Einzelschritte:

- **Erzeugen eines Customer Gateways**: Dies ist die AWS Entität, die das eigene VPN Gateway, in unserem Beispiel die lokale Fortinet Firewall, beschreibt. Hier gibt der Admin einen Namen sowie die extern sichtbare IP-Adresse an und wählt aus ob statisches oder dynamisches Routing verwendet werden soll. Letzteres kann dynamisch via BGP geschehen, wenn das lokale Gerät dies unterstützt. Sonst müssen die Routen in Richtung des Firmennetzes in AWS manuell auf das VPN Gateway gerichtet werden.
- **VPN Gateway:** Dies ist der Partner auf AWS-Seite, der den Tunnel hier terminiert. Dieser muss nach dem Erzeugen noch dem VPC zugeordnet werden.
- **Site2Site-Connection:** Nachdem AWS beide Partner kennt, kann nun die eigentliche Site2Site-Connection erstellt werden. Hier werden beide Gateways eingetragen und nochmals ausgewählt, ob das Routing statisch oder dynamisch erfolgen soll. Es ist möglich, loopback Adressen für die Tunnel zu definieren. Darüber hinaus kann der Admin hier eigene pre shared secrets für die Tunnel eingeben. Alternativ werden sowohl die Adressen als auch die Passwörter von AWS generiert.

Nachdem der Tunnel angelegt wurde, bietet die AWS Console die Möglichkeit, die Konfiguration für eine große Reihe gängiger, VPN fähiger Netzwerkendgeräte herunterzuladen. Was hierbei besonders ist: AWS legt aus Redundanzgründen grundsätzlich zwei Tunnel an, so dass auch auf der eigenen Seite beide Tunnel definiert und mit einem entsprechenden Fail Over versehen werden können.

Liegt das eigene Gerät noch hinter Network Address Translation (NAT), so ist die heruntergeladene Konfiguration gegebenenfalls anzupassen.

Step 5: Routing

Die Routingtabelle der Transfernetze muss wissen, dass es das VPN Gateway gibt. Zumindest der Traffic in den lokalen Adressbereichen muss auf das VPN Gateway zeigen, welches in AWS Routing Tabellen das Ziel einer Route sein kann. Es ist aber auch möglich, die Defaultroute auf das VPN Gateway zu setzen, da das VPC keinen Internet-Breakout benötigt.

Step 6: Remote Access VPN

Bevor mit der Arbeit begonnen werden kann, ist zunächst eine Entscheidung zu treffen, wie die Benutzer sich an diesem VPN künftig anmelden sollen. Zur Auswahl stehen hier Active Directory (kurz: AD) oder Zertifikate. Bei AD kann ausgewählt werden,

ob ein lokal in AWS gehostetes AD oder ein lokales AD, welches über AD-Kopplung mit AWS verbunden ist, verwendet werden soll. Letzteres hat den Vorteil, dass alle bestehenden Benutzer Zugriff haben. Dieses hat aber auch den Nachteil, dass nur eine einfache Authentisierung stattfindet. Bei Authentisierung mit Zertifikaten kann entweder die eigene Certificate Authority (kurz: CA) oder der CA-Service von AWS verwendet werden. Auf jeden Fall benötigt der Client VPN Server (dies ist der Name für das Remote Access VPN in AWS) ein Serverzertifikat. Im Beispiel-Aufbau wurde die Zertifikatsoption gewählt, so dass jeder Benutzer ein individuelles Client-Zertifikat aus der CA bekommt. Das Erstellen der Zertifikate übernimmt im Testaufbau der AWS Certificate Manager mit einer privaten CA, da die Zertifikate ja nicht von Browsern evaluiert werden müssen.

Nachdem das Server Zertifikat erstellt wurde, kann der Client VPN Endpoint erzeugt werden. Dieser benötigt einen symbolischen Namen und einen IPv4 Adressblock, aus dem die Clients bedient werden. Dieser Adressblock sollte entsprechend der zu erwartenden gleichzeitigenden Benutzer dimensioniert werden. Da dieser Block durch den Dienst genatted wird, kann im Prinzip ein beliebiger Block verwendet werden. Es sollte aber keine Überschneidung mit den Zieladressen im eigenen Netz geben. In dieser Konfiguration kann auch noch ein DNS Server mitgegeben werden, den die Clients verwenden sollen. Hier bietet sich der interne DNS Server hinter dem VPN an.

Step 7: VPN Endpoint

Zum Abschluss muss der VPN Endpoint noch dem richtigen Subnetz zugewiesen werden. Dies geschieht über den AWS Menüpunkt „association“. Der letzte Arbeitsschritt ist nun noch eine Route in der Routingtabelle des VPN-Endpoints. Diese enthält per Default nur das Subnetz des VPCs. Die Netze im Hausnetz müssen hier mit dem des Subnetzes eingetragen werden. Die Routingtabelle des Subnetzes ihrerseits sorgt dann wieder dafür, dass die Pakete im VPN Tunnel landen.

3.2 Bewertung

Diese Konfiguration kann je nach verwendeter Authentisierungsmethode extrem kosteneffizient sein. Es ist zudem zu bedenken, dass der Schutz der Clients hier nicht kontrolliert wird. Einzig am VPN-Ausgang in das lokale Netz, kann der so eintretende Traffic höheren Kontrollen (Virenscanner, Intrusion Detection etc.) unterworfen werden. Des Weiteren gibt es innerhalb des VPCs eine kurze Strecke, in der der Client Traffic unverschlüsselt übermittelt wird.

Demgegenüber steht der gut kalkulierbare Preis. Das Site2Site VPN kostet ca. 40,- €/Monat zzgl. des Traffics. Der VPN Client Endpoint 10 Cent/Stunde = 72,- €. Hier kommen pro VPN Client und Stunde 5 Cent hinzu. Somit lässt sich abhängig von der Benutzerzahl gut kalkulieren, was diese Erweiterung kostet. Kosten entstehen darüber hinaus nur nach verbrauchter Leistung.

4 Skalierbares Remote Access VPN via AWS mit FortiGate und SD-WAN

Wie bereits beschrieben, sind Infrastrukturen für den Remote Access von Mitarbeitern in der Regel auf einen gewissen Prozentsatz der Mitarbeiter skaliert und den massiven Anforderungen in Krisenzeiten häufig nicht gewachsen. Im ersten Teil des Whitepapers wurde eine Infrastruktur vorgestellt, welche die Skalierungsprobleme in der Kernfunktion des SSL VPN adressiert. Was diese Lösung jedoch nicht mitigiert, sind Kapazitätsprobleme im Internetzugang. Darüber hinaus bietet die Lösung keinen Schutz im VPN Client – lediglich der Traffic in das Hausnetz kann kontrolliert werden.

Im Folgenden wird eine weitere Lösung vorgestellt, die diese Aspekte abdeckt. Jedoch werden die nativen AWS-Dienste Site2Site VPN und Client VPN durch eine virtuelle Appliance der Firma Fortinet ersetzt, die beide VPN-Verbindungen terminiert und mittels SD-WAN-Technologie ermöglicht, die benötigte Bandbreite über mehrere Leitungen in das Firmennetz zu verteilen. Die Appliance läuft in AWS und kann dort auch als Cluster betrieben werden. In der Performance kann sie durch Anpassen der Instanzparameter nach oben skaliert werden.

