Leistungsbeschreibung

O_2 Business SD-WAN (Fortinet)

Inhaltsverzeichnis

1 Allgemeine Beschreibung

Telefónica Germany GmbH & Co. OHG (im Folgenden „Telefónica Germany“ oder „Anbieter“ genannt) richtet für den Auftraggeber (im Folgenden auch „Kunde“ genannt) das Produkt „O_2 Business SD-WAN“ (im Folgenden auch „Produkt“ genannt) ein und ermöglicht im Rahmen der technischen und betrieblichen Möglichkeiten die Nutzung eines sogenannten Software-Defined Wide Area Networks (SD-WAN) über bestehende Internet- und MPLS-Verbindungen.

Das Produkt nutzt eine virtuelle Architektur mit einer zentralen Managementplattform in einer Cloud (Deutschland), mit dem der Kunde für seine Standorte beliebige Wege für die Datenübertragung von IP-Paketen kombinieren kann, um Benutzer über ein SD-WAN mit Anwendungen zu verbinden.

Die Leistungen des Produktes werden durch vor Ort installierte Hardwarekomponenten an den Kundenstandorten erbracht. Die Einrichtung, Steuerung und Konfiguration der Leistungen erfolgt durch Telefónica Germany über ein zentrales, webbasiertes Konfigurationsportal.

Beim Produkt handelt sich um einen so genannten Over-the-Top-Service (OTT). Für die Nutzung erforderliche Internet- und MPLS-Anschlüsse sind daher vom Kunden bereitzustellen oder im Rahmen eines eigenständigen Vertrages bei Telefónica Germany zu beauftragen. Sofern und insoweit Anschlussleistungen von Telefónica Germany bezogen werden, gelten für diese ausschließlich die diesen zugrundeliegenden vertraglichen Vereinbarungen.

2 Vertragliche Regelungen

Für alle in Anspruch genommenen Varianten des Produktes gilt entweder das Dokument „Allgemeine Geschäftsbedingungen Festnetz (Business)“ oder ein Rahmenvertrag von Telefónica Germany.

3 Standardleistungen

Die Leistungen des Produktes werden dem Auftraggeber für seine Standorte zur Übermittlung von IP-Paketen im LAN, WLAN und WAN im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten zur Verfügung gestellt.

Voraussetzung für die Leistungserbringung durch Telefónica Germany ist die Bereitstellung von mindestens einem Internetanschluss pro Standort durch den Auftraggeber, der diesen für die Nutzung durch das Produkt freigibt. Alternativ kann auch eine MPLS-Anbindung mit Zugriff auf einen Internet-Breakout genutzt werden.

Die nachstehend angegebenen Übertragungsgeschwindigkeiten gelten ausschließlich für die dem Kunden im Rahmen des Produktes bereitgestellten Endgeräte (im Folgenden auch „SD-WAN-Router“ genannt). Telefónica Germany übernimmt keine Gewährleistung oder Garantie für die Übertragungsgeschwindigkeiten im Kunden-LAN bzw. WLAN sowie die vom Kunden bereitgestellten physikalischen Anschlüsse in das Internet. Das Produkt unterstützt ein Hub-and-Spoke-

Netzwerkarchitektur, bei dem ein oder mehrere zentrale Hub-Standorte mit Spoke-Standorten verbunden werden.

Telefónica Germany kategorisiert Kundenstandorte anhand der erforderlichen Bandbreitenkapazität und der empfohlenen maximalen Anzahl gleichzeitiger Nutzer (ohne Remote User). Davon abhängig werden dem Auftraggeber die in der nachstehenden Tabelle aufgeführten SD-WAN-Router für die Dauer des Vertragsverhältnisses überlassen. Die Gerätemodelle werden zur Orientierung beispielhaft genannt, es besteht jedoch kein Anspruch auf ein konkretes Gerätemodell.

Folgende Standortkategorien stehen zur Verfügung:

Standortgröße	Durchsatz Firewall und VPN	Empfehlung gleichzeitige Nutzer	SD-WAN-Router
S – Kleiner Standort	800 Mbit/s 4,4 Gbit/s	bis zu 15	FG 40
M – Mittlerer Standort	1 Gbit/s 6,5 Gbit/s	bis zu 25	FG 60
M – Mittlerer Standort	1 Gbit/s 7,1 Gbit/s	bis zu 50	FG 80
L – Großer Standort	1,6 Gbit/s 11,5 Gbit/s	bis zu 150	FG 100
L – Großer Standort	3,5 Gbit/s 13 Gbit/s	bis zu 200	FG 200
XL – Sehr großer Standort	10 Gbit/s 55 Gbit/s	bis zu 400	FG 400
XL – Sehr großer Standort	11,5 Gbit/s 55 Gbit/s	bis zu 1.000	FG 600

Alle Durchsatzraten (NGFW Enterprise Mix und IPsec VPN 512 Byte) sind Bruttoangaben (Up- und Downstream aller Anschlüsse eines Standortes addiert) und für die jeweiligen Standortgrößen als Maximalwerte zu verstehen, deren Erreichung auch von Art und Umfang der in Anspruch genommenen Leistungen abhängig ist. Die tatsächlich am Standort nutzbare Bandbreite hängt von der Bandbreite der Festnetzanschlüsse, an die der SD-WAN-Router angeschlossen ist, der Mobilfunkverfügbarkeit, der Mobilfunkbandbreite und der örtlichen Netzabdeckung ab.

Für die Nutzung des Produktes ist für jeden SD-WAN-Router genau eine Lizenz erforderlich. Das Produkt umfasst drei (3) Arten von Lizenzen, die dem Kunden je nach gewünschtem Leistungsumfang pro SD-WAN-Router von Telefónica Germany für die Dauer des Vertragsverhältnisses überlassen werden:

- Lizenz „SD-WAN“
- Lizenz „Basic Security (ATP)“

  Erweitert die Leistungsmerkmale der Lizenz „SD-WAN” um grundlegende Sicherheitsfunktionen
- Lizenz „Advanced Security (UTP)“

  Erweitert die Leistungsmerkmale der Lizenzen „SD-WAN“ und „Basic Security (ATP)“ um zusätzliche Sicherheitsfunktionen

Im Produkt enthalten ist zudem auf Anfrage ein webbasiertes Kundenportal.

3.1 Lizenz „SD-WAN“

Die Lizenz „SD-WAN“ stellt folgende Leistungen bereit:

- Verschlüsselte Kommunikation zwischen den Kundenstandorten über ein SD-WAN-Overlay-Netzwerk durch automatisch generierte Tunnel über alle an den Kundenstandorten ins SD-WAN eingebundenen Zugangsnetze. Das Overlay basiert auf einem mit IPsec verschlüsselten GRE-Tunnel, wodurch die Integrität der Informationen gewährleistet wird. Mindestens ein SD-WAN-Router mit fester, öffentlicher IP-Adresse muss dabei als Hub fungieren. Die SD-WAN-Router FG 40 und FG 60 können nur als Spoke konfiguriert werden
- Mehrere Anschlüsse (Traffic Balancing): O_2 Business SD-WAN ist unabhängig von der Art der verwendeten Verbindung. Es besteht die Möglichkeit, verschiedene Arten von Verbindungen, wie MPLS, feste Internetzugänge und mobile Zugangsverbindungen (LTE/5G), zu nutzen. Die Auswahl einer Verbindung erfolgt dynamisch auf Basis der Leitungsparameter
- Multilink (Hybride Standorte): Konsolidierung mehrerer physikalischer Verbindungen zu einem logischen Link, auch über unterschiedliche Verbindungsarten
- Kompatibilität mit MPLS: Bereitstellung von Netzwerk- und Sicherheitsfunktionen über private MPLS-Netzwerke
- QoS Overlay: Intelligente Verkehrssteuerung von Anwendungsverkehr (Priorisierung, Depriorisierung, Bandbreitenlimitierung)
- Alle Netzwerkfunktionen sind mit grundsätzlichen Sicherheitsfunktionen ausgestattet (bis zu zehn (10) statische Layer 3 und 4-Firewallregeln)
- Applikationskontrolle: Identifizierung von charakteristischem Verhalten bei mehr als 5000 Applikationen, Ableiten von Routing-Priorisierungen
- URL-Filterung (statisch pro Domain): Überwachung und Kontrolle des http-Protokolls. Verhindert die Anzeige von unangemessenen oder nicht autorisierten Webinhalten und verhindert das Ausführen von eingebetteten und Cookie basierten Java- oder ActiveX-Skripten auf Webseiten

- Monitoring von Transport- und Netzwerkfunktionen

3.2 Lizenz „Basic Security (ATP)“

Die Lizenz „Basic Security (ATP)“ erweitert den Leistungsumfang der Lizenz „SD-WAN“ um folgende Funktionen. Alle Verkehrsströme werden durch eine fortschrittliche Bedrohungserkennung, Datenkontrolle, Abhilfemaßnahmen und Threat Intelligence Services abgesichert.

- Applikationskontrolle (FortiGuard Lab Kategorisierung): Erkennen und Blockieren von bösartigen und unerwünschten Anwendungen sowie Vermeidung von VPN oder Proxy Verkehrsströmen, die Webfilter umgehen
- Modifikation von Firewall Richtlinien
- DMZ: Sicherheitsbereich im Unternehmensnetzwerk zur sicheren Bereitstellung von Diensten, wie DNS, DHCP etc. sowie Vermeidung von Informationslecks
- Antivirus/Malware Protection: Erkennung von infizierten oder potenziell virenartigen Dateien (.bat, .exe etc.). Abgabe von Warnmeldungen, Blockade oder Ablage der Datei in Quarantäne
- IDS/IPS (Intrusion Detection/Protection System): Erkennung und Abwehr von Eindringlingen, abnormalen und verdächtigen Verkehrsströmen sowie Angriffssignaturen in Echtzeit (z.B. DDoS/DoS Attacken, Exploits, Botnets)
- SSL Inspection: Überprüfung und Blockade bedrohlicher SSL-verschlüsselter Verkehrsströme (z.B. https, smtps, pop3s, imaps, ftps)
- Sandboxing: Analyse und Identifikation verdächtiger Dateien (z.B. Mailanhänge) auf ihre Schädlichkeit und Bereitstellung einer isolierten Umgebung zum Testen und Ausführen von verdächtigen Programmen/URLs, um den Rest des Unternehmensnetzwerkes vor den negativen Auswirkungen zu schützen. Die Aktivierung von SSL Inspection wird unbedingt empfohlen
- Virtual Patching: Bereitstellung von Security Patches im IPS (Intrusion Prevention System) im Gegensatz zur Bereitstellung von Security Patches auf Geräteebene. Das IPS-System dient dazu, den Datenverkehr nach schädlichen Aktivitäten zu untersuchen und diese zu blockieren, indem die Netzwerkregeln angepasst werden
- Security Monitoring

3.3 Lizenz „Advanced Security (UTP)“

Die Lizenz „Advanced Security (UTP)“ erweitert den Leistungsumfang der Lizenzen „SD-WAN“ und „Basic Security (ATP)“ um folgende Funktionen:

- Vollständige Verkehrskontrolle für Web und Video: Überwachung und Kontrolle des http-Protokolls. Verhinderung die Anzeige von unangemessenen oder nicht autorisierten Webinhalten und Ausführungsverhinderung von eingebetteten und Cookie basierten Java- oder ActiveX-Skripten auf Webseiten
- Dynamische Web-/Videofilterung: Erweiterte Web-Filterung basierend auf dynamischen Kategorien, wie Nachrichten, Terrorismus, Malware etc., die automatisch auf der Grundlage der von den FortiGuard Labs gepflegten, zentralen Datenbank aktualisiert werden. Die Datenbank selbst wird alle vier (4) Stunden aktualisiert
- Antispam: Analyse und Identifizierung von E-Mails zum Zweck der Blockierung solcher Nachrichten, deren Signatur als von einer verdächtigen und/oder bösartigen Quelle stammend eingestuft wird. Der Mailserver muss sich an einem Kundenstandort befinden und die SSL-Prüfung ist zwingend zu aktivieren

3.4 SD-WAN-Router

Zur Nutzung des Produktes werden dem Auftraggeber die in der nachstehenden Tabelle aufgeführten SD-WAN-Router (oder gleichwertige SD-WAN-Router) mit WAN- und LAN-seitigen Ethernet-Interfaces auf Basis der benötigten Bandbreitenkapazität und der Anzahl gleichzeitiger Nutzer für die Dauer des Vertragsverhältnisses überlassen. Werden an einem Kundenstandort physische Server betrieben, auf die externe Nutzer zugreifen, sollte pro Server ein zusätzlicher Bedarf von zehn (10) gleichzeitigen Nutzern eingeplant werden.

Für jeden als Spoke konfigurierten SD-WAN-Router wird der maximale aggregierte Datendurchsatz (Up- und Downstream) in Abhängigkeit von der genutzten Leistung aufgeführt:

- Nur Nutzung von SD-WAN-Funktionen
- Gleichzeitige Nutzung von SD-WAN und Security (ATP oder UTP)

Router	Anzahl gleichzeitiger Nutzer		SD-WAN (in Gbit/s)	SD-WAN + Security (in Gbit/s)
	Empfehlung	Maximum		
FG 40	bis 15	35	2,70	0,70
FG 60	bis 25	50	4,15	0,85
FG 80	bis 50	70	4,15	0,95
FG 100	bis 150		6,85	1,30
FG 200	bis 200		13,00	3,25
FG 400	bis 400		16,00	5,50
FG 600	bis 1.000		17,50	8,25

Die angegebene Maximalanzahl gleichzeitiger Nutzer an einem Kundenstandort überschreitet die Empfehlung und ist nur in Verbindung mit der Lizenz „SD-WAN“ sowie ohne zusätzliche Optionen wie Remote User, WLAN-Accesspoint oder LAN-Switch gültig.

Der maximale Datendurchsatz von SD-WAN-Routern, die als Hub fungieren, ist leicht reduziert, da diese zusätzlich die Kommunikation mit der Managementplattform steuern müssen.

4 Bereitstellung und Nutzung

Telefónica Germany stellt je nach gewählter Produktkonfiguration den jeweiligen Service in der nachfolgend beschriebenen Weise bereit.

Der Kunde wird vor der Aktivierung bei der Festlegung der Konfiguration (High Level Design) von Telefónica Germany unterstützt. Die Konfigurationsklärungen zwischen dem Anbieter und dem Auftraggeber über die Ersteinrichtung eines Regelwerkes sind im Rahmen eines gesamten Zeitaufwands von maximal zwei (2) Stunden inklusive und erfolgen über das von Telefónica Germany bereitgestellte Formular „End Customer Data Collection“.

Der Anbieter generiert auf Basis der Kundenvorgaben im Rahmen des vom Produkt bereitgestellten Leistungsumfangs die Konfiguration für den Service und weist diese dem Produkt des Kunden zu. Der Kunde stimmt zu, dass Telefónica Germany der Fortinet, Inc. den Kundennamen sowie Anzahl und Typ der gelieferten Geräte mitteilt.

4.1 Managed Service

O_2 Business SD-WAN ist ein Managed Service. Sowohl Installation, Aktivierung und Betrieb der Dienstleistung als auch die erstmalige Konfiguration wird von Telefónica Germany durchgeführt. Beim Full Managed Service werden Konfigurationsänderungen ebenfalls von Telefónica Germany durchgeführt, beim Co-Managed Service erhält der Kunde über das FortiPortal eingeschränkte Möglichkeiten zur Konfiguration der Produktbestandteile SD-WAN und Security:

- Änderung von SD-WAN-Regeln (z.B. Priorisierung, Art der Regeln)
- Änderung der definierten Probes
- Konfiguration von Firewall-Regeln
- Konfiguration der Web-Filterung nach Kategorien
- Erstellung von Black-/Whitelisten für Web- und URL-Filterung
- Änderung der vorinstallierten IDS/IPS-Pakete (restriktiv, Standard)
- Übernahme/Aktivierung der generierten Änderungen
- Erstellung von Konfigurations-Backups für den Fall, dass eine Änderung fehlschlägt

4.2 Bereitstellung an Kundenstandorten

Soweit nicht anders vereinbart erfolgt die Vor-Ort-Installation von zur Nutzung überlassenen Geräten durch einen vom Anbieter beauftragten Techniker. Telefónica Germany vereinbart mit dem Auftraggeber im Rahmen der betrieblichen Möglichkeiten einen Termin in den Geschäftsräumen des Kunden. Sagt der Kunde den abgestimmten Termin weniger als drei (3) Werktage vor dem geplanten Zeitpunkt ab, ist er verpflichtet, dem Anbieter einen pauschalierten Schadenersatz in Höhe der diesbezüglich vereinbarten Vergütung für die Vor-Ort-Installation zu zahlen. Dem Kunden steht gegenüber dem Anbieter der Nachweis eines geringeren Schadens offen.

Die Konfiguration und Aktivierung des Produktes erfolgen remote durch Telefónica Germany.

4.2.1 Internetanschluss über Mobilfunknetz

Zusätzlich zum Zugang über festnetzbasiertes Internet bietet das Produkt die Möglichkeit, sich mit einem mobilen Netzwerk zu verbinden. Der mobile Zugang wird als zusätzlicher Internetzugang im webbasierten Konfigurationsportal konfiguriert. Der mobile Zugang funktioniert wie jeder andere aktive Internetzugang.

Die tatsächlich nutzbaren Übertragungsgeschwindigkeiten sind von der bestehenden Netzauslastung im Mobilfunknetz an dem jeweiligen Kundenstandort abhängig. Ebenso können die angegebenen Übertragungsgeschwindigkeiten nur dann realisiert werden, wenn die am Kundenstandort verfügbare Mobilfunkabdeckung und insbesondere die Mobilfunkverfügbarkeit (Indoor) am vom Kunden gewünschten Aufstellungsort des Empfangsgerätes dies technisch ermöglichen. Die tatsächlich mögliche Mobilfunkbandbreite kann erst während der Installation festgestellt werden. Sollte sich

aufgrund von Umständen, die außerhalb des Einflussbereichs der Telefónica Germany liegen (insbesondere bauliche Gegebenheiten, wie z.B. Stahlbetonwände oder bedampfte Scheiben), ergeben, dass diese Bandbreite in nicht unerheblicher Weise geringer ist als die erforderliche Mindestbandbreite, hat der Kunde einen anderen Standort für das Empfangsgerät zur Verfügung zu stellen. Sofern der Kunde dieser Mitwirkungspflicht nicht nachkommt, kann Telefónica Germany nicht wegen verminderter Bandbreite in Anspruch genommen werden.

4.2.2 Internet-Breakout

Das Produkt bietet die Möglichkeit, bestimmte Datenverkehre so zu steuern, dass sie über Internetanschlüsse, die an den jeweiligen Standorten vom Kunden bereitzustellen sind, direkt in das öffentliche Internet geleitet werden, um die Belastung des verschlüsselten Kundennetzwerks mit Internetverkehr zu verringern.

4.3 Überlassung und Rückgabe von technischen Geräten

Zur Nutzung des Produktes werden dem Auftraggeber notwendige technische Endgeräte für die Dauer des Vertragsverhältnisses überlassen.

Die Geräte werden, falls nicht abweichend im Auftrag vereinbart, von Telefónica Germany innerhalb Deutschlands an den Kunden versendet.

Der Kunde ist verpflichtet die Endgeräte bei Vertragsbeendigung an Telefónica Germany zurückzusenden. Hierfür erhält der Kunde entsprechende Rücksendedokumente zugesandt, die für die Rücksendung zu verwenden sind. Gleiches gilt nach Abschluss der Datenerfassungsphase bei Beauftragung von CTAP.

4.4 Voraussetzungen / Mitwirkungspflichten

Der Kunde ist verpflichtet, die zur Leistungserbringung seinerseits erforderlichen Mitwirkungshandlungen zeitgerecht zu erbringen. Das umfasst auch die Bereitstellung von Informationen, die für die Konfiguration und Bereitstellung der Leistung erforderlich sind. Überlassene Geräte sind vom Kunden gegen physische Einwirkung von Feuer, Wasser, Strom sowie gegen Diebstahl zu schützen. Die Komponenten sind in ausreichend geschützten Räumen unterzubringen und gemäß der Gerätespezifikation bei geeigneten Umgebungsbedingungen zu betreiben.

Die Ermittlung und Vorbereitung geeigneter und zulässiger Installationsorte ist vom Kunden vorab in Eigenregie durchzuführen und mit dem Anbieter abzustimmen. Das betrifft insbesondere die Positionierung von WLAN-Accesspoints. Entsprechende Montagepunkte müssen mit einer Standardleiter zugänglich sein und dürfen sich maximal in 2,5 Meter Höhe befinden. Sollte der Kunde eine Befestigung von WLAN-Accesspoints mittels Direkt- oder Dübelmontage benötigen, ist dies vorab bei Telefónica Germany anzumelden. Ein späterer Rückbau und die Wiederherstellung von Installationsorten obliegen dem Kunden.

Für den Betrieb der Geräte ist, falls erforderlich, das Vorhandensein geeigneter Steckdosen (Schuko, Typ F) in maximal einem (1) Meter Entfernung zu den Installationsorten der anzuschließenden Geräte Bedingung für die Leistungserbringung. Darüber hinaus ist für einige Leistungen des Anbieters das Vorhandensein oder die Beschaffung einer geeigneten strukturierten LAN- und Inhouse-Verkabelung notwendig. Der Abstand erforderlicher Netzwerkdosen vom Installationsort des anzuschließenden Gerätes darf einen (1) Meter nicht überschreiten. Die Verantwortung für die Schaffung der genannten Voraussetzungen, die Bereitstellung geeigneter Patch-Kabel in erforderlicher Anzahl und Länge und die Einhaltung von Normen und Gerätespezifikationen liegt ausschließlich beim Kunden. Stellt der Kunde während oder nach einem Technikereinsatz fest, dass er die nötige Verkabelung endgültig nicht bereitstellen kann oder diese nicht frei zugänglich ist, wird der entsprechende Einzelauftrag für diesen Standort rückwirkend aufgehoben, ohne dass dem Kunde hieraus Ansprüche gegenüber dem Anbieter erwachsen. Die bereits entstandenen Kosten sowie noch entstehende Kosten für die Abwicklung wird Telefónica Germany dem Kunden berechnen.

Für den Betrieb von WLAN-Accesspoints sollte die Stromversorgung nach Möglichkeit über Power over Ethernet (PoE) gemäß Gerätespezifikation auf Basis der vom Kunden bereitzustellenden Verkabelung und einer ebenfalls bereitzustellenden, PoE-fähigen LAN-Switch-Infrastruktur erfolgen. Sollte keine Speisung über PoE zur Verfügung stehen, kann eine externe Speisung über ein Steckernetzteil erfolgen.

Voraussetzung für die Leistungserbringung durch Telefónica Germany ist die Bereitstellung von mindestens einem Internetanschluss pro Standort, der nicht Bestandteil des Produktes ist und durch den Auftraggeber für die Nutzung durch das Produkt zur Verfügung zu stellen ist. Alternativ kann auch eine MPLS-Anbindung genutzt werden, sofern über diese seitens des Kunden ein Zugriff auf einen Internet-Breakout gewährleistet wird. Hierbei hat der Kunde dafür Sorge zu tragen, dass eine bidirektionale Kommunikation zwischen bereitgestellten SD-WAN-Routern und der zentralen Managementplattform von Telefónica Germany über diese Anschlüsse möglich ist. Weiterhin muss der Kunde eine bidirektionale Kommunikation zwischen bereitgestellten LAN-Switches, WLAN-Accesspoints und den am

Kundenstandort bereitgestellten SD-WAN-Routern ermöglichen, die als LAN- und WLAN-Controller fungieren. Die Integration von kundenseitigen Datenbanken (z.B. Active Directory, LDAP-Server, TACACS+, Identity Provider) ist nur dann möglich, wenn alle involvierten SD-WAN-Router darauf zugreifen können. Bei Einsatz einer kundeneigenen Firewall müssen möglicherweise Konfigurationsänderungen an dieser vorgenommen werden. Der Kunde hat sicherzustellen, dass die benötigten Protokolle / Ports für die Einrichtung, Steuerung und Konfiguration des Produktes freigeschaltet werden. Bei Beauftragung von CTAP ist der Auftraggeber vollständig für die Einbindung der vom Anbieter bereitgestellten Geräte in das Standortnetzwerk verantwortlich. Dazu zählen insbesondere die eigenständige Installation sowie die Durchführung aller erforderlichen Konfigurationen an den eigenen Geräten. Die erforderlichen Informationen werden dem Kunden ab dem Zeitpunkt des Vertragsabschlusses zur Verfügung gestellt.

Die Belegung und Konfiguration von Ports der im Rahmen des Produktes bereitgestellten LAN-Switches ist vorab im Rahmen der Gerätespezifikation mit Telefónica Germany abzustimmen. Auf Wunsch kann der Kunde die Installation und Inbetriebnahme von LAN-Switches und WLAN-Accesspoints eigenständig durchführen. Eine nachträgliche Überprüfung der ausgeführten Arbeiten durch den Anbieter erfolgt in diesem Fall nicht. Die Anbindung des lokalen Netzwerkes an die LAN-Switches sowie die funktionsfähige Umsetzung von Geräten innerhalb eines Standortes liegen immer in der Verantwortung des Kunden.

Der Auftraggeber ist verantwortlich für das Herunterladen, die Installation und die Aktualisierung von Software, Lizenzen und Zertifikaten auf seinen eigenen Endpunkten. Falls der Anbieter eine automatische Remote-Aktualisierung der Dienstleistung anbietet und der Auftraggeber dies wünscht, muss der Auftraggeber entsprechende Vorkehrungen treffen, um dies zu ermöglichen.

Die Nutzung der Fortinet Produkte unterliegt dem Fortinet „Product License Agreement / EULA and Warranty Terms“ (verfügbar unter: www.fortinet.com/content/dam/fortinet/assets/legal/EULA.pdf).

Sofern und solange der Kunde seine Mitwirkungspflichten verletzt, ist Telefónica Germany von ihrer Leistungspflicht befreit, soweit diese von der unterlassenen Mitwirkungshandlung betroffenen ist. Etwaig vereinbarte Service Level gelten insoweit nicht. Gleichwohl bleibt der Kunde zur Zahlung der vereinbarten Vergütungen verpflichtet.

Der Kunde hat die Kosten der Erfüllung seiner Mitwirkungspflichten selbst zu tragen.

5 Optionale Leistungen

Die nachfolgend aufgeführten, optionalen Leistungen werden jeweils nach Vereinbarung und in Erweiterung oder Änderung zu den oben beschriebenen Standardleistungen der Produktvarianten im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten angeboten.

Die Wahl einer dieser Optionen ist jeweils mit zusätzlichen Entgelten verbunden. Diese können der bei Vertragsabschluss der Option gültigen Preisliste oder dem individuellen Angebot der Telefónica Germany entnommen werden. Die Berechnung erfolgt zzgl. des Preises der Standardleistung.

Der Anbieter erbringt im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten folgende optionale zusätzliche Leistungen:

5.1 Anbindung mobilfunkgestützter Internetanschlüsse

Der Kunde kann zur Anbindung mobilfunkgestützter Internetanschlüsse die Überlassung so genannter Mobilfunk-Extender für die Dauer des Vertragsverhältnisses bei Telefónica Germany als Option beauftragen. Diese separaten Geräte müssen mit einem von Telefónica Germany bereitgestellten, aktiven SD-WAN-Router verbunden werden.

5.2 Redundante Anbindung der O_2 Business SD-WAN Standorte

Zusätzlich kann an angebundenen Standorten zum primären SD-WAN-Router ein zweiter SD-WAN-Router zur Ermöglichung einer redundanten Anbindung beauftragt werden. Für die Nutzung des redundanten SD-WAN-Routers erforderliche Internet- und MPLS-Anschlüsse sind vom Kunden bereitzustellen. Voraussetzung für eine redundante Anbindung ist immer eine aktive Anbindung des Standortes über einen primären SD-WAN-Router und die direkte Kabelverbindung zwischen beiden SD-WAN-Routern. Der redundante SD-WAN-Router muss vom gleichen Routertyp sein wie der primäre SD-WAN-Router. Der SD-WAN-Router FG 40 kann im Redundanz-Szenario weder als primärer noch als redundanter Router eingesetzt werden.

5.3 Kundenportal für Monitoring und Co-Management

Telefónica Germany stellt dem Auftraggeber im Rahmen der Bereitstellung von O_2 Business SD-WAN auf Anfrage einen webbasierten Zugang zu einem einfach zu bedienenden Kundenportal FortiPortal zur Verfügung. Der Zugriff auf das Portal ermöglicht ausgewählte Self-Service- und Monitoring-Funktionen, deren Verfügbarkeit und Umfang von der jeweils zugewiesenen Lizenz abhängt. Die Konfiguration erfolgt im Rahmen des Co-Managements stets über sogenannte

Templates (Konfigurationsvorlagen), die mehreren Standorten mit gleicher Netzwerktopologie zugewiesen sein können. Änderungen durch den Kunden wirken sich somit auf alle betroffenen Standorte aus. Die Erstellung neuer Templates sowie deren Zuweisung zu Standorten ist ausschließlich Telefónica Germany vorbehalten. Die bereitgestellten Funktionen lassen sich drei übergeordneten Bereichen zuordnen:

Monitoring und Berichte

- Einsicht in physikalische Verbindungen und Übertragungsparameter (z. B. Bandbreitennutzung pro Verbindung und nach Standorten aggregiert)
- Überwachung von VPN-Verbindungen (Latenz, Paketverlust, Jitter, Verbindungsstatus)
- Analyse von sicherheitsrelevanten Ereignissen (z. B. IPS, Policy Hits, Webfilter-Aktivitäten)
- Visualisierung der aktuellen SD-WAN-, WiFi-, LAN- und Security-Konfigurationen (nur lesender Zugriff)
- Echtzeit-Monitoring aller genannten Bereiche
- Abruf von Berichten und Auswertungen bei Bedarf
- Zugriff auf Dashboards, Audit-Daten sowie technische Dokumentationen und Links

Konfiguration grundlegender Sicherheitsfunktionen

- Erstellung und Anpassung von Firewall-Regeln innerhalb bestehender Sicherheitsrichtlinien
- Webfilterung auf Basis von Kategorien sowie Verwaltung individueller Black- und Whitelists
- Auswahl und Aktivierung vorkonfigurierter IDS/IPS-Pakete (z. B. „restrictive“, „standard“)
- Erstellung und Bearbeitung von Sicherheitsprofilen (z. B. Antivirus-, Webfilter-, Application-Control-Profile)
- Erstellung von Konfigurations-Backups zur Wiederherstellung
- Anwendung von Änderungen im Rahmen zugewiesener Templates durch gezielte Installation auf betroffenen Geräten

Grundlegende SD-WAN-Funktionalitäten

- Bearbeitung zugewiesener SD-WAN-Templates (Erstellung und Neuvergabe sind ausgeschlossen)
- Anpassung bestehender SD-WAN-Regeln, z. B. Priorisierung, Regelstrategie, Routingziele
- Verwaltung definierter Monitoring-Probes zur Pfadüberwachung (inkl. Schwellenwerten für Latenz, Jitter, Paketverlust)
- Erstellung von Konfigurations-Backups zur Wiederherstellung
- Konfiguration und Aktivierung von Änderungen

5.4 LAN-Switch

Im Rahmen der Option LAN-Switch überlässt Telefónica Germany dem Auftraggeber für die Dauer des Vertragsverhältnisses je Kundenstandort bis zu vier (4) LAN-Switches zum Betrieb einer LAN-Ethernet-Netzwerkinfrastruktur. Dies erfolgt im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten. Eine IP-Verbindung zu einem vom Anbieter am Standort bereitgestellten, aktiven SD-WAN-Router und ein aktiver Service O_2 Business SD-WAN sind notwendige Grundlagen für die Installation und den Betrieb der LAN-Switches.

Die in der nachstehenden Tabelle aufgeführten LAN-Switches werden dem Auftraggeber mit und ohne Half Power PoE für die Dauer des Vertragsverhältnisses überlassen. Die maximal verfügbare PoE-Leistung und Anzahl der PoE-Ports ergibt sich aus der jeweiligen Gerätespezifikation. Die Gerätemodelle werden zur Orientierung beispielhaft genannt, es besteht jedoch kein Anspruch auf ein konkretes Gerätemodell.

LAN-Switch	Anzahl Ports (GE RJ45)	Switching Kapazität (in Gbit/s)	Redundante Stromversorgung	Zusätzliche Schnittstellen
FS 108	8	20	nein	2xSFP 1G
FS 124	24	56	nein	4xSFP+ 10G
FS 148	48	104	nein	10G 4xSFP+
FS 424	24	128	ja	10G SFP+
FS 448	48	176	ja	10G SFP+

Es ist zulässig, kundeneigene LAN-Switches zu betreiben. Diese sind vom O_2 Business SD-WAN unabhängig und eine Einbindung in die zentrale Managementplattform ist nicht möglich. In diesem Fall ist der Kunde für die Konsistenz der LAN-Konfiguration (IP-Segmente, VLANs, etc.) sowie die Konfiguration und/oder Verfügbarkeit des LANs verantwortlich. Sollten kundenspezifische LAN-Switches zwischen den SD-WAN-Routern und den im Rahmen des Produktes bereitgestellten LAN-Switches installiert werden, muss es sich um Layer-2-Switches handeln. Die für die 802.1X-Authentifizierung notwendige Infrastruktur ist durch den Kunden zu stellen.

5.4.1 Technische Leistungsmerkmale LAN

Die nachfolgend aufgelisteten technischen Leistungsmerkmale werden in im Rahmen von O_2 Business SD-WAN unterstützt:

- Virtuelle, lokale Netzwerke (VLANs): Nutzung mehrerer VLANs, um ein LAN zu unterteilen. VLANs ermöglichen die Definition unterschiedlicher Richtlinien für verschiedene Benutzertypen und eine

feinere Kontrolle über den LAN-Verkehr. Bis zu fünf (5) VLANs sind im Leistungsumfang enthalten. Die maximale Anzahl kann sich je nach eingesetztem LAN-Switch unterscheiden und ergibt sich aus der Gerätespezifikation

- Link Aggregation: Bündelung von bis zu acht (8) physischen Schnittstellen zu einer aggregierten Linkgruppe mit der Bandbreite aller kombinierten Links. Es können maximal acht (8) Linkgruppen erstellt werden. Wenn eine Verbindung innerhalb einer (1) Linkgruppe ausfällt, wird der Datenverkehr automatisch auf die verbleibenden Schnittstellen übertragen
- Port Blocking: Unterstützung von Funktionen zur Port-Steuerung, z. B. Blockieren oder Quarantäne von Ports. Ports können basierend auf Sicherheitsrichtlinien blockiert oder isoliert werden, um unerwünschten Datenverkehr zu verhindern
- Switch-Sicherheit: Port-Security ermöglicht die Begrenzung der Anzahl der MAC-Adressen, die an einem Port zugelassen sind. 802.1X-Authentifizierung ermöglicht die Authentifizierung von Geräten, bevor sie Zugriff auf das Netzwerk erhalten

5.5 WLAN-Accesspoint

Im Rahmen der Option WLAN-Accesspoint überlässt Telefónica Germany dem Auftraggeber für die Dauer des Vertragsverhältnisses je Kundenstandort bis zu fünf (5) WLAN-Accesspoints zur Bereitstellung eines WLAN-Netzes, die die kabellose Übermittlung von Daten in Form von IP-Paketen im LAN in den Geschäftsräumen des Kunden ermöglichen. Dies erfolgt im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten. Eine IP-Verbindung zu einem vom Anbieter am Standort bereitgestellten, aktiven SD-WAN-Router und ein aktiver Service O_2 Business SD-WAN sind notwendige Grundlagen für die Installation und den Betrieb der WLAN-Accesspoints. Zwischen WLAN-Accesspoints und SD-WAN-Router können LAN-Switches zwischengeschaltet werden, die nach Möglichkeit PoE-fähig sein sollten, um auf diesem Weg die Speisung der WLAN-Accesspoints durchzuführen. Hierbei werden die im Rahmen von O_2 Business SD-WAN angebotenen LAN-Switches empfohlen. Alternativ können geeignete, kundeneigene Layer-2-Switches eingesetzt werden. In diesem Fall ist der Kunde für die Konsistenz der WLAN-Konfiguration (IP-Segmente, VLANs, etc.) sowie die Konfiguration und/oder Verfügbarkeit des LANs verantwortlich.

Die in der nachstehenden Tabelle aufgeführten WLAN-Accesspoints werden dem Auftraggeber für die Dauer des Vertragsverhältnisses überlassen. Die Gerätemodelle werden zur Orientierung beispielhaft genannt, es besteht jedoch kein Anspruch auf ein konkretes Gerätemodell.

WLAN-Accesspoint	Empfehlung gleichzeitige Nutzer	Anwendungsfall	Antennen	Bandbreite (in Gbit/s)
FAP 231	bis 20	Kleine Abdeckung, geringe Nutzerdichte	2x2 WiFi6	2,4 GHz: ≤ 0,5 5 GHz: ≤ 1,2
FAP 431	bis 50	Große Abdeckung, hohe Nutzerdichte	4x4 WiFi6	2,4 GHz: ≤ 1,0 5 GHz: ≤ 2,5
FAP 831	bis 100	Sehr große Abdeckung, sehr hohe Nutzerdichte	8x8 WiFi6	2,4 GHz: ≤ 1,0 5 GHz: ≤ 4,0

Die festzulegende Auswahl und Kombination der Gerätevarianten für die benötigte WLAN-Netzabdeckung in den jeweiligen Geschäftsräumen sind abhängig von den baulichen Gegebenheiten, den genutzten Anwendungen sowie der Anzahl und WLAN-Fähigkeit der Endgeräte der Nutzer des Auftraggebers. Die Ermittlung der vorgenannten Anforderungen und insbesondere der WLAN-Ausleuchtung der Geschäftsräume liegt in der Verantwortung des Kunden.

Da jeder WLAN-Accesspoint eine eigene WLAN-Netzabdeckung zur Verfügung stellt, kann es bei einem Wechsel zwischen den verschiedenen WLAN-Netzabdeckungen aufgrund eines Standortwechsels innerhalb der Geschäftsräume des Auftraggebers zu einem Abbruch und gleichzeitigem Neuaufbau zum nächstgelegenen WLAN-Accesspoint kommen. Es ist zulässig kundeneigene WLAN-Accesspoints zu betreiben. Eine Einbindung in die zentrale Managementplattform des Produkts und ein Nutzerwechsel von zu im Rahmen des O_2 Business SD-WAN bereitgestellten WLAN-Accesspoints ist nicht möglich. Die für die 802.1X-Authentifizierung notwendige Infrastruktur ist durch den Kunden zu stellen.

5.5.1 Technische Leistungsmerkmale WLAN

Die nachfolgend aufgelisteten technischen Leistungsmerkmale werden in im Rahmen von O_2 Business SD-WAN unterstützt.

- WLAN-Standard: WiFi 6 nach Standard 802.11ax, WiFi 5 nach Standard 802.11ac und WiFi 4 nach Standard 802.11n. Zusätzliche Unterstützung der Standards 802.11a, b, und g (WiFi 3)
- WLAN-Sicherheit: WPA2, WPA2 Enterprise und WPA3
- Multiple SSIDs: Nutzung mehrerer, separater WLANs mit eigenem Namen und eigenen Sicherheitseinstellungen. Die Anzahl kann sich je nach

eingesetztem WLAN-Accesspoint unterscheiden und ergibt sich aus der Gerätespezifikation

- WiFi Threats Inspection and Detection (WIDS): Identifikation, Erkennung und Abschwächung von Bedrohungen und Angriffen auf der Grundlage einer Analyse des drahtlosen Datenverkehrs, die es ermöglicht, den als Angriff identifizierten Datenverkehr pro WLAN-Accesspoint zu überwachen und zu blockieren
- Rogue AP Detection: Erkennung nicht autorisierter WLAN-Accesspoints, die an das kabelgebundene Netzwerk des Kundenstandortes angeschlossen wurden
- Quality of Service (QoS): Priorisierung von Datenverkehr für Anwendungen mit hoher Bandbreitenanforderung, z.B. VoIP oder Video-Streaming
- Gästeportal: Einrichtung von Anmeldeseiten und Zugriffsbeschränkungen für Gäste
- Beamforming: Die WLAN-Accesspoints nutzen zur Verbesserung der Signalqualität und Erhöhung der Reichweite die Beamforming-Technologie, um das WLAN-Signal gezielter auf die verbundenen Geräte richten zu können
- Band Steering: Wenn möglich automatische Umlenkung von Endgeräten auf das 5-GHz-Band zur Verbesserung der Leistung und Reduktion von Störungen
- Airtime Fairness: Alle Endgeräte erhalten fairen Zugriff auf die verfügbaren Übertragungskapazitäten im WLAN. Dies verhindert, dass einzelne Geräte den gesamten Kanal blockieren

Die Leistungsfähigkeit eines WLAN-Accesspoints in Bezug auf Senden und Empfangen und die damit verbundene physikalische Bandbreite des WLAN-Signals hängt von verschiedenen Faktoren ab. Dazu gehören der Installationsort, die Antennenausrichtung, eventuell in der Nähe installierte Funkanlagen, geografische und physikalische Besonderheiten sowie die Beschaffenheit des Gebäudes. Die maximal erreichbare und durchschnittliche Bandbreite der drahtlosen Netzwerkverbindung am Standort kann je nach Tageszeit variieren und hängt auch von der Entfernung der Nutzer vom WLAN-Accesspoint ab. Aus technischen Gründen lässt sich die genaue Bandbreite nicht vor der Installation des WLAN-Accesspoints am Standort präzise vorhersagen.

5.6 Virtueller Standort

Ein Virtueller Standort ermöglicht die Einbindung und Nutzung von Cloud-Umgebungen in das SD-WAN mittels einer FortiGate Virtual Machine (im Folgenden auch „Virtueller SD-WAN-Router“ genannt). Virtuelle Standorte werden dabei immer als Spoke-Standorte eingerichtet. In Kombination mit dem Hub-Standort ermöglicht die ADVPN-Funktionalität eine direkte Kommunikation zu den Standorten im O_2 Business SD-WAN. Für die Nutzung ist für jeden Virtuellen SD-WAN-Router genau eine der in den Abschnitten 3.1, 3.2 und 3.3 beschriebenen Lizenzen erforderlich, die dem Kunden je nach gewünschtem Leistungsumfang von Telefónica Germany für die Dauer des Vertragsverhältnisses überlassen wird.

Folgende Ausprägungen stehen zur Verfügung:

	VM01	VM02	VM04	VM08	VM16
Anzahl CPUs	1	2	4	8	16
Speicher	2 GB	2 GB	2 GB	2 GB	2 GB
SD-WAN Performance	1.5 Gbit/s	2.8 Gbit/s	5.4 Gbit/s	11 Gbit/s	21.5 Gbit/s
Security Performance	400 Mbit/s	1.1 Gbit/s	1.9 Gbit/s	3.8 Gbit/s	7.2 Gbit/s
Vergleichbarer SD-WAN-Router	FG 40	FG 100	FG 400	FG 600	FG 1100

Der Kunde benötigt für die Bereitstellung eines Virtuellen Standortes ein Konto bei Amazon Web Services und muss dort für die Dauer des Vertragsverhältnisses eine Virtual Private Cloud inkl. der erforderlichen Ressourcen für den Virtuellen SD-WAN-Router anlegen. Der Anbieter stellt dem Kunden notwendige Daten über ein Terraform-Skript zur Verfügung, damit dieser die FortiGate Virtual Machine erstellen und initial konfigurieren kann. Die anschließende Konfiguration des Produktes wird von Telefónica Germany durchgeführt. Hierfür stellt der Kunde dem Anbieter die AWS Instance ID und die zugehörige öffentliche IP-Adresse zur Verfügung.

5.7 Remote User

Die Leistung Remote User basiert auf der Applikation FortiClient für Endpunkte von Fortinet, Inc. und ermöglicht im O_2 Business SD-WAN den sicheren Zugriff von Nutzern auf das Unternehmensnetzwerk, Anwendungen und Dokumente und bietet Überwachungsfunktionen. Hierfür muss jedem Remote User eine eigene Lizenz zugewiesen werden.

Es sind drei (3) Arten von Lizenzen verfügbar, die dem Kunden je nach gewünschtem Leistungsumfang vom Anbieter für die Dauer des Vertragsverhältnisses in Paketen von je 25 Lizenzen überlassen werden:

- Lizenz „VPN“
- Lizenz „ZTNA“

  Erweitert die Leistungsmerkmale der Lizenz „VPN“ um grundlegende Sicherheitsfunktionen

- Lizenz „EPP“

  Erweitert die Leistungsmerkmale der Lizenzen „VPN“ und „ZTNA“ um zusätzliche Sicherheitsfunktionen

Es ist nicht erlaubt, verschiedene Lizenztypen in einem O_2 Business SD-WAN zu mischen. Telefónica Germany benötigt für die Bereitstellung des Dienstes eine eindeutige und gültige E-Mail-Adresse je neuem Nutzer vom Auftraggeber. Die einzelnen Nutzer erhalten eine E-Mail mit einem Download-Link, über den diese die vorkonfigurierte Endpunkt-Anwendung FortiClient herunterladen und auf ihren Endgeräten eigenständig installieren müssen.

Über den FortiClient kann Nutzern Zugriff auf einen oder mehrere physische oder virtuelle Standorte im O_2 Business SD-WAN eingerichtet werden. Die SD-WAN-Router an diesen Standorten benötigen mindestens die Lizenz „Basic Security (ATP)“, empfohlen wird jedoch die Lizenz „Advanced Security (UTP)“. Zudem müssen die Router eine feste, öffentliche IP-Adresse aufweisen, alternativ können Remote User aber auch über einen der für die Funktion des SD-WANs erforderlichen Hub-Router mit einem Kundenstandort ohne feste, öffentliche IP-Adresse verbunden werden.

5.7.1 Lizenz „VPN“

Die Lizenz „VPN“ stellt folgende Leistungen bereit:

- Einrichtung von IPsec/SSL-Tunneln
- Zugelassene Verbindung zu den Komponenten des Unternehmensnetzwerks gemäß den Sicherheitsrichtlinien
- Nutzung der Internetkonnektivität über den zugewiesenen Kundenstandort
- Kontinuierliche Überwachung des Datenverkehrs
- Kontinuierliche Überwachung des Konnektivitätsstatus von Endgeräten des Unternehmensnetzwerks
- Kontinuierliche Überwachung von Endgeräten auf Schwachstellen und Risiken und laufende Aktualisierung des Sicherheitsstatus der Endgeräte
- Endgeräteschutz durch automatische Updates des FortiClients (Remote)
- Identifizierung von veralteten Anwendungen und Bereitstellung dieser Informationen als PDF-Bericht über das FortiPortal
- Inventarisierung von Nutzern
- Protokollierung der letzten Anmeldungen von Nutzern
- Fernaktualisierung von Konfigurationen
- Die Authentifizierung erfolgt über einen im O_2 Business SD-WAN als Hub-fungierenden SD-WAN-Router. Die Integration mit einer Kundendatenbank (Active Directory, LDAP-Server oder Identity Provider) ist Voraussetzung. Telefónica Germany wird für diese Integration nach vorheriger Vereinbarung ein individuelles Angebot im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten erstellen.

5.7.2 Lizenz „ZTNA“

Die Lizenz „ZTNA“ erweitert den Leistungsumfang der Lizenz „VPN“ um folgende Funktionen

- Festlegung von ZTNA-Tags und kontinuierliche Prüfung des Sicherheitsstatus, ob ein Endgerät den erforderlichen Sicherheitsstandard erfüllt, um eine Verbindung zu spezifischen IT-Assets herzustellen
- Anwendung von ZTNA-Regeln auf Sicherheitsrichtlinien im SD-WAN-Router, um bedingten, der Rolle des Nutzers entsprechenden Zugang zu ermöglichen
- Modifikation von ZTNA-Richtlinien zur Anpassung an vom Kunden gewünschte Änderungen
- Schutz vor nicht gepatchten, potenziell unsicheren Anwendungen durch Erzwingung von Updates auf Endgeräten
- Konfiguration von Richtlinien für Web-Filterung direkt in der FortiClient Applikation
- Dashboards für Schwachstellen: Bereitstellung regelmäßiger PDF-Berichte über das FortiPortal

5.7.3 Lizenz „EPP“

Die Lizenz „EPP“ erweitert den Leistungsumfang der Lizenzen „VPN“ und „ZTNA“ um folgende Funktionen:

- Antivirus/Malware Protection: Erkennung von potenziell oder tatsächlich virusinfizierten Dateien am Endgerät. Abgabe von Warnmeldungen und Blockade der Verbreitung von Malware
- Sandboxing: Identifikation und Analyse verdächtiger Dateien (z.B. Mailanhänge) auf ihre Schädlichkeit und Bereitstellung einer isolierten Umgebung zum Testen und Ausführen von verdächtigen Programmen/URLs, um den Rest des Unternehmensnetzwerkes vor den negativen Auswirkungen zu schützen. Die Aktivierung von SSL Inspection wird unbedingt empfohlen.
- Geräte-Quarantäne: Erkennung von Malware-Infektionen auf Endgeräten. Manuelle oder automatische Quarantänisierung des betroffenen Endpunktes

- USB-Geräte-Überwachung: Verhinderung des Einschleusens von Malware durch Überwachung der USB-Ports von Endgeräten
- Überwachung aller Sicherheitsfunktionen (Virenerkennung, risikobehaftete und unter Quarantäne gestellte Endgeräte, Erkennung von Bedrohungen durch Sandboxing, USB-Verbindungen mit Malware usw.) mit einem Echtzeit-Dashboard für Blockierungen und Schwachstellen.

5.8 Dedizierte Managementplattform

O_2 Business SD-WAN bietet die Möglichkeit, eine dedizierte, zentrale Managementplattform in der Cloud von Amazon Web Services (Deutschland) zu nutzen. Der Anbieter wird auf Wunsch ein separates Angebot für den Kunden erstellen. Die dedizierte Plattform nutzt die gleiche, Cloud-basierte Umgebung (Virtual Private Cloud) wie die zentrale Managementplattform für den Standarddienst. Abgesehen vom Backup-System werden keine weiteren Elemente mit der Standardplattform geteilt (Datenbanken, Festplatten, IP-Adressen). Wenn nicht ausdrücklich anders vereinbart, verfügt die dedizierte Plattform über dieselben Standarddienstleistungsmerkmale, dieselbe Architektur, dieselben Dimensionierungsregeln, denselben Zugriff auf die Plattformelemente sowie dieselben Rechte und Rollen wie die Standardplattform.

5.9 Anbindung einer kundenseitigen Überwachungsinfrastruktur

O_2 Business SD-WAN kann über die zentrale Managementplattform Service-Logs an eine kundenseitig bereits vorhandene Überwachungsinfrastruktur, wie SIEM oder Syslog-Service, senden, sofern diese standardisierte Protokolle, wie Common Event Format und Syslog, oder spezifische Fortinet Protokolle unterstützt und einen für die Übermittlung dieser Logs freigeschalteten Internetzugang aufweist. Es wird somit eine zentrale Überwachung, erweiterte Log-Aggregation sowie Nachverarbeitung und Weiterverarbeitung unterstützt, ohne die Überwachungsfunktionen im FortiPortal zu verlieren.

5.10 Cyber Threat Assessment Program

Das Cyber Threat Assessment Program (CTAP) unterstützt gezielt die Planungsphase von O_2 Business SD-WAN und anderer Security-Services der Telefónica Germany. Durch CTAP erfolgt eine detaillierte Analyse der Netzwerksicherheit und -leistung an Kundenstandorten, ohne den laufenden Betrieb zu beeinträchtigen. Hierzu wird dem Kunden im Rahmen von O_2 Business SD-WAN ein speziell konfigurierter SD-WAN-Router für die Dauer des CTAP ohne Mindestvertragslaufzeit überlassen. Standardleistungen gemäß Ziffer 3 werden nicht erbracht. Der SD-WAN-Router wird in ein bestehendes Standortnetzwerk integriert, der den Netzwerkverkehr sowohl von als auch zu WAN-Verbindungen über einen festgelegten Zeitraum hinweg überwacht. Im Verlauf des CTAP werden die im Rahmen des CTAP-Programms erhobenen technischen Informationen an eine CTAP-Plattform der Fortinet, Inc. mit geografischem Serverstandort in Deutschland übermittelt, um eine umfassende Analyse der Netzwerksicherheit und -leistung durchzuführen. Die Art der übermittelten Daten umfasst Netzwerkverkehrsdaten, die durch den Kunden vergebenen privaten IP-Adressen des Kunden-Netzwerks, Verbindungsprotokolle, Verkehrsmuster, Anwendungsnutzung und Leistungsdaten. Personenbezogene Daten i. S. d. Art. 4 Nr. 1 DS-GVO werden durch die Telefónica Germany hierbei nicht verarbeitet. Der Kunde soll der Telefónica Germany keine Informationen zur Verfügung stellen, um eine Identifizierbarkeit natürlicher Personen zu ermöglichen. Dies umfasst insbesondere Daten und Informationen, die eine Zuordnung zu einer Kennung wie einem Namen, einer Kennnummer, Standortdaten, einer Online-Kennung oder einem oder mehreren besonderen Merkmalen einer natürlichen Person erlauben. Im Rahmen von CTAP werden keine weiteren kundenspezifischen Daten ausgewertet, korreliert oder weitergegeben – weder vom Kunden, noch aus anderen Quellen, noch durch die Nutzung anderer Services von Telefónica Germany. Dies schließt ausdrücklich auch öffentliche IP-Adressen des Kunden ein, die weder direkt noch indirekt einer Identifizierung der Nutzer zugeführt werden. Kundendaten wie Namen, Adressen, Kontaktdaten und kundenspezifische Inhalte von Datenpaketen werden ebenfalls nicht übermittelt.

CTAP identifiziert potenzielle Bedrohungen wie Malware, Ransomware, Botnets und andere schädliche Aktivitäten, die möglicherweise unentdeckt geblieben sind. Zusätzlich zur Bedrohungsanalyse werden auch Einblicke in die Anwendungsnutzung geliefert, indem aufzeigt wird, welche Anwendungen im Netzwerk verwendet werden und welche Risiken damit verbunden sein könnten. Zudem bewertet CTAP die Netzwerkperformance und identifiziert Engpässe, um die Effizienz und Geschwindigkeit zu optimieren.

Nach Abschluss der Analyse erhält der Kunde von Telefónica Germany einen umfassenden Bericht mit den wichtigsten Ergebnissen. Der Anbieter unterstützt den Kunden bei der Interpretation und schlägt konkrete Handlungsempfehlungen zur Verbesserung der Sicherheitsmaßnahmen und der Netzwerkleistung vor.

Der Kunde ist für die Einhaltung arbeitsrechtlicher und sonstiger Vorschriften im Rahmen der Analyse des eigenen, internen Netzverkehrs verantwortlich.

5.11 Verlegung, Auswechselung oder Änderung der Anschaltung und Verlegung der Endeinrichtung

Da die Leistung standortbezogen ist, kann Telefónica Germany die vereinbarte Leistung an einem neuen Standort nur nach Prüfung und bei Vorliegen gleicher technischer Gegebenheiten erbringen, d.h., je nach den örtlichen Gegebenheiten kann es sein, dass die gewünschte Realisierungsleistung nicht oder nur in verändertem Leistungsumfang zur Verfügung gestellt werden kann.

Die zur Realisierung ggf. notwendige technische Aufrüstung des Inhouse-Netzes hat durch den Kunden zu erfolgen.

5.12 Professional Services

Für Dienstleistungen, die über den Leistungsumfang von O_2 Business SD-WAN hinausgehen, einschließlich zusätzlicher technischer und konzeptioneller Beratung, Konfigurationsklärungen sowie Unterstützung bei Projekten und Implementierungen, erstellt der Anbieter nach vorheriger Vereinbarung ein individuelles Angebot, welches im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten auf Basis von Tagessätzen (je 8 Stunden) abgerechnet wird. Anteilige Tagessätze sind ebenfalls möglich. Zusätzliche Kosten, wie Reisekosten, werden nach vorheriger Absprache separat in Rechnung gestellt.

5.13 Weitere Leistungen

Für weitere Leistungen, die über den Leistungsumfang von O_2 Business SD-WAN hinausgehen, z.B. Integration von kundenseitigen Datenbanken (z.B. Active Directory, LDAP-Server, TACACS+, Identity Provider), Proof-of-Concept Implementierungen, die Installation zusätzlicher Geräte des Auftraggebers oder umfangreiche Verkabelungen am Kundenstandort, erstellt Telefónica Germany nach vorheriger Vereinbarung ein individuelles Angebot im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten.

6 Service Level

6.1 Verfügbarkeit

Die zentrale Managementplattform des Produktes im Netz von Telefónica Germany und das webbasierte Konfigurationsportal haben pro Betriebsmonat, beginnend ab dem Datum der technischen Bereitstellung, eine Mindestverfügbarkeit von 99,9%.

Bei den bereitgestellten SD-WAN-Routern an den Kundenstandorten beträgt die Mindestverfügbarkeit 99,9% pro Betriebsmonat.

Eine Nichterreichbarkeit des Konfigurationsportals hat keine Auswirkungen auf die grundsätzliche Funktion des Produktes und wird somit nicht für die Bestimmung der Verfügbarkeit der zentralen Managementplattform herangezogen. Es entstehen allerdings Einschränkungen bei Konfigurationsänderungen und statistischen Auswertungen.

Die Verfügbarkeit eines Produktes wird als Prozentwert dargestellt, der angibt, zu welchem Anteil der Gesamtbetriebszeit der Dienst mindestens verfügbar sein wird. Ausfallzeiten durch geplante Arbeiten (siehe Ziffer 6.4), aufgrund von Ursachen, die dem Auftraggeber zugerechnet werden können, sowie aufgrund von höherer Gewalt, werden nicht als Nichtverfügbarkeit gezählt. Sie errechnet sich wie folgt:

$$Verfügbarkeit = \frac{(Betriebszeit - geplante\ Arbeiten - Nichtverfügbarkeit)}{(Betriebszeit - geplante\ Arbeiten)} * 100\%$$

„Betriebszeit“ bezeichnet die Anzahl der Minuten im Betriebsmonat. „Geplante Arbeiten“ bezeichnet die Summe der Minuten im Betriebsmonat, in denen die Leistung aufgrund geplanter Arbeiten außer Betrieb war. „Nichtverfügbarkeit“ bezeichnet die Summe aller nicht geplanten Einzelausfallzeiten pro Betriebsmonat.

Für die Ermittlung einer Einzelausfallzeit wird die jeweilige Entstörzeit herangezogen. Die Entstörzeit ist die Zeit zwischen dem Eingang der Störungsmeldung durch den Auftraggeber beim Anbieter, sie endet mit der Wiederverfügbarkeit des Dienstes. Ausfallzeiten werden vom Anbieter protokolliert.

Dem Kunden ist bekannt, dass die Leistung des Produktes von Telefónica Germany nur erbracht werden kann, wenn der Kunde für jeden O_2 Business SD-WAN Standort mindestens einen Internetanschluss zur Verfügung stellt und für die Nutzung durch das Produkt freigibt. Dies umfasst auch die Freischaltung kundeneigener Firewalls. Telefónica Germany übernimmt im Rahmen des Produktes keine Gewährleistung für die ständige Verfügbarkeit solcher Internetanschlüsse und damit für die jederzeitige Erbringung der Leistung des Produktes. Die Anschlussverfügbarkeiten dieser Internetanschlüsse werden für die Bestimmung der in diesem Abschnitt beschriebenen Verfügbarkeiten nicht einbezogen. Für das Produkt nicht vollständig freigeschaltete, kundeneigene Firewalls werden nicht als Ausfall des Produktes gewertet.

6.2 Monitoring

Im Rahmen der Überwachungsaktivitäten überwacht die zentrale Managementplattform ständig 24x7x365 die Betriebsvariablen des Produktes und die wichtigsten Kennwerte der Plattform, der Kontrollelemente und der Infrastruktur.

Weiterhin überwacht das zentrale Portal automatisiert den Zustand der bereitgestellten Endgeräte. Das umfasst die Überwachung der für die Endgeräte wichtigsten Parameter (z. B. Speicherstatus, CPU usw.).

Die Überwachung von Sicherheitsattacken (z.B. Erkennung von bösartigen Paketen) ist nicht Teil des Supports, den das Service Operations Center von Telefónica Germany erbringt.

6.3 Reporting

Der Kunde kann bei Bedarf vordefinierte Berichte, für die in der zentralen Plattform erfassten Variablen anfordern. Dies umfasst die bereitgestellten Endgeräte sowie SD-WAN- und Security-Services. Je nach der Lizenz, die der Kunde erworben hat, handelt es sich um die folgenden Berichte:

SD-WAN

- Performance Report
- SD-WAN-Auslastungsreport

Basic Security (ATP)

- Alle unter SD-WAN genannten Reports
- Firewall-Report
- Antivirus-Report
- IPS-Report
- App-Control-Report

Advanced Security (UTP)

- Alle vorgenannten Reports
- Web-Filter-Report
- AntiSpam-Report

WLAN und LAN

- Report WLAN-Abdeckung
- Report LAN-Switch-Nutzung

Die automatische Übermittlung von Berichten an den Kunden ist nicht im Leistungsumfang enthalten.

6.4 Geplante Arbeiten

Geplante Arbeiten sind Wartungs-, Installations- und Umbauarbeiten an bereitgestellten Endgeräten und an zentralen Systemen der Telefónica Germany oder seiner Vorleistungspartner. Der Anbieter behält sich vor, überlassene Hard- und Software jederzeit zu aktualisieren.

Geplante Arbeiten an zentralen Systemen werden in der Regel nachts in festgelegten Wartungsfenstern durchgeführt. Telefónica Germany hat das Recht, die Produkte für geplante Arbeiten außer Betrieb zu nehmen. Betroffene Kunden werden auf Wunsch fünf Werktage vor dem Wartungstermin über die Arbeiten und die voraussichtlichen Ausfallzeiten informiert.

6.5 Entstörung

Der Anbieter behebt die Störungen seiner technischen Einrichtungen im Rahmen der bestehenden technischen und betrieblichen Möglichkeiten.

6.5.1 Annahme der Störungsmeldung

Die zentrale Störungsannahme ist im Rahmen der technischen und betrieblichen Möglichkeiten täglich in der Zeit von 0:00 Uhr bis 24:00 Uhr unter der kostenlosen Rufnummer des Geschäftskunden-Service 0800 22 10 422 erreichbar.

Aus dem Ausland erfolgt die Störungsannahme unter der Telefonnummer (+49) (0)40 41 43 0202. Je nach Land und Telefonanbieter können dem Auftraggeber dabei unterschiedliche Gebühren entstehen, die der Auftraggeber trägt. Die Störungsannahme erfolgt in deutscher und englischer Sprache. Änderungen der Erreichbarkeit werden dem Auftraggeber schriftlich mitgeteilt.

6.5.2 Störungskategorien

Die Qualität einer Störung wird in vier (4) Prioritätskategorien eingeteilt.

Priorität	Beschreibung
Critical	Der Service ist mit allen wichtigen Funktionen nicht verfügbar
High	Der Service ist wesentlich beeinträchtigt, wichtige Funktionen sind nicht verfügbar
Medium	Der Service ist beeinträchtigt, die wichtigsten Funktionen sind verfügbar
Low	Der Service ist gering beeinträchtigt, alle wichtigen Funktionen sind verfügbar

Die Klassifizierung einer Störung anhand der Prioritätskategorien erfolgt, auf Basis der Störungsmeldung, durch den Anbieter. Hierbei wird bei der Störungsaufnahme eine Klassifizierung gemäß den Beschreibungen vorgenommen und dem Auftraggeber unverzüglich mitgeteilt. Sofern der Auftraggeber mit der Klassifizierung einer Störung nicht einverstanden ist, hat er dies gegenüber dem Auftragnehmer unverzüglich mitzuteilen. Dabei sind dem Auftragnehmer die Gründe für eine aus Sicht des Auftraggebers abweichende Klassifizierung mitzuteilen und entsprechend nachzuweisen. In jedem Fall ist der Kunde für die Klassifizierung einer Störung beweispflichtig.

6.5.3 Reaktionszeit

Nach Eingang der Störungsmeldung beginnt Telefónica Germany unverzüglich mit den Arbeiten zur Störungsbeseitigung. Die mittlere Reaktionszeit nach Eingang einer Störungsmeldung beträgt 30 Minuten.

6.5.4 Entstörzeit

Die Entstörzeit (Mean Time To Repair – MTTR) beginnt nach Eingang der telefonisch durchgegebenen Störungsmeldung.

Telefónica Germany beseitigt Störungen, die zum Ausfall des dem Auftraggeber bereitgestellten Dienstes führen, innerhalb der Prioritätskategorien gemäß nachfolgenden Entstörzeiten:

Priorität	Entstörzeiten (MTTR)*
Critical	4 Stunden
High	8 Stunden
Medium	24 Stunden
Low	72 Stunden

(*) Die Entstörzeiten gelten nicht für Störungen bei Internetanschlüssen, Entstörbearbeitungszeiten sind bei der Zeitbemessung entsprechend zu berücksichtigen.

6.5.5 Fehlkonfiguration durch den Kunden

Im Falle von durch den Kunden verursachten, teilweisen oder vollständigen Ausfällen der Leistung einer fehlerhaften Konfiguration im Konfigurationsportal wird Telefónica Germany die Funktion im Rahmen einer Entstörung manuell wiederherstellen, sofern eine Störungsmeldung erfolgt. Die Reaktions- und Entstörzeiten für die Bearbeitung werden hierbei ausgesetzt. Der Aufwand für die Wiederherstellung der Funktion kann dem Kunden im Nachgang in Rechnung gestellt werden.

Das gleiche gilt im Falle von Sicherheitsrisiken, die auf eine fehlerhafte Konfiguration des Kunden zurückzuführen sind.

6.5.6 Lokale Internetanschlüsse anderer Anbieter

Bei Nutzung von lokalen Internetanschlüssen anderer Anbieter stellt der Kunde vor einer Störungsmeldung bei Telefónica Germany sicher, dass diese Anschlüsse des Fremdanbieters einwandfrei funktionieren und als Fehlerquelle ausgeschlossen werden können. Dies betrifft sowohl Festnetz- als auch Mobilfunkprodukte.

Stellt Telefónica Germany im Rahmen der Störungsbearbeitung fest, dass sich die Fehlerquelle im Verantwortungsbereich des Fremdanbieters befindet, endet die Störungsbearbeitung durch den Telefónica Germany bzw. wird ausgesetzt bis zur Instandsetzung / Anschlussüberprüfung durch den Fremdanbieter.

Die Meldung von Störungen bei lokalen Internetanschlüssen anderer Anbieter obliegt dem Kunden. Eine Mitwirkung von Telefónica Germany erfolgt nicht. Die mit der Fehlersuche bei Telefónica Germany anfallenden Kosten können dem Kunden in Rechnung gestellt werden, sofern kein Fehler vorliegt, oder der Fehler nicht von Telefónica Germany zu vertreten ist.

7 Laufzeit und Kündigung

Sofern die vorliegende Leistungsbeschreibung Bestandteil eines Rahmenvertrages ist, gelten dessen Regelungen zu Laufzeit und Kündigung vorrangig. Im Übrigen gelten die folgenden Bestimmungen.

Die Laufzeit des Produktes richtet sich nach der Laufzeit der gebuchten standortbezogenen und standortunabhängigen Leistungen von O_2 Business SD-WAN an den Kundenstandorten. Hat ein Auftraggeber mehrere Dienste an einem Standort gebucht, so richtet sich die Laufzeit des Standortes nach der längsten Dienstlaufzeit an dem jeweiligen Standort. Die Kündigung eines Standortes ist möglich, soweit alle standortbezogenen Dienste an diesem Standort gekündigt werden. Eine Kündigung des Produktes ist möglich, soweit alle Dienste an allen Standort gekündigt und zudem alle standortunabhängigen Leistungen gekündigt werden.

Einzelverträge können erstmalig mit einer Frist von einem (1) Monat zum Ende der jeweiligen Mindestlaufzeit gekündigt werden. Wird ein Einzelvertrag nicht rechtzeitig gekündigt, verlängert sich die Laufzeit des Einzelvertrages unbefristet und kann jederzeit mit einer Frist von einem (1) Monat gekündigt werden.

Das Vertragsverhältnis kann von beiden Parteien jederzeit schriftlich mit einer Frist von vier (4) Wochen zum Monatsende gekündigt werden, erstmals jedoch zum Ende der Mindestvertragslaufzeit.

8 Kundenbetreuung

Die Kundenbetreuung ist im Rahmen der technischen und betrieblichen Möglichkeiten täglich von 0:00 bis 24:00 Uhr unter der kostenlosen Rufnummer 0800 22 10 422 erreichbar.

9 Rechnungsstellung

Die Rechnungsstellung für die Produkte erfolgt gemäß der bei Vertragsschluss gültigen Preisliste des Produktes bzw. dem individuellen Angebot der Telefónica Germany. Die Rechnung wird standardmäßig einmal im Monat versendet.

Soweit nicht abweichend vereinbart, beginnt die Entgeltpflicht des Kunden mit dem Tag der betriebsfähigen Bereitstellung der Leistung.

10 Sonstiges

Telefónica Germany behält sich das Recht vor, Dritte mit dem Aufbau, Betrieb und Management eines Dienstes oder Teilen davon zu beauftragen.

Telefónica Germany GmbH & Co. OHG