Leistungsbeschreibung Drei SD-WAN.

Stand: 30.04.2025

DreiBusiness.
Macht's einfach.

Inhalt.

1. Einleitung.

SD-WAN (Software-Defined Wide Area Network) ist eine Overlay-Lösung, die unabhängig von der zugrunde liegenden Netzwerkinfrastruktur funktioniert. SD-WAN lässt sich nahtlos über verschiedene Transporttypen wie Breitband, LTE/5G oder Satellit hinweg einsetzen. Durch die Abstraktion der Kontroll- und Verwaltungsebene vom physischen Netzwerk, ermöglicht SD-WAN Unternehmen, die Verkehrsführung basierend auf Anwendungsanforderungen und Leistungsanforderungen zu optimieren. Diese Flexibilität ermöglicht es Unternehmen, kostengünstige Transportoptionen zu nutzen und gleichzeitig an allen Standorten eine konsistente Sicherheit und Leistung aufrechtzuerhalten. Als Overlay bietet SD-WAN zentrale Netzwerksichtbarkeit und -kontrolle.

SD-WAN bietet gegenüber herkömmlichen MPLS-Netzwerken (Multiprotocol Label Switching) mehrere Vorteile und ist daher für moderne Unternehmen die beste Wahl. Im Gegensatz zu MPLS, das auf festen, privaten Leitungen basiert, nutzt SD-WAN jede Internetverbindung. Es ermöglicht eine zentrale Verwaltung und ermöglicht eine dynamische Verkehrsführung basierend auf Echtzeitleistung und Geschäftsprioritäten, was die Anwendungsleistung und das Benutzererlebnis verbessert. Darüber hinaus vereinfacht SD-WAN die Netzwerkbereitstellung und reduziert die Abhängigkeit von teuren MPLS-Verbindungen, indem verteilte Standorte sicher über öffentliche Internetverbindungen verbunden werden. Die Fähigkeit, Sicherheitsfunktionen wie integrierte Firewalls und Verschlüsselung zu integrieren, gewährleistet Datenschutz ohne zusätzliche Hardware. Da Unternehmen die Anforderungen erweitern und Multi-Cloud-Lösungen einführen, ist SD-WAN aufgrund seiner Agilität und Skalierbarkeit eine zukunftssicherere Lösung als MPLS.

Die folgende Abbildung zeigt die SD-WAN-Lösung von Drei:

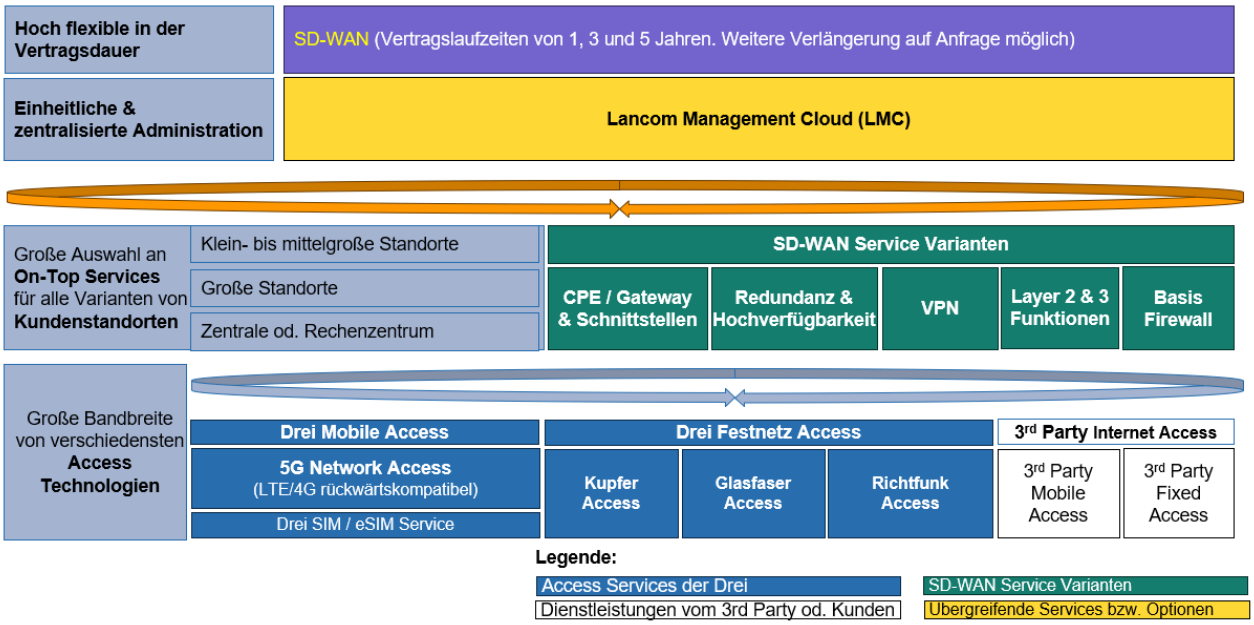

Abbildung 1: SD-WAN Portfolio Übersicht.

Unsere SD-WAN-Lösung ist für die flexible Kombination verschiedener Internet-Underlay-Lösungen von Drei oder von Drittanbietern konzipiert. Wenn der 5G-Internet-Underlay von Drei bereitgestellt wird, kann die Lösung mit demselben SD-WAN-Gerät angeboten werden (One-Box-Lösung für SD-WAN-Overlay und 5G Internet-Underlay).

Ein weiterer Vorteil ist die zentrale, cloudbasierte Administration über die LMC (Lancom Management Cloud) *, die sämtliche SD-WAN-Einstellungen sowie das Performance-Monitoring abdeckt. So können sich die Netzwerkspezialisten auf ihre Kernaufgaben konzentrieren und mithilfe der LMC viele bisher komplexe Netzwerkkonfigurationen ganz einfach erstellen, was den Zeitaufwand für das Ausrollen mehrerer oder aller Standorte deutlich reduziert.

Dank des „Zero Touch Deployment“- Ansatzes ist vor Ort meist kein spezielles Fachwissen erforderlich, um unsere SD-WAN-Lösung in Betrieb zu nehmen.

Unsere SD-WAN-Lösung bietet eine nahezu unbegrenzt skalierbare Vernetzungsoption – von der Anbindung zweier Standorte bis hin zur Enterprise-Größe mit mehreren tausend Niederlassungen – und überzeugt mit entscheidenden Vorteilen:

- Hochskalierbare und redundante Unternehmensvernetzungen
- gleichzeitige Nutzung mehrerer Aktiv-Aktiv-Verbindungen
- Einfache, cloudbasierte *) Administration inkl. Monitoring aller SD-WAN Features
- Voll- bzw. teilautomatisierte Provisionierungslösung über die Cloud *)

Drei bietet eine schlüsselfertige bzw. vollständig verwaltete SD-WAN-Lösung an, d. h. die End-to-End-Verantwortung für den Dienst liegt bei Drei.

*) Ausfälle der Cloud basierten Administration (LMC) haben keine Auswirkung auf Ihren Betrieb. Die Konfiguration Ihrer SD-WAN Lösung werden lokal je Standort in Ihrem vor Ort installierten CPE/Gateway abgespeichert.

1.1 Vorteile.

Die Drei SD-WAN-Lösung basiert auf dem LANCOM SD-WAN-Produktportfolio und bietet:

- Hochintegrierte, kosteneffiziente „One-Box“-Lösungen für SD-WAN-Overlay und -5G Underlay
- 100% Cloud-verwaltet und erweiterbar (LAN, WLAN, Sicherheit)
- Zero-Touch Provisionierung durch SSL, Auto-VPN zwischen den Standorten
- Höchste Effizienz und Skalierbarkeit durch LANCOM High Scalability VPN (HSVPN)
- Sofortige Erhöhung der am Standort verfügbaren Gesamtbandbreite durch Active/Active-Betrieb mehrerer Leitungen (Load Balancing – Session Basierend)
- Top-Qualität für digitale Anwendungen dank Dynamic Path Selection
- Schnelle und sichere Bereitstellung neuer Dienste an allen Standorten
- „One-Click-Security“an allen Standorten
- Höchste Skalierbarkeit dank zentraler Netzwerk- und Security-Orchestrierung für die gesamte Infrastruktur
- Vertrauenswürdige Cloud, die in Deutschland entwickelt und gehostet wird
- Agil, Made in Germany & DSGVO-konform und vielfach BSI-zertifiziert
- Netzwerksicherheit nach NIS2-Vorgaben
- Maximale Agilität & Performance
    - Automatisierte und standortunabhängige Provisionierung neuer Anwendungen, Arbeitsplätzen und Filialen
    - Flexible Anwendungspriorisierung
    - Hochmoderne WAN-Optimierung
- Schnelligkeit & Zuverlässigkeit
    - Optimierte Trouble Shooting Möglichkeiten durch Zentrales Management (LMC)
    - Steigerung der Bandbreite durch Ausnutzung aller am Standort verfügbaren Leitungen (bis 4 Leitungen)
    - Maximale Ausfallsicherheit
- Höchste Kostenersparnisse & Automatisierung
    - Ersatz/Ergänzung teurer MPLS-Leitungen durch kostengünstige Internetzugänge