4.1 Lastverteilung per SD-WAN

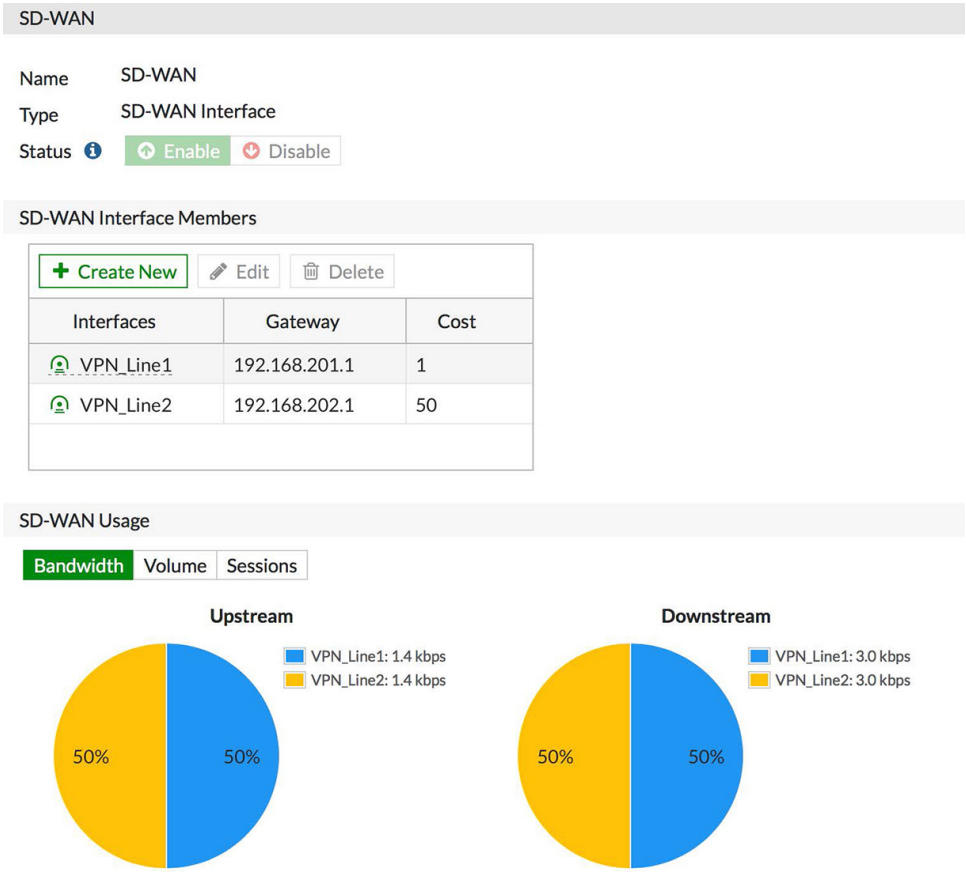
FortiGate-Geräte beherrschen schon lange das Routing über mehrere Leitungen zum selben Ziel. In der Grundversion bedeutete dies eine einfache Überwachung der „Hauptleitung“ und bei Ausfall ein Schwenk. Dabei wurde aber nur eine Leitung benutzt. Mittels der von Fortinet massiv weiterentwickelten WAN-Technologie ist es nun möglich, mehrere Leitungen gleichzeitig zu verwenden, dabei Leitungen zu priorisieren und dies sogar auf Anwendungsebene herunterzubrechen. Damit lassen sich Szenarien implementieren wie beispielsweise „SAP nur über die Standleitung, Intranet auch über die Backup VPN-Leitung“.

Zusätzlich wird ein ständiges Quality of Service Monitoring durchgeführt. Die Entscheidung, über welche Leitung eine Session präferiert läuft, kann auch abhängig von diesen Werten durchgeführt werden.

Mehr Informationen unter: https://www.fortinet.com/de/products/sd-wan.html

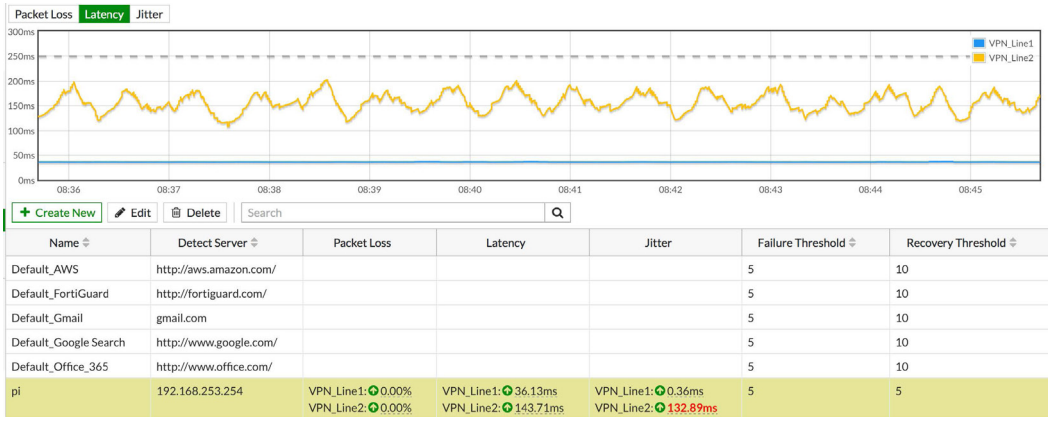
Für den Anwendungsfall, der hier vorgestellt werden soll, wird pro Internetanbindung ein VPN Tunnel zwischen der Firewall im Hausnetz und der FortiGate in AWS erstellt. Über den Parameter local-id bzw. peer-id können die Firewalls die Tunnel auseinanderhalten. Jeder VPN Tunnel taucht dann als „Interface“ in der FortiGate in AWS auf. Über diese wird dann das SD-WAN aufgespannt.

Abb. 2: Definition des SD-WAN auf der FortiGate



Zur SD-WAN-Definition gehört ein SLA, mittels dessen die Leitungen und ihre Güte überwacht werden. Hierzu dient ein Server (oder mehrere) im Hausnetz, der via Ping oder HTTP Requests gemonitored wird. Im einfachen Beispiel reicht ein Ping auf einen internen Server.

Abb. 3: Performance Monitor des SD-WAN



Idealerweise findet sich auf der Gegenstelle im Hausnetz ebenfalls eine FortiGate mit einer spiegelgleichen Konfiguration. Die Mindestanforderung ist allerdings ein Gerät, welches es erlaubt, dass die Pakete auf beiden Tunneln ankommen können.

4.2 Remote Access VPN

Remote Access VPN ist eine Standardfunktion von FortiGate Firewalls. Benutzer können dabei lokal angelegt werden oder werden per Radius / LDAP / AD / TACACS authentisiert. Der Zugang gelingt entweder über die Software FortiClient, welche auch auf den Endgeräten die Sicherheit – auch durch einen Virenscanner – überprüft oder über ein Webportal, in dem interne Applikationen bereitgestellt werden. Das beinhaltet neben Webapplikationen, die einfach in die Webseite eingebunden werden, auch Zugänge über Microsoft Remote Desktop oder Secureshell, die dann im Browser ablaufen.

In der Logik der FortiGate erscheint auch das Remote Access VPN als Interface. Damit ergibt sich eine sehr einfache Regel (sofern die Remote Worker nicht eingeschränkt werden sollen):

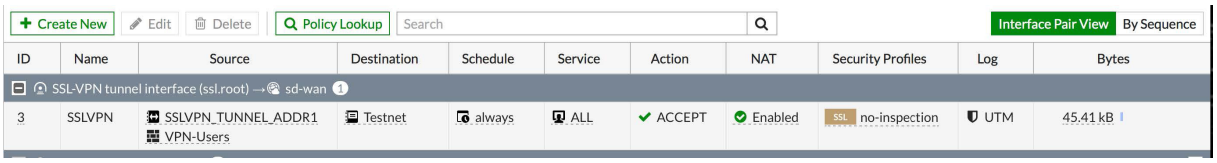


Abb. 4: Firewall-Regel für die Remote Access Clients. „Testnet“ ist hierbei das interne Hausnetz.

Die Gesamtarchitektur ergibt sich damit wie folgt:

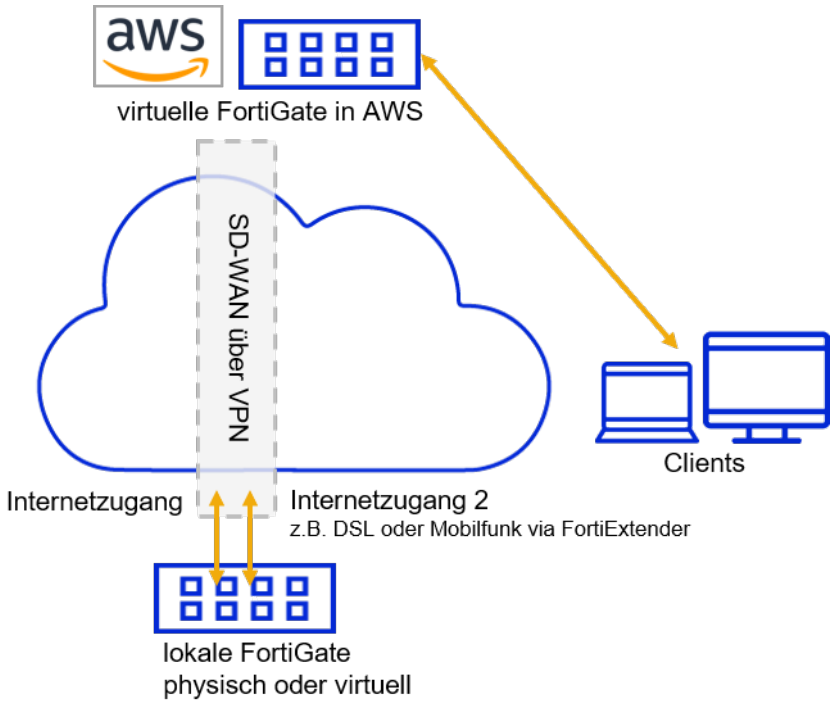


Abb. 5: Gesamtarchitektur Remote Access VPN via AWS mit FortiGate und SD-WAN

4.3 Bewertung

Die vorgestellte Lösung lässt sich schnell und einfach umsetzen. Auch Hardware muss nicht unbedingt angeschafft werden. Im Hausnetz kann auch eine virtuelle FortiGate verwendet werden, so dass lediglich Lizenzen beschafft werden müssen. In der Cloud bietet sich außerdem die Möglichkeit, das pay-as-you-go-Lizenzmodell zu verwenden, bei welchem keine Lizenz beschafft werden muss, sondern nur für die Laufzeit eine Miete abgerechnet wird.

Über matrix

Die matrix technology AG gehört mit mehr als 2000 erfolgreich abgeschlossenen Projekten zu den führenden Spezialisten für Planung, Aufbau, Steuerung und Betrieb der IT für internationale Konzerne und den anspruchsvollen Mittelstand. Mit Leidenschaft, fachlicher Kompetenz und technologischem Know-how stellen sich die über 200 Mitarbeiter täglich der Herausforderung, unternehmenskritische IT-Systeme bedarfsgerecht und mit höchster Qualität zu konzipieren, aufzubauen und zu betreiben.

Das Portfolio der matrix umfasst Leistungen in den Bereichen IT-Services und IT-Beratung. Insbesondere bei der Entwicklung von IT-Strategien und deren Umsetzung, der Migration in die Cloud sowie dem Betrieb im Rahmen des IT-Outsourcings verhilft die matrix Unternehmen zu Höchstleistungen. An ihrem Hauptsitz in München sowie weiteren Standorten in Deutschland und Europa erbringt die matrix IT-Dienstleistungen für Kunden weltweit.

Kontakt

Konstantin Agouros
matrix technology AG
Telefon +49 89 589395-600
Telefax +49 89 589395-711
Web: www.matrix.ag
E-Mail: kontakt@matrix.ag