Leistungsbeschreibung

O_2 Business Secure Hub

1 O_2 Business Secure Hub

O_2 Business Secure Hub ist eine Lösung für die gesicherte Übertragung von Daten zwischen mobilen Endgeräten über das Mobilfunknetz von Telefónica Germany GmbH & Co. OHG (im Weiteren „Telefónica Germany“), dem O_2 Business Secure Hub und dem Kundennetzwerk. Für die Nutzung des O_2 Business Secure Hubs müssen entsprechende Mobilfunk Einzelverträge über Mobilfunkleistungen (SIM-Karten) mit Telefónica Germany separat vereinbart werden.

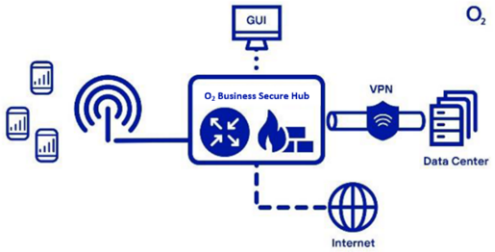

Abbildung 1 O_2 Business Secure Hub Funktion

Die Daten werden von den mobilen Endgeräten über das Mobilfunknetz von Telefónica Germany auf den zentralen O_2 Business Secure Hub von Telefónica Germany geleitet. Von dort werden die Daten mittels Virtual Private Network Tunnel (im Weiteren „VPN-Tunnel“) gesichert über das öffentliche Internet in das Kundennetz übermittelt. Unter anderem können so das Rechenzentrum des Kunden, Cloud-Anbieter oder VPN-Endpunkte des Kunden erreicht werden. Optional können die mobilen Endgeräte auch miteinander kommunizieren.

Hinweis: O_2 Business Secure Hub kann eine herkömmliche Ende-zu-Ende-Verschlüsselung (z.B. HTTPS, TLS etc.) nicht ersetzen.

Ein Hub ist eine unabhängige Routing- und Firewall-Instanz des O_2 Business Secure Hubs mit einer eindeutigen Hub ID.

Jedem Hub werden ein- oder mehrere IP-Adressbereich(e) (im Weiteren „Netzwerk für mobile Endgeräte“) aus dem 100.64.0.0/10 IPv4 Netz zugewiesen. Ein Netzwerk für mobile Endgeräte erhält bei der Einrichtung eine eindeutige Netzwerk-ID. Jede SIM-Karte erhält aus den zugewiesenen IP-Adressbereichen eine statische Internet-Protokoll-Adresse (im Weiteren „IP-Adresse“). Die Übertragung der Daten erfolgt über einen Access Point Name (im Weiteren „APN“) des O_2 Business Secure Hubs.

Für die VPN-Verbindung kann der Kunde sowohl Internet Protocol Security (im Weiteren „IPsec“) als auch WireGuard verwenden. Die redundante Infrastruktur des O_2 Business Secure Hubs ist transparent für den Kunden und ermöglicht eine erhöhte Verfügbarkeit der VPN-Tunnel und zugleich eine einfache Konfiguration zu nur einem VPN-Endpunkt des O_2 Business Secure Hubs.

Neben dem VPN-Tunnel zum Firmennetzwerk stellt Telefónica Germany über den O_2 Business Secure Hub optional einen konfigurierbaren Zugangspunkt zum Internet (im Weiteren „Internet-Breakout“) zur Verfügung. Dieser kann bei Bedarf auf einzelne IP-Adressbereiche beschränkt werden, z.B. für den Download von Firmware-Updates.

Weiterhin kann optional eine Netzwerkadress-übersetzung (Network Address Translation, im Weiteren „NAT“) eingerichtet werden, um die statischen IP-Adressen der SIM-Karten auf einen kundenspezifischen Adressbereich zu übersetzen.

Auch kann optional durch die Einrichtung eines sogenannten „Alias-APN“ ein beliebiger freier APN-Name vergeben werden.

Telefónica Germany führt eine Anforderungsanalyse durch, um die spezifischen Bedürfnisse des Kunden zu verstehen und zu dokumentieren. Die Konfiguration der Leistungen von O_2 Business Secure Hub erfolgt zwischen den Ansprechpartnern von Telefónica Germany und dem Kunden in einem On-Boarding Call.

2 Features und Optionen

2.1 Features

- Vergabe von statischen IP-Adressen der mobilen Endgeräte im Kundenetzwerk
- Umfangreiche Web UI zur Selbstadministration (O_2 Hub)
- Konfigurierbare DNS-Namen (mydevicename.myhubname.o2hub.de) ermöglichen die Erreichbarkeit von mobilen Endgeräten im Kundennetzwerk
- VPN-Technologien IPsec und WireGuard einsetzbar
- Bis zu zwei VPN-Tunnel inklusive
- Redundante Infrastruktur
- Passwortschutz zur Authentifizierung der mobilen Endgeräte bei Bedarf (Radius Authentifizierung)
- Kundeneigener DNS-Server (bei Bedarf)

2.2 Optionen

- APN-Alias für kundespezifische APN-Namen (CS-APN)

- NAT für kundespezifische statische IP-Adressen
- API-Bereitstellung
- Internet-Breakout

3 Weitere Leistungsmerkmale

3.1 Maximale Größe des Netzwerks für mobile Endgeräte

Derzeit können einem oder mehreren Hubs maximal 65.534 IPv4 Adressen zugewiesen werden. Wird ein größeres Netzwerk für die mobilen Endgeräte benötigt, kann dies individuell auf Projektebene geprüft werden.

Sobald alle verfügbaren statischen IP-Adressen eines Hubs vergeben sind, können keine weiteren Einzelverträge über Mobilfunkdienstleistungen / SIM-Karten hinzugefügt werden. Zur Erweiterung kann ein zusätzliches Netzwerk für mobile Endgeräte bestellt, oder es kann das vorhandene Netzwerk durch ein Größeres ersetzt werden.

3.2 Anzahl der Netzwerke für mobile Endgeräte pro Hub und Änderung von statischen IP-Adressen

Einem Hub können weitere Netzwerke für mobile Endgeräte zugeordnet werden, wenn das vorhandene Netzwerk bzw. die vorhandenen Netzwerke nicht mehr ausreichend IP-Adressen zur Verfügung stellt bzw. stellen. Dem jeweiligen Netzwerk werden die nächsten verfügbaren IP-Adressen zugeordnet, d.h. die IP-Adressen der Netzwerke sind nicht zusammenhängend. Alternativ kann der Kunde vereinbaren, dass das vorhandene Netzwerk durch ein neues größeres Netzwerk ersetzt wird. In diesem Fall ändern sich die IP-Adressen der mobilen Endgeräte. Die Anzahl der Netzwerke sollte möglichst geringgehalten werden.

In seltenen Fällen kann es aus organisatorischen Gründen notwendig sein, die IP-Adressen anzupassen. Dies wird vorab von Telefónica Germany mitgeteilt.

3.3 Anzahl der VPN-Tunnel pro Hub.

Es können bis zu zwei VPN-Tunnel an einen Hub angebunden werden. Die Netzwerkadressen auf Kundenseite pro VPN-Netzwerk (Hub) müssen unterschiedlich sein.

Es können in einem Hub IPsec und WireGuard gleichzeitig genutzt werden.

Mit IPsec kann jeweils ein VPN-Tunnel pro öffentlicher IP-Adresse auf Kundenseite aufgebaut werden. Sollen mehrere IPsec VPN zu einem Hub aufgebaut werden, muss die öffentliche IP-Adresse je IPsec VPN unterschiedlich sein.

Für die Nutzung von WireGuard ist keine statische IP-Adresse auf Kundenseite notwendig. Für die Nutzung von WireGuard muss der kundenseitige VPN-Endpunkt nicht aus dem öffentlichen Internet erreichbar sein.

Alle VPN-Tunnel eines Hubs sind für alle mobilen Endgeräte eines Hubs sichtbar.

3.4 NAT

Je Netzwerk für mobile Endgeräte kann maximal ein NAT eingerichtet werden. NAT ist mit mehreren VPN-Tunneln nutzbar.

3.5 Individueller Domain Name System Server (im Weiteren „DNS-Server“)

Es können individuelle DNS-Server pro Hub oder auch nur für einzelne mobile Endgeräte konfiguriert werden, so dass auf dem jeweiligen mobilen Endgerät eine Namensauflösung möglich ist. Damit ist z.B. auch eine firmeninterne Namensauflösung möglich und die mobilen Endgeräte können firmeninterne Server über ihren Namen statt über IP-Adressen aus dem Netzwerk der mobilen Endgeräte heraus adressieren.

3.6 Passwort Zugang für mobile Endgeräte

Es können für einen Hub oder auch nur für einzelne mobile Endgeräte Passwörter vergeben werden. Das mobile Endgerät kann nur dann eine Datenverbindung aufbauen, wenn das Passwort in der Mobilfunkkonfiguration des mobilen Endgerätes gesetzt wird.

3.7 APN-Name für mobile Endgeräte

Für die Nutzung des O_2 Business Secure Hubs im mobilen Endgerät muss der folgende APN hinterlegt werden: „all2hub“

4 Besonderheiten und Einschränkungen

Im Rahmen der Nutzung von O_2 Business Secure Hub sind bestimmte Voraussetzungen zu erfüllen und Einschränkungen zu beachten.

4.1 Voraussetzungen für die Nutzung

Der O_2 Business Secure Hub ist nur in Kombination mit einem der folgenden Tarife nutzbar:

O_2 Business Blue Choice, O_2 Business Blue Choice Data, O_2 Business Blue S, O_2 Business Blue S (2022), O_2 Business Blue S+, O_2 Business Blue M, O_2 Business Blue L, O_2 Business Blue XL, O_2 Business Unlimited Max, O_2 Business Unlimited Smart, O_2 Business Unlimited Basic, O_2 Business Unlimited Max Data, O_2 Business Unlimited Smart Data, O_2 Business Unlimited

Max (2021), O_2 Business Unlimited Smart (2022), O_2 Business Match

4.2 Einschränkungen beim Datenroaming

Datenroaming ist ausschließlich in der Weltzone „EU+“ möglich. In den Weltzonen „World Select“ und „Restliche Welt“ steht Datenroaming nicht zur Verfügung.

4.3 Zweckgebundene Nutzung

Der O_2 Business Secure Hub ist ausschließlich für geschäftliche Zwecke vorgesehen und darf nicht privat genutzt werden, z.B. während eines Urlaubs.

4.4 Nicht gestattete Nutzungen

O_2 Business Secure Hub darf nicht genutzt werden zum automatisierten Datenaustausch zwischen Endgeräten (Machine-to-Machine „M2M“), zur Herstellung dauerhafter Sprach- oder Datenverbindungen im Sinne einer Standleitung oder für Verbindungen, bei denen der Kunde oder ein Dritter aufgrund der Verbindung oder der Verbindungsdauer Zahlungen oder andere Vermögenswerte als Gegenleistung erhält oder erhalten soll.

4.5 Einsicht in den Datenverbrauch

Der unter Nutzung von O_2 Business Secure Hub generierte Datenverbrauch kann nicht über die O_2 Business App, per SMS oder IVR abgefragt werden. Informationen hierzu sind ausschließlich über die Service-Hotline unter 0800 22 111 22 verfügbar.