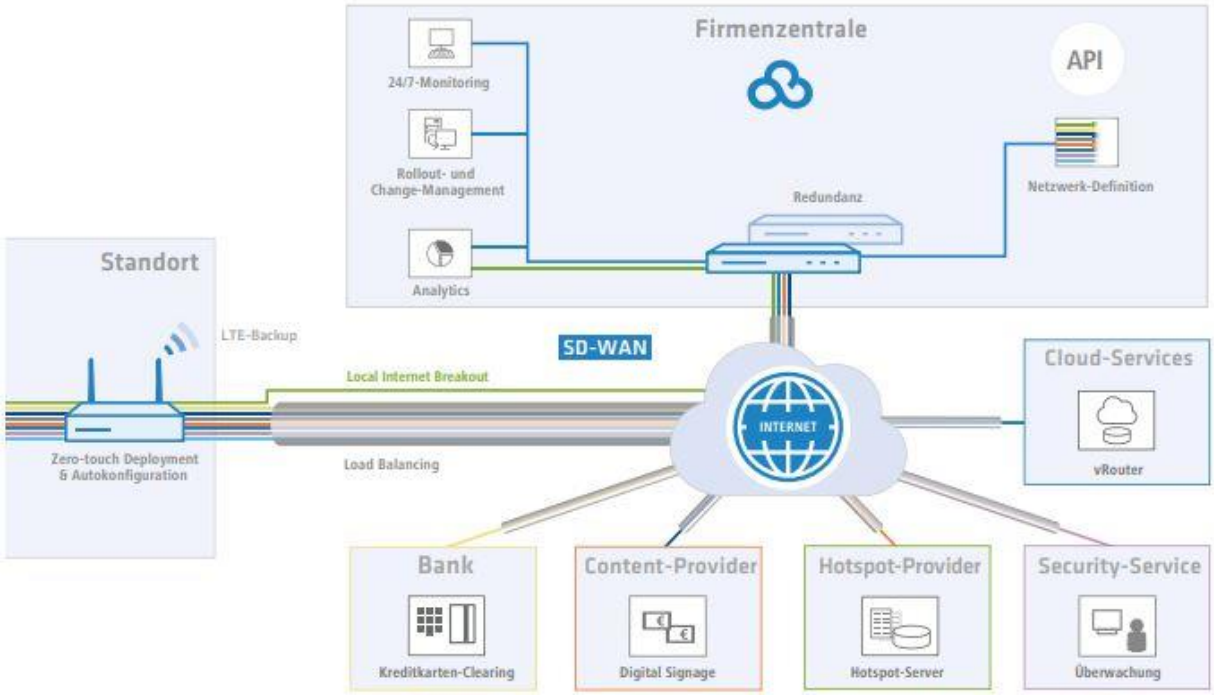

Abbildung 2: Generelle Übersicht - Drei SD-WAN.

Die Drei SD-WAN Lösung eignet sich für folgende Anwendungsfälle:

- Dynamische Standortvernetzung
- Multicloud-Konnektivität
- Sicherer Internetzugriff
- Automatische Optimierung der WAN-Kapazität (Load Balancing)
- Performante Anwendungen
- Sichtbarkeit von Netzwerk und Datenverkehr
- Skalierbarkeit

2. Technische Servicebeschreibung.

Drei SD-WAN wird in drei verschiedenen Varianten implementiert. Der Dienst kann mit Durchsatzbandbreiten bis zu 10 Gbit/s und unterschiedlicher Anzahl gleichzeitiger IPSec-VPN-Verbindungen implementiert werden. Die Varianten können mit unterschiedlichen Customer Premises Equipments (CPEs) umgesetzt werden. SD-WAN-Funktionalitäten sind über alle Varianten hinweg homogen und können über alle Varianten hinweg aktiviert werden.

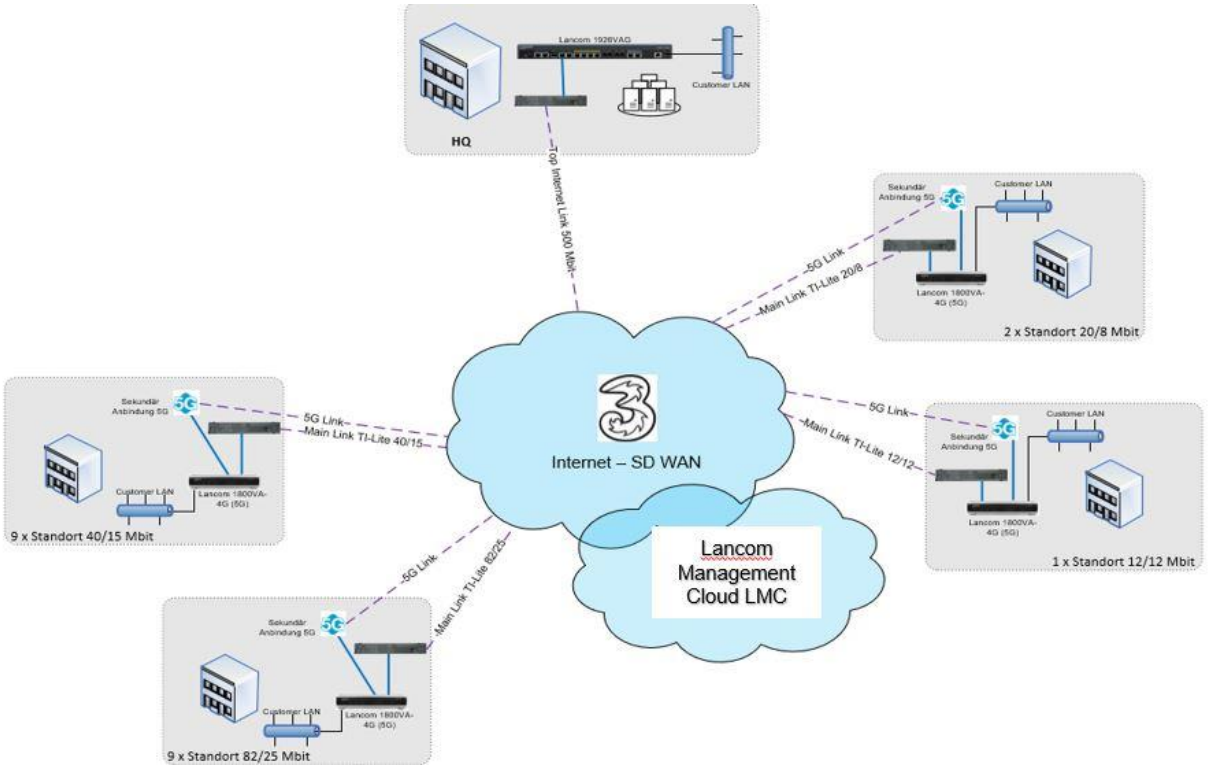

Abbildung 3: Technische Übersicht - Drei SD-WAN.

Drei SD-WAN kann in folgenden Varianten realisiert werden:

- SD-WAN für kleine oder mittlere Standorte – für Bandbreiten bis 1Gbps und 5 bis 25 simultane IPSec-VPN-Verbindungen
- SD-WAN für große Standorte – für Bandbreiten bis 1Gbps und 25 bis 100 simultane IPSec-VPN-Verbindungen
- SD-WAN für Hauptstandorte / Zentralen – für Bandbreiten bis 10Gbps und 100 bis 3000 simultane IPSec-VPN-Verbindungen

Die Realisierung der Varianten ist hardwareabhängig.

Eingesetzte CPE-Modelle für die verschiedenen Varianten können sich bedingt durch den Hardware-Lebenszyklus ändern.

2.1 SD-WAN Produkt Portfolio Übersicht (Service Varianten).

Drei SD-WAN-Lösung bietet ein breites Spektrum an Möglichkeiten je nach Durchsatz, Zugangstechnologie, WAN- und LAN-Schnittstellen, Mobilfunk- oder WLAN-Optionen. Die folgende Tabelle zeigt eine detaillierte Ansicht der Lösungsoptionen. **)

		1800EF	1800EF -5G	1800EFW	1800VA	1800VA - 5G	1800VAW	1930EF	1930EF-5G	1926VAG	1936VAG-5G	ISG-5000	ISG-8000	ISG-5000 + 750-5G	ISG-8000 + 750-5G	1926VAG + ISG-5000	1926VAG + ISG-8000
Standort Varianten	**Klein- bis mittelgroße Standorte** - bis 1Gbps	x	x	x	x	x	x										
	Große Standorte - bis 1Gbps							x	x	x	x					x	x
	Zentrale/Rechenzentrum - bis 10Gbps											x	x	x	x	x	x
Access Technologien	5G Network		x			x			x		x						
	Kupfer				x		x			x							
	Ethernet (Glasfaser oder Richtfunk)	x		x				x				x	x				
	Kupfer + 5G Access					x					x						
	Ethernet (Glasfaser oder Richtfunk) +5G		x						x					x	x		
	Kupfer + Ethernet (Glasfaser oder Richtfunk)				x		x			x						x	x
	Glasfaser + Ethernet (Glasfaser oder Richtfunk) + 5G					x					x			x	x		
Layer 2 Funktionen	Layer 2-Funktionen - VLAN, Multicast	x						x				x					
	Layer 2-Protokolle - Ethernet über GRE-Tunnel (EoGRE), L2TPv3, ARP-Lookup, LLDP, DHCP-Option 82, etc.	x						x				x					
Layer 3 Funktionen	Firewall	x						x				x					
	QoS	x						x				x					
	PPP, PAP, CHAP, MS-CHAP und MS-CHAPv2	x						x				x					
	Router - IPv4-, IPv6-, NetBIOS/IP-Multiprotocol-Router, IPv4/IPv6 Dual Stack	x						x				x					
	SD-WAN Application-Routing	x						x				x					
	SD-WAN Dynamic Path Selection	x						x				x					
	SD-WAN Zero Touch Deployment	x						x				x					
	Router-Virtualisierung - ARF (Advanced Routing und Forwarding)	x bis zu 16 Kontexten						x bis zu 64 Kontexten				x bis zu 256 Kontexten					
	Dynamische Routing-Protokolle - RIPv2, BGPv4, OSPFv2, LISP	x						x				x					
	Multicast Routing	x						x				x					
	WAN-Betriebsarten - VDSL, ADSL1, ADSL2 oder ADSL2+ mit externem Modem an einem ETH-Port (auch simultan zum LAN-Betrieb)	x						x				x					

		1800EF	1800EF -5G	1800EFW	1800VA	1800VA - 5G	1800VAW	1930EF	1930EF-5G	1926VAG	1936VAG-5G	ISG-5000	ISG-8000	ISG-5000 + 750-5G	ISG-8000 + 750-5G	1926VAG + ISG-5000	1926VAG + ISG-8000
Layer 3 Funktionen	WAN-Protokolle - PPPoE, Multi-PPPoE, L2TPv2 (LAC oder LNS), L2TPv3 mit Ethernet-Pseudowire und IPoE (mit oder ohne DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 und IPv4/IPv6 Dual Stack Session), IP(v6) oE	x						x				x					
	Tunnelprotokolle (IPv4/IPv6)	x						x				x					
Basis Firewall	Stateful Inspection Firewall mit Paketfilterung	x						x				x					
	Erweitertes Port-Forwarding	x						x				x					
	N:N IP-Adressumsetzung	x						x				x					
	Paket-Tagging	x						x				x					
	Threat Prevention: Intrusion Detection System / Intrusion Prevention System (IDS/IPS)	x						x				x					
	IP-Spoofing	x						x				x					
	Access-Control-Listen	x						x				x					
	Denial-of-Service Protection	x						x				x					
	URL-Blocker	x						x				x					
	CPEs Client VPN	x						x				x					
Redundanz und Hoch-verfügbarkeit	VRRP	x						x				x					
	FirmSafe	x						x				x					
	Load-Balancing	x						x				x					
	VPN-Redundanz	x						x				x					
VPN	IPSec over HTTPS	x						x				x					
	Anzahl der VPN-Tunnel	5 Tunnel gleichzeitig aktiv (25 mit VPN-25 Option) 25 Tunnel gleichzeitig aktiv (50 in Verbindung mit der VPN-50 Option, bzw. 100 in Verbindung mit der VPN-100 Option)						25 Tunnel gleichzeitig aktiv (50 in Verbindung mit der VPN-50 Option, bzw. 100 in Verbindung mit der VPN-100 Option)				ISG5000: 100 Tunnel gleichzeitig aktiv (200 in Verbindung mit der VPN-200 Option, 500 in Verbindung mit der VPN-500 Option bzw. 1000 in Verbindung mit der VPN-1000 Option) ISG8000: 250 Tunnel gleichzeitig aktiv (bis zu 3000 Tunnel in Verbindung mit der VPN +250 Option)					
	IKE, IKEv2	x						x				x					
	NAT-Traversal	x						x				x					
	LANCOM Dynamic VPN	x						x				x					
	Dynamic DNS	x						x				x					
	Pv4 VPN über IPv6 WAN	x						x				x					
	IPv6 VPN über IPv4 WAN	x						x				x					
	RADIUS	x						x				x					
	High Scalability VPN (HSVPN)	x						x				x					

		1800EF	1800EF -5G	1800EFW	1800VA	1800VA - 5G	1800VAW	1930EF	1930EF-5G	1926VAG	1936VAG-5G	ISG-5000	ISG-8000	ISG-5000 + 750-5G	ISG-8000 + 750-5G	1926VAG + ISG-5000	1926VAG + ISG-8000
VPN	IKEv2-EAP	x						x				x					
	Advanced Mesh VPN	x						x				x					
CPE / Gateway Schnittstellen	WAN	Ethernet 10/100/1000 MBit/s Gigabit Ethernet			VDSL / ADSL2+			Ethernet 10/100/1000 MBit/s Gigabit Ethernet		WAN: G.FAST / VDSL / ADSL2+ Ethernet 10/100/1000 MBit/s Gigabit Ethernet		Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus)		WAN 1: 5G WAN2: Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus)		WAN 1: G.FAST / VDSL / ADSL2+ WAN2: Jeder Ethernet-Port kann frei konfiguriert werden (LAN, DMZ, WAN, Monitor-Port, Aus)	
	Ethernet Ports	4 individuelle Ports, 10/100/1000 MBit/s Gigabit Ethernet. Bis zu 3 Ports können als zusätzliche WAN-Ports geschaltet werden			5 individuelle Ports, davon 1 Combo Port (TP/SFP), 10/100/1000 MBit/s Gigabit Ethernet, im Auslieferungszustand ist 1 Port als WAN geschaltet. Weitere 3 Ports können als zusätzliche WAN-Ports geschaltet werden			6 individuelle Ports, davon 1 Combo Port (TP/SFP), 10/100/1000 MBit/s Gigabit Ethernet, im Auslieferungszustand sind 2 Ports als WAN geschaltet. Weitere 3 Ports können als zusätzliche WAN-Ports geschaltet werden				ISG5000: 6 ETH-Ports (10/100/1000 MBit/s Ethernet) und zwei SFP+-Ports (10 GBit/s); bis zu 5 Ports können als zusätzliche WAN-Ports inkl. Load-Balancing geschaltet werden ISG8000: 8 ETH-Ports (10/100/1000 MBit/s) und zwei SFP+-Ports (10 GBit/s); bis zu 9 Ports können als WAN-Ports inkl. Load-Balancing geschaltet werden			
	USB-Host-Port	1xUSB 2.0						1xUSB 2.0				ISG5000: 2x USB 3.0 ISG8000: 2xUSB 2.0					
Drei Mobile Access / 3rd Party Mobile Access	5G-, LTE-, UMTS		x			x			x Dual SIM		x Dual SIM			x	x		
	5G Standalone (SA), 5G Non-Standalone (NSA)		x			x								x	x		
	Diversity / MIMO		x			x								x	x		
WLAN Erweiterung	Frequenzband 2,4 GHz und 5 GHz			x			x										
	IEEE 802.11ax (Wi-Fi 6)			x			x										
	IEEE 802.11ac (Wi-Fi 5)			x			x										
	IEEE 802.11n (Wi-Fi 4			x			x										
Management und Monitoring	LMC (LANCOM Management Cloud)	x						x				x					

**) Die Entscheidung der einzusetzenden Hardware wird Projektabhängig und nach Abstimmung individuell ausgewählt

2.2 Übersicht der SD-WAN Features & Funktionen.

Drei SD-WAN Lösung bietet eine Vielzahl von Möglichkeiten. Die wichtigsten Funktionalitäten sind hier aufgeführt:

- Policy Based Routing
- Application Monitoring
- Active/Active-Modus – Load Balancing
- Dynamic Path Selection (DPS)
- Advanced Routing and Forwarding (ARF)
- LAN-Segmentierung
- High Scalability Virtual Private Network (HSVPN)
- Verschlüsselte VPN-Tunnel
- Advanced VPN Client
- Basis Firewall
- Hub & Spoke -Topologie
- Advanced Mesh VPN
- Wireless LAN-Option
- Mobilfunk-Option (4G/5G)
- Lokaler Internet Breakout
- Trennung der Control Plane und Data Plane
- Zentrales Management aller Komponenten über die Lancom Management Cloud (LMC)
- WAN-Uplinks
- Network Functions Virtualization (NFV) – vRouter Option.
- Network Performance Monitoring

In den folgenden Kapiteln werden die wichtigsten SD-WAN-Funktionalitäten beschrieben.

2.2.1 Policy Based Routing.

Die Steuerung, welche Anwendungen in Unternehmensnetzwerken erlaubt oder blockiert sind, ist essenziell. Dies ist innerhalb des Orchestrators eines modernen SD-WAN problemlos möglich: Ein Policy Based Routing kann Anwendungen etwa „umleiten“ oder „blockieren“. Für vertrauenswürdige Anwendung empfiehlt sich an den einzelnen Standorten zudem eine Priorisierung durch ein Local Internet Breakout, sodass die Verbindung zur Zentrale nicht unnötig belastet und somit die Performance des gesamten Netzwerkes erhöht wird.

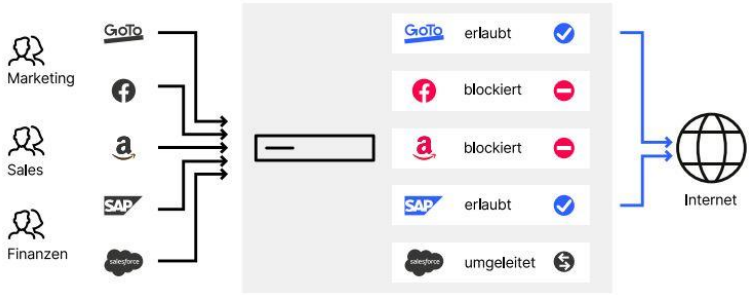

Abbildung 4: Policy Based Routing.

2.2.2 Application Monitoring.

Heutzutage ist es sehr wichtig, zu wissen, welche Anwendungen im Netzwerk verwendet werden, um dann eine entsprechende Steuerung im Bereich „Application Management“ vornehmen zu können. Drei SD-WAN erfasst rund um die Uhr, welche Benutzer welche Anwendungen in welchem Ausmaß verwenden (Top-Benutzer / Top-Anwendungen). Eine historische Protokollierung und grafische Auswertung bieten die beste Übersicht für sinnvolle Netzwerkentscheidungen.

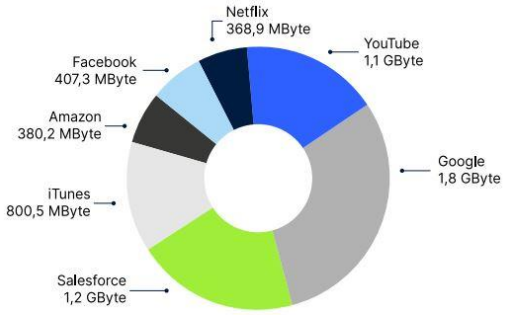

Abbildung 5: Application Monitoring.

2.2.3 Active/Active-Modus – Load Balancing.

Ein Active/Active-Betrieb, also die parallele Nutzung bzw. Load Balancing mehrerer Internetzugänge an einem Standort, erhöht die zur Verfügung stehende Gesamtbandbreite und erlaubt eine dynamische Lastverteilung. Dieser Modus erlaubt eine flexible und gleichzeitige Nutzung jeglicher Art kabelgebundener Leitungen – egal ob Ethernet, Glasfaser, xDSL an externem Modem oder sogar Mobilfunk.

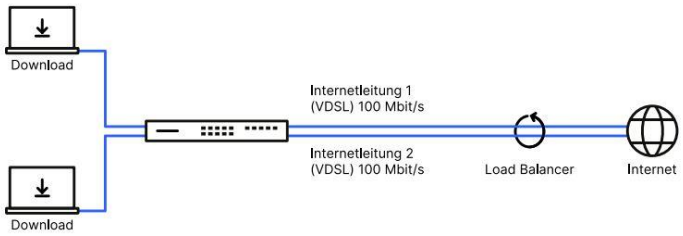

Abbildung 6: Active/Active-Modus – Load Balancing.

Hinweis: Die Active-Active-Funktionalität kann nur mit privaten LAN-IP-Adressen angeboten werden.

Wird der Public IP Bereich der Internetanbindungen direkt beim Nutzenden verwendet (z.B. Firewall), wird kein Active-Active (Load Balancing) in Richtung Internet unterstützt.

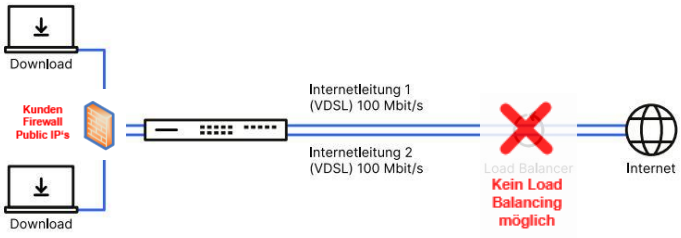

Abbildung 7: Active/Active-Modus – Load Balancing.

2.2.4 Dynamic Path Selection (DPS).

Bei Nutzung mehrerer Internetleitungen an einem Standort, kommt eine der größten Stärken eines modernen SD-WANs zur Geltung: Durch DPS, also eine intelligente Auswahl der für bestimmte Anwendungen qualitativ besten Leitung, wird maximale Performance und höchste Verfügbarkeit für digitale Anwendungen sichergestellt. Mit DPS werden in einem SD-WAN geschäftskritische Anwendungen stets über die qualitativ beste Leitung geroutet. Dabei werden alle Leitungen kontinuierlich durch aktives Monitoring mithilfe von ICMP-Paketen überwacht und daraus Metriken für Last, Paketverlust, Latenz und Jitter berechnet. Die Qualitätsanforderungen der einzelnen Anwendungen sind durch vordefinierte Richtlinien (Realtime Video, Voice over IP, Low Latency, Best Effort und Low Priority) an Leitungen festgelegt, beispielweise der erlaubte Paketverlust oder die maximale Latenz einer Leitung. Der Algorithmus zur DPS wählt für Sessions einer bestimmten Anwendung die Leitung mit der besten Qualität

aus. Erfüllen mehrere Leitungen die geforderten Richtlinien, so wird ein Load Balancing im Round-Robin-Verfahren über diese Leitungen durchgeführt.

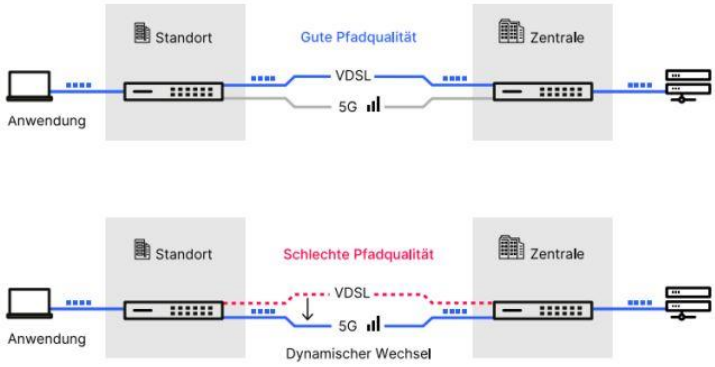

Abbildung 8: Dynamic Path Selection – DPS.

DPS ist konzipiert für den Einsatz in klassischen SD-WAN-Szenarien. Ein solches Szenario könnte so aussehen: Eine Filiale ist per VPN an die Zentrale angebunden. Dabei wird Internet Traffic über die Zentrale geroutet. Nur vertrauenswürdige, per se verschlüsselte Anwendungen, wie zum Beispiel Office 365, werden per Local Internet Breakout direkt ins Internet geroutet, ohne Umwege über die Zentrale. Dies reduziert den Internet-Traffic auf der Zentralseite und reduziert die Latenz für die direkt übertragenen Anwendungen. Damit ein Load Balancing mit DPS stattfinden kann, verfügt die Filiale über mehrere WAN-Verbindungen, bestenfalls von verschiedenen Providern. Diese Leitungen sind gleichzeitig aktiv, also in einem „Active/Active“-Betrieb.

2.2.5 Advanced Routing and Forwarding (ARF).

Diese Technologie dient dazu, über ein zentrales Gateway für unterschiedliche Anwenderkreise (beispielsweise Buchhaltung, Entwicklung und Management) jeweils einen separaten Kommunikationskanal einzurichten. Alle Kommunikationskanäle oder IP-Kontexte sind dabei gegeneinander abgeschirmt. Somit kann mehreren Teilnehmern je nach Anforderung die Berechtigung für bestimmte IP-Kontexte erlaubt werden, während ihnen andere Bereiche vorenthalten werden.

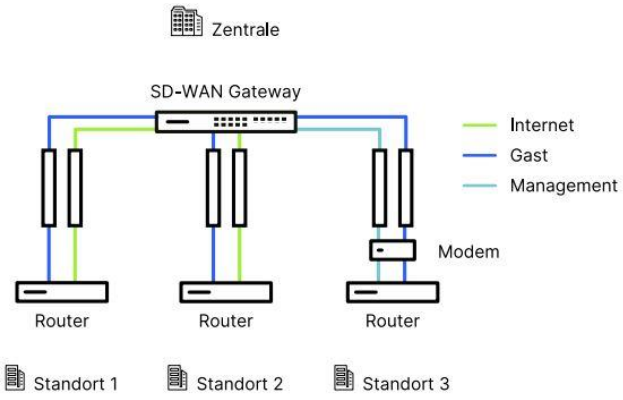

Abbildung 9: Advanced Routing and Forwarding (ARF).

2.2.6 LAN-Segmentierung.

Mit ARF wird die LAN-Segmentierung und sichere Implementierung IP-basierter Netzwerke über einen einzigen zentralen Router ermöglicht. Mit dieser Konfiguration können mehrere externe Teilnehmer mit unterschiedlichen Anforderungen in das unternehmensinterne IP-Netzwerk integriert werden, ohne ihnen gleichzeitig Zugriff auf das firmeneigene Intranet zu gewähren. Dadurch entfallen separate Kommunikationsnetze für jede Anwendung und Wartung und Konfiguration können zentral von einem Standort aus durchgeführt werden.

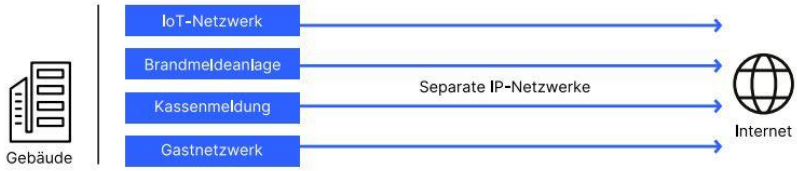

Abbildung 10: LAN-Segmentierung.

2.2.7 High Scalability Virtual Private Network (HSVPN).

Je komplexer eine Netzwerkinfrastruktur ist, desto mehr sollte bei der Planung und Umsetzung insbesondere der standortübergreifenden Übertragungswege ein passendes Netzwerkvirtualisierungsverfahren gewählt werden. Dabei empfiehlt sich grundsätzlich der Ansatz, die Anzahl der zum Einsatz kommenden Datentunnel gering zu halten, ohne auf die strikte Trennung der Routing-Kontexte und die Sicherheit eines modernen IPSecs zu verzichten. Genau dies wird mit HSVPN erreicht.

Eine effiziente Netzwerk Virtualisierung über IPSecVPN sollte allerdings grundsätzlich die Anzahl der verwendeten Tunnel - IPSec oder PPTP - möglichst geringhalten und die verfügbare MTU möglichst groß wählen. Dies geschieht hier mit dem Optimierungsschritt HSVPN, bei dem die Anzahl der IPSec-Tunnel deutlich reduziert wird.

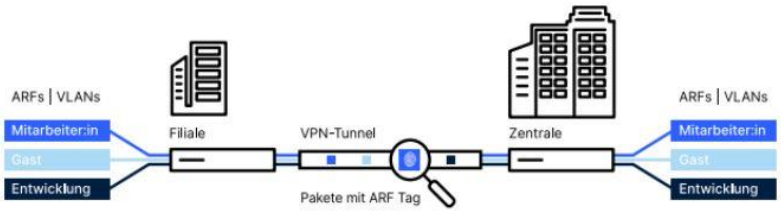

Abbildung 11: High Scalability Virtual Private Network (HSVPN).

HSVPN ist aus Verschlüsselungssicht ein modernes IPSec auf Basis von standardkonformem IKEv2 und bietet somit exakt dieselbe Sicherheit wie IKEv2. Zudem ist es nicht auf zentrale Verwaltungsinstanzen angewiesen und arbeitet als unabhängiges dezentrales System.

2.2.8 Verschlüsselte VPN.

Die SD-WAN-Lösung sorgt für „One-Click-Security“ an allen Standorten. Sie nutzt modernste Verschlüsselung mit IKEv2-IPSec-VPN gemäß den Anforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Das heißt: Egal wie viele digitale Anwendungen im SD-WAN-Netzwerk genutzt werden, alle werden sicher und strikt voneinander getrennt und über einen einzigen VPN-Tunnel an allen gewünschten Unternehmensstandorten bereitgestellt.

2.2.9 Advanced VPN Client.

Mit dem Advanced VPN Client können sich mobile Mitarbeiter jederzeit über einen verschlüsselten Zugang in das Unternehmensnetzwerk einwählen – ob im Home-Office oder unterwegs, im Inland wie im Ausland. Die Anwendung ist dabei denkbar einfach, denn nach einmalig erfolgter Konfiguration des VPN-Zugangs (Virtual Private Network) wird die sichere VPN-Verbindung intuitiv mit nur einem Klick über das beste verfügbare Verbindungsmedium aufgebaut, auch über das Mobilfunknetz. Für weiteren Schutz der Daten sorgt hierbei die integrierte Stateful Inspection Firewall, die Unterstützung aller IPSec-Protokollerweiterungen sowie weitere zahlreiche Sicherheitsfeatures.

2.2.10 Basis Firewall.

Die SD-WAN-Geräte unterstützen die folgenden Sicherheits-Firewall-Funktionen

- Stateful Inspection Firewall mit Paketfilterung
- erweitertes Port-Forwarding
- N:N IP-Adressumsetzung

- Paket-Tagging
- Threat Prevention: Intrusion Detection System / Intrusion Prevention System (IDS/IPS)
- IP-Spoofing
- Access-Control-Listen
- Denial-of-Service Protection
- URL-Blocker
- CPE Client VPN

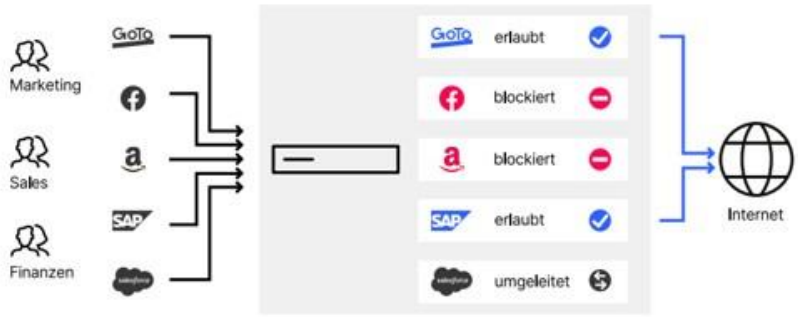

Abbildung 12: Basis Firewall.

2.2.11 Hub & Spoke SD-WAN Topology.

Die Topology des Overlay Netzwerks kann entweder als Hub & Spoke Architektur oder als Any 2 Any Architektur definiert werden. Hub & Spoke ermöglicht die Kommunikation einzelner Endknoten (Spokes) nicht direkt untereinander, sondern nur über einen zentralen Knoten (Hub). Je nach Konfiguration kann die Kommunikation zwischen Endknoten auch ganz unterbunden werden. Die jeweilige SD-WAN Topologie wird im Lösungsvorschlag festgelegt.

2.2.12 Advanced Mesh VPN.

Klassische VPN-Szenarien in der Standortvernetzung sind in der Regel sternförmig (Hub & Spoke) aufgebaut. Dabei bauen die angebundenen Filialen (Spokes) VPN-Tunnel zu einer oder mehreren Zentralen (Hubs) auf. In solchen traditionellen Szenarien ist ein Hub & Spoke-Netzwerk-Design eine logische Topologie Entscheidung, denn es fließen Daten hauptsächlich zwischen Filiale und Zentrale, da dort zentrale Server stehen, z. B. das Warenwirtschaftssystem, Datenbanken oder Webserver. Die Vorteile dieses sternförmigen Netzwerkdesigns sind der einfache Aufbau und die zentrale Steuerung in der Zentrale. Der Nachteil ist jedoch, dass sämtlicher Datenverkehr – auch der zwischen einzelnen Filialen wie z. B. Telefonie oder Dateiaustausch über einen File-Server – immer über den indirekten Weg über die Zentrale erfolgt. Dadurch wird die Internetanbindung der Zentrale mit dem Datenverkehr zwischen den Filialen belastet und somit zum Flaschenhals der gesamten Kommunikation.

Wir bieten für dieses Szenario die Lösung Advanced Mesh VPN. Hierbei besteht zunächst eine klassische sternförmige VPN-Struktur, in der alle Filialen zu Beginn einen VPN-Tunnel zur Zentrale aufbauen. Gibt es nun Datenverkehr zwischen den Filialen, so wird dynamisch ein VPN-Tunnel als Abkürzung zwischen den beiden beteiligten Filialen aufgebaut. Die Daten fließen nun direkt in einem VPN-Tunnel zwischen den Filialen, ohne dass die Daten den Weg über die Zentrale gehen.

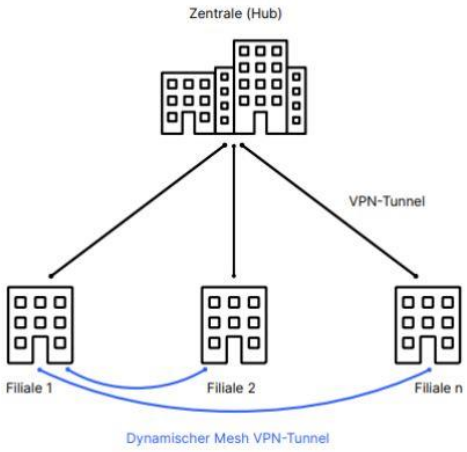

Abbildung 13: Advanced Mesh VPN.

Dabei fließen nur die ersten Datenpakete immer den langen Weg von der Filiale A über die Zentrale zur zweiten Filiale B. Erst beim Empfang der ersten Datenpakete in der Zielfiliale initiiert die Zielfiliale einen dynamischen VPN-Tunnel zur Filiale mit dem Ursprung des Datenpakets. Fließen nach einiger Zeit keinen Daten mehr, so wird der Tunnel dynamisch wieder abgebaut. Der Vorteil: Deutlich weniger Traffic in der Zentrale und einhergehend höhere Performance im gesamten Unternehmensnetzwerk.

2.2.13 Wireless LAN-Option.

Bestimmte CPE-Modelle sind mit einem integrierten WiFi Access Point ausgestattet. Dieser kann lokal am Standort aktiviert und benutzt werden. Es stehen sowohl das 2,4 GHz Band als auch das 5 GHz Band zur Verfügung, bis zu 14 SSID können eingerichtet werden.

Folgende WLAN-Optionen stehen zur Verfügung:

- Wi-Fi (Frequenzband 2,4 GHz und 5 GHz)
- IEEE 802.11ax (Wi-Fi 6)
- IEEE 802.11ac (Wi-Fi 5)
- IEEE 802.11n (Wi-Fi 4)
- IEEE 802.11b/g (Wi-Fi 2/3)
- IEEE 802.11a/h (Wi-Fi 1)

2.2.14 Mobilfunk-Option (4G/5G).

Bestimmte CPE-Modelle sind mit einem integrierten Mobilfunkmodul ausgestattet. Dieses kann aktiviert und genutzt werden, wenn die Lösung auf dem 5G-Zugang basiert. Wenn Mobilfunkleistungen von Drei genutzt werden, gilt der entsprechende Mobilfunktarif. Bei Drei Mobile Access stellen wir dem Nutzenden eine DreiSIM-Karte mit maximaler 5G Bandbreite 500/50 Mbit/s (Download/Upload) und dem dazugehörigen Drei-Tarif „Professional Flex Internet“ Plus 5G Daten Turbo zur Verfügung.

Bei WAN-Uplinks, die über Mobilfunk realisiert werden, sind je nach Nutzungsstandort und Standort des CPE qualitative Einschränkungen oder Empfangsprobleme möglich (Best Effort).

Folgende Mobilfunk-Optionen stehen zur Verfügung:

- UMTS
- 4G- (LTE)
- 5G-
- 5G Standalone (SA)
- 5G Non-Standalone (NSA)
- Diversity / MIMO

2.2.15 Local Internet Break Out.

Drei SD-WAN kann bestimmte Applikationen bzw. Services am Standort direkt ins Internet routen (Local Break Out).

2.2.16 Trennung von Control und Data Plane.

Ein wesentliches Merkmal für die Sicherheit einer modernen SD-WAN-Infrastruktur ist die strikte Trennung von Management- (Control Plane) und Datenverbindungen (Data Plane):

Während die Datenverbindungen (z. B. VPN-Tunnel) direkt zwischen den VPN-Gateways aufgebaut werden, wird jede einzelne Netzwerkkomponente direkt über eine unabhängige Managementverbindung mit einem Orchestrator verbunden. Das bedeutet: Nutzdaten bleiben für das Managementsystem verborgen und das Management und Monitoring der Netzwerkkomponenten erfolgt unabhängig vom Zustand der Datenverbindungen. Das Ganze erfolgt zudem vollautomatisch und ohne gesonderte vorherige Konfiguration der Geräte (zero-touch Provisionierung) durch einen gesicherten Verbindungsaufbau vom Gerät zum Management-System.

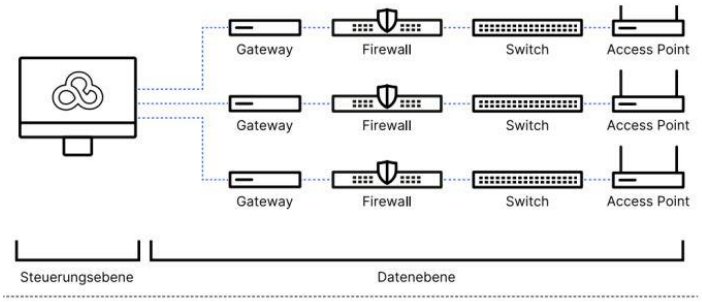

Abbildung 14: Trennung von Control und Data Plane.

Durch diese Verlagerung der Control Plane, also des Netzwerkmanagements in eine zentrale Cloud, entsteht der Vorteil einer permanent erreichbaren, standortunabhängigen, zentralen, Web-basierten Administrationsoberfläche für alle Geräte und alle Anwendungen an allen Standorten.

2.2.17 Zentrales Monitoring aller Komponenten über die LANCOM Management Cloud (LMC).

Die LANCOM Management Cloud (LMC) ist das Kontrollzentrum der Drei SD-WAN-Lösung und ist verantwortlich für Konfigurationsanpassungen, Firmware-Updates, Monitoring, Rollouts und Fehlerbehebung. Alle diese Aktivitäten erfolgen automatisiert und effizient gemäß den Erwartungen.

LMC bietet ausgezeichnetes Netzwerkmanagement mit folgenden Funktionalitäten:

- Eine Lösung, die den Netzwerkbetrieb automatisiert steuert und optimiert.
- Ein System, das Security-Policies und Compliance-Vorgaben umsetzt und überwacht.
- Eine Plattform, die die Komplexität und Betriebskosten nachhaltig reduziert und ein zentrales, skalierbares und zukunftssicheres Netzwerkmanagement ermöglicht.
- LMC steuert den gesamten Netzwerkbetrieb in den Bereichen WAN, LAN, WLAN und Security dynamisch über eine einzige Cloud-basierte Plattform – so automatisiert, wie gewünscht
- Erst entwerfen, dann bereitstellen
- Out-of-the-box-Lösung für alle Komponenten
- Automatische Gerätekonfiguration für weniger Fehlkonfigurationen
- Zentrales Netzwerkmanagement & Monitoring
- Leicht skalierbare Anbindung von Standorten, Home-Offices und Außendienstmitarbeitern
- Umfassende Firmware-Inventarisierung inklusive Zeitplanung
- Interoperabilität mit Drittsystemen dank offener API
- Individuelles Scripting durch Add-Ins

Abbildung 15: LANCOM Management Cloud – LMC.

2.2.18 WAN-Uplinks.

Drei SD-WAN kann je nach eingesetzter CPE-Variante bis zu 4 verschiedene IP-Services als Underlay-Netzwerk nutzen. Alle 4 Leitungen können aktiv für die Daten Kommunikation genutzt werden. (Active/Active/Active/Active-Nutzung des Underlay-Netzwerks). Als Internet-Underlay-Lösung mit 5G-Zugang kann die One-Box 5G-Lösung von Drei eingesetzt werden. Für andere Access Technologien können beliebige Drei-Internet-Lösungen (TopInternet oder OCI) oder Internet-Produkte anderer ISPs (Third-Party-Access) verwendet werden.

Multiple Uplinks.

Eine CPE unterstützt mehrere Uplinks (bis zu 4 aktive Uplinks) und bringt so zusätzliche Uplink-Resilienz und Bandbreite zu den Zweigstellen. Stehen mehrere WAN-Verbindungen an einem Standort zur Verfügung, optimiert Dynamic Path Selection (DPS) die Übertragungsqualität anhand der Ansprüche verschiedener Anwendungen. Die Verbindungen werden in einem 'Active-Active' Load Balancer-Verbund betrieben und bezüglich der Übertragungsqualität kontinuierlich vermessen. Viele häufig genutzte Anwendungen werden automatisch erkannt und sind anhand ihrer typischen Qualitätsansprüche bereits den DPS-Kategorien Voice over IP, Real Time Video, Low Latency, Best Effort und Low Priority zugeordnet. Es können auch individuelle Applikationen definiert werden.

2.2.19 Network Functions Virtualization (NFV) – vRouter Option.

Der vRouter ist ein softwarebasierter Router für den Betrieb in virtualisierten Umgebungen auf Basis eines Hypervisors wie VMware ESXi, Amazon Web Services (AWS), Hyper-V oder Microsoft Azure. Mit seinem umfassenden Funktionsumfang und den zahlreichen Sicherheitsfeatures auf Basis des Betriebssystems LCOS bietet er die beste Basis für moderne Infrastrukturen. Ob als virtueller VPN-Router (vCPE) oder als Central Site VPN-Gateway (vGateway) eignet er sich optimal für den Einsatz in mittleren und großen Unternehmen.

Der vRouter bietet:

- Virtueller, softwarebasierter Router für den Betrieb mit VMware ESXi, Amazon Web Services (AWS), Hyper-V oder Microsoft Azure
- Einsetzbar als Branch Router (vCPE) oder Central Site VPN Gateway (vGateway)
- IPSec-VPN-Funktionalität für bis zu 3.000 VPN-Kanäle
- Einfaches Management über die LANCOM Management Cloud oder LAN-tools´
- Radikale Vereinfachung der Konfiguration mit SD-WAN
- Instant Deployment überall: Drastische Reduzierung der Bereitstellungszeiten überall dort, wo der Router benötigt, wird
- Verfügbar als vRouter 50, 250, 1.000 und Unlimited für unterschiedliche Leistungsanforderungen
- Integrierte Public Spot Option (inkl. PMS Accounting plus)
- Integrierte HA-Clustering-Funktion

Es ist vorgesehen, dass die für diese Lösungsvariante einzusetzende Hardwarekomponenten vom Nutzenden bereitgestellt wird. Für diese Hardwarekomponenten wird seitens Drei keine Verantwortlichkeit noch Wartung bereitstellt. Die für die Hardwaredimensionierung zu berücksichtigenden Systemanforderungen (z.B.: RAM, CPU, Disk Space, Cores, etc) werden dem Kunden im Zuge des Angebots oder spätestens in der Projektphase von Drei bekannt gegeben.

2.2.20 Network Performance Monitoring.

Drei SD-WAN kann die genutzten Underlay-Services auf deren Qualität und Übertragungs-Performance überwachen. Hierbei werden periodisch Application Probes zu den aktiven Routing Zielen (andere CPEs, Cloud Instanzen, etc.) gesendet und die Qualität der Übertragung anhand der Parameter Latency, Jitter, Packet Drops ermittelt.

3. Hardware-Portfolio.

SD-WAN Edge-Komponenten sorgen in Form des ausgereiften Router-Portfolios für starke Bandbreiten, sichere Kommunikation und vertraulichen Datenaustausch in professionellen Netzwerken. Dieses Portfolio mit integrierten Schnittstellen für Glasfaser (inkl. GPON), xDSL, Gigabit Ethernet, SuperVectoring, LTE-Advanced und 5G vernetzt kleine, mittlere und große Unternehmen.

Alle Geräte unterstützen maximale Zukunftsfähigkeit, Zuverlässigkeit und Sicherheit „Engineered in Germany“. Sie unterstützen außerdem Zero-Touch-Inbetriebnahme, Auto-VPN und Auto-VLAN über die LANCOM Management Cloud – LMC.

Abhängig vom ausgewählten Modell (siehe Kapitel 2.1) können die CPEs die folgenden physischen Schnittstellen unterstützen:

- ETH-Ports (10/100/1000 MBit/s)
- VDSL (VDSL2, VDSL SuperVectoring, VDSL2-Vectoring)
- ADSL2+
- SFP-Module für Fibre Optic

Die Modelle ISG-5000 und ISG-8000 bieten die folgende Möglichkeit:

- 2x 10G SFP+-Ports
- 6x GE-ETH-Ports – ISG-5000
- 8x GE-ETH-Port – ISG-8000

3.1 LANCOM 1800EF.

Beste Verbindung für Ihr kleines bis mittleres Unternehmen: Mit einem integrierten SFP-Port nutzt dieser Business-VPN-Router die Performance moderner Glasfaseranschlüsse. Größtmögliche Flexibilität bezüglich der am Standort verfügbaren Internetleitungen wird über den Gigabit Ethernet WAN-Port gewährleistet. Mit ausgezeichnetem LANCOM IPSec-VPN und SD-WAN werden 5 (optional 25) Standorte und mobile Mitarbeiter sicher miteinander vernetzt.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800EF/DS_1800EF_DE.pdf

3.2 LANCOM 1800EF-5G.

Hohe Performance und Ausfallsicherheit: In Unternehmensstandorten mit datenintensiven und geschäftskritischen Anwendungen garantiert dieser Business-VPN-Router aufgrund seiner hohen Schnittstellenvielfalt eine zuverlässige Vernetzung. Er eignet sich für den direkten Anschluss sowohl an moderne Glasfaseranschlüsse als auch an externe Modems. Das zusätzlich integrierte 5G-Modem sorgt bei Ausfall des kabelgebundenen Internets aber auch als mobiler Primärzugang für jederzeit beste Verbindung. Mit ausgezeichnetem LANCOM IPSec-VPN und SD-WAN werden 5 (optional 25) Standorte und mobile Mitarbeiter sicher miteinander vernetzt.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800EF-5G/DS_1800EF-5G_DE.pdf

3.3 LANCOM 1800EFW.

Starke Performance für kleinere Unternehmensstandorte mit hohem Datenaufkommen: Ausgestattet mit schnellem Wi-Fi 6 bindet dieses SD-WAN Gateway mobile Endgeräte zuverlässig und parallel in den 5 GHz- und 2,4 GHz-Bändern ins Netzwerk ein. Für schnelles Internet nutzt es über den integrierten SFP-Port die Performance moderner Glasfaseranschlüsse. Größtmögliche Flexibilität bezüglich der am Standort verfügbaren Internetleitungen wird über den Gigabit Ethernet WAN-Port gewährleistet. Mit ausgezeichnetem LANCOM IPSec-VPN und SD-WAN werden 5 (optional 25) Standorte und mobile Mitarbeiter sicher miteinander vernetzt.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800EFW/DS_1800EFW_DE.pdf

3.4 LANCOM 1800VA.

Mit dem SD-WAN Gateway LANCOM 1800VA vernetzen Sie Ihre kleinen und mittelgroßen Unternehmens- und Filialinfrastrukturen einfach, sicher und zuverlässig. Das integrierte VDSL-Modem sowie eine optionale Glasfaser-Anbindung gewährleisten auch bei hohem Datenaufkommen eine schnelle Internetverbindung für Ihre Anwendungen. Die unkomplizierte Vernetzung mobiler Mitarbeitender oder Standorte ist durch ausgezeichnetes LANCOM IPSec-VPN garantiert. Ebenfalls unkompliziert: Durch die Integration des LANCOM 1800VA in die LANCOM Management Cloud (LMC) automatisiert und zentralisiert sich Ihr Netzwerkmanagement, damit administrative Aufgaben wie der Rollout neuer Netzwerkkomponenten, das Monitoring sowie die Verwaltung der Bestandsgeräte auch für viele Filialstandorte im Handumdrehen erledigt ist.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800VA/DS_1800VA_DE.pdf

3.5 LANCOM 1800VA-5G

Sicher, flexibel, hochverfügbar – so kann die Standortvernetzung über SD-WAN für Ihre mittelständischen Filialinfrastrukturen aussehen. Der LANCOM 1800VA-5G stellt mit der parallelen Nutzbarkeit mehrerer Internetzugänge via VDSL, Glasfaser und 5G beste Verbindungsqualität für Ihre geschäftskritischen Anwendungen sicher. Dank 5G sind intelligente Backup-Szenarien oder der Primärbetrieb mit niedrigen Latenzen für Echtzeitanwendungen kein Zukunftsszenario mehr. Durch die Erhöhung der bereitgestellten

Bandbreiten binden Sie mobile Mitarbeitende und Standorte auch bei höherem Datenaufkommen sicher mit LANCOM IPSec-VPN an Ihre Zentrale an. Mit nur wenigen Klicks integrieren Sie den LANCOM 1800VA-5G in die LANCOM Management Cloud (LMC) und zentralisieren, automatisieren und beschleunigen Ihr Netzwerkmanagement.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800VA-5G/DS_1800VA-5G_DE.pdf

3.6 LANCOM 1800VAW.

Die aktuelle Herausforderung für die IT mittelständischer Unternehmen liegt in einer zuverlässigen und hochgradig sicheren Standortvernetzung. Mit skalierbarer SD-WAN-Technologie und schnellem Dual-Band Concurrent Wi-Fi 6 bringt der LANCOM 1800VAW genau die Power mit, die Sie dafür brauchen. Auch bei hohem Datenaufkommen ist eine performante Internetanbindung dank des integrierten VDSL-Modems sowie der optionalen Glasfaser-Anbindung sichergestellt. Ihre Filialen und mobilen Mitarbeitende vernetzen Sie mit LANCOM IPSec-VPN unkompliziert und schnell. Mit dem zentralen Management des LANCOM 1800VAW und weiterer Geräte in der LANCOM Management Cloud (LMC) automatisieren und beschleunigen Sie nicht nur Ihre Arbeitsabläufe, sondern nutzen wertvolle Ressourcen wie Geld und Zeit effizienter.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1800VAW/DS_1800VAW_DE.pdf

3.7 LANCOM 1930EF.

Für die Standortvernetzung mittelgroßer und großer Unternehmen bietet der LANCOM 1930EF als SD-WAN Gateway flexibel verschiedene Internetanschlüsse auf einem Gerät. Über Gigabit Ethernet können beliebige externe DSL- oder Kabelmodems angebunden werden. Mit dem Anschluss an Glasfaserleitungen über ein optionales Modul profitieren Sie zudem von Highspeed-Internet selbst bei datenintensivem Datenverkehr. Die intelligente Lastverteilung auf zwei Internetleitungen mittels Load Balancing erhöht die zur Verfügung stehende Bandbreite und reduziert die Auslastung des Netzwerkes. Über die LANCOM Management Cloud (LMC) verwaltet, zentralisieren Sie das Management des LANCOM 1930EF, sorgen für ein einheitliches und sicheres Netzwerkmanagement und profitieren von Security „Engineered in Germany“.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1930EF/DS_1930EF_DE.pdf

3.8 LANCOM 1930EF-5G.

Bei hohen Leistungsansprüchen auf Filialseite ist der LANCOM 1930EF-5G die erste Wahl, um eine flexible und ausfallsichere Standortvernetzung zu realisieren. Mit Dual-SIM 5G-Mobilfunk ausgestattet, ist der Primärbetrieb für datenintensive und latenzkritische Echtzeitanwendungen ebenso wie intelligente Backup-Szenarien möglich. Zusätzlich sorgt der Anschluss an Glasfaserleitungen über ein optionales Modul für Highspeed-Internet bei geschäftskritischem Datenverkehr. Der LANCOM 1930EF-5G kann zusammen mit weiteren Netzwerkkomponenten zentral über die LANCOM Management Cloud (LMC) konfiguriert und verwaltet werden.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1930EF-5G/DS_1930EF-5G_DE.pdf

3.9 LANCOM 1926VAG.

Dieses high-end SD-WAN Gateway kombiniert erstmals zwei VDSL-SuperVectoring-Modems in nur einem Gerät für eine Bandbreite von 2x 300 MBit/s durch gleichzeitige Nutzung beider Anschlüsse. Alternativ kann das Gerät auch an einem G.Fast-Gigabit-Anschluss betrieben werden. Ausgestattet mit State-of-the-art SD-WAN-Technologie für sichere und automatisierte VPN-Standortvernetzung ist der LANCOM 1926VAG die Top-Lösung in mittelgroßen und großen Filialinfrastrukturen.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1926VAG/DS_1926VAG_DE.pdf

3.10 LANCOM 1936VAG-5G.

Mit dem LANCOM 1936VAG-5G Gerät erfüllen Sie höchste Leistungsansprüche auf Filialseite: Die Kombination aus zwei integrierten VDSL-Supervectoring-Modems, einem Dual-SIM 5G-Modem und einer optionalen Glasfaser-Anbindung sorgt für eine hochverfügbare Multi-WAN-Anbindung Ihrer Standorte – selbst bei geschäftskritischem Datenverkehr und erhöhtem Datenaufkommen. Mit 5G-Mobilfunk sind der Primärbetrieb mit niedrigen Latenzen für Echtzeitanwendungen oder intelligente Backup-Szenarien clever realisierbar. Durch die parallele Nutzung mehrerer Internetzugänge wird die Last im Netzwerk ideal verteilt und die Bandbreite optimal genutzt (Load Balancing). Ein zentrales Netzwerkmanagement über die LANCOM Management Cloud (LMC) rundet das Gesamtpaket des LANCOM 1936VAG-5G ab und automatisiert Ihre Administration von mittelgroßen und großen Netzwerken.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-1936VAG-5G/DS_1936VAG-5G_DE.pdf

3.11 LANCOM 750-5G.

Erweitern Sie Ihre Netzwerkinfrastruktur komfortabel um schnellen 5G-Mobilfunk. Das Gerät ist ideal geeignet für den Einsatz als Modem bzw. "externe 5G-Antenne". Außerdem können Sie den LANCOM 750-5G entweder als mobilen Primärzugang oder für Backup-Zwecke nutzen. Auch als Router lässt sich das Gerät einfach in das Netzwerk integrieren und kann dank Power over Ethernet auch ohne zusätzliches Netzteil mit Strom versorgt werden. So kann das Gerät flexibel an Orten mit bester 5G-Abdeckung platziert werden.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-750-5G/DS_750-5G_DE.pdf

3.12 LANCOM ISG-5000.

Multi-Service-IP-Netzwerke benötigen auf der Zentralseite absolute Hochleistung und Zuverlässigkeit. Das Multi-Gigabit-Gateway LANCOM ISG-5000 bildet den sicheren und zukunftsfähigen Kern Ihrer VPN-Vernetzungsstrategie dank leistungsstarker Plattform mit modernsten Verschlüsselungstechnologien, High Scalability VPN und Redundanz-Funktionen. Vernetzen Sie über SD-WAN mühelos Standorte, Filialen und externe Mitarbeiter. Und bei Bedarf erweitern Sie das Gerät um weitere Funktionen wie Hotspot, Clustering oder bis zu 1.000 VPN-Kanäle.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-ISG-5000/DS_ISG-5000_DE.pdf

3.13 LANCOM ISG-8000.

Sehr große Multi-Service-IP-Netzwerke benötigen auf der Zentralseite Hochleistung und Zuverlässigkeit. Das Multi-Gigabit-Gateway LANCOM ISG-8000 bildet den sicheren und hoch performanten Kern Ihres SD-WAN. Dank leistungsstarker Plattform mit modernsten Verschlüsselungstechnologien, High Scalability VPN und umfangreichen Redundanz-Funktionen erhalten Sie ein Software-Defined Wide Area Network (SD-WAN), das Ihnen den Administrationsaufwand deutlich erleichtert. So vernetzen Sie über die LANCOM Management Cloud eine Vielzahl an Standorten, Filialen und externen Mitarbeitern. Und bei Bedarf erweitern Sie dieses Integrated Services Gateway um weitere Funktionen wie Hotspot, Clustering oder bis zu 3.000 VPN-Kanäle.

Genauere technische Informationen können aus dem technischen Datenblatt entnommen werden:

https://www.lancom-systems.de/fileadmin/download/LC-ISG-8000/DS_ISG-8000_DE.pdf

4. Service Einrichtung (Herstellung), Support und SLA.

4.1 Prüfung und Herstellung des SD-WAN-Services.

Drei errichtet an jedem Endpunkt ein SD-WAN Service am Standort, sofern es wirtschaftlich und technisch möglich ist. Dazu erfolgt in der Pre-Sales Phase eine genaue Prüfung der technischen Umsetzbarkeit (z.B: Möglichkeiten zur Umsetzung der Drei Mobile oder Drei Festnetz Access Anbindung) wie des am Standort möglichen SLA-Portfolios.

Die Herstellungsphase kann mehrere Phasen der Realisierung durchlaufen, welche mit dem Nutzenden im Zuge der Pre-Sales Phase definiert; und vereinbart werden.

- Als Option:
  - Proof of Concept (POC) Phase
- Im Zuge der Herstellung:
  - Pilot Phase (maximal 1-2 Standorte)
  - Rollout der Gesamtlösung (alle Kundenstandorte)
    - Rollout der restlichen Standorte lt. IML (Ihre Maßgeschneiderte Lösung)
    - Rollout In Tranchen aufgeteilt (bei hoher Standortanzahl) lt. IML

4.2 Proof of Concept (POC) Phase:

Die Proof of Concept (POC) Phase dient dazu, dem Nutzenden die Möglichkeit vor einer Bestellung der SD-WAN Lösung zu geben, die angestrebte Lösung in der hauseigenen Umgebung (auf 2 bis max. 3 ausgewählte „Teststandorte“ des Nutzenden) auf die prinzipiell vom Nutzenden gesuchte Funktionsweise und Kompatibilität prüfen zu können.

Im Zuge dessen erhält der Nutzende zur Entscheidungsfindung eine optimale Vorstellung („Look and Feel“) über die von Drei angebotene SD-WAN Lösung, dessen Potential und Interoperabilität mit einer eigenen IT-Infrastruktur und Business Applikationen.

Der Lieferung der POC ist eine optionale Dienstleistung, welche besonders bei komplexen Anforderungen im Zuge der POC-Phase zu empfohlen ist.

Vorteile:

1. Risikominimierung: Potenzielle Schwachstellen und Herausforderungen werden frühzeitig identifiziert.
2. Kostenersparnis: Entscheidungen Verbesserung vor der Pilot- und Rollout-Phase
3. Praxisbezug: Direkt ersichtlich, wie die Lösung ihre spezifischen Anforderungen erfüllt.
4. Schnelle Ergebnisse: Der POC liefert in kurzer Zeit Einblicke in die Machbarkeit und den Nutzen.
5. Entscheidungsgrundlage: Der POC erleichtert es, die fundierten Entscheidungen zu treffen und interne Stakeholder von der Drei IML-Offerte zu überzeugen.

Bekannte Anforderungen & Limitationen im POC:

- Es gibt keine Garantie die gewünschte Funktionalität auch erreichen zu können
- Der POC dient rein als „Testumgebung“; und ist für eine reale Betriebsphase nicht vorgesehen
  - Somit gelten keine SLAs für eine in Betrieb genommene POC
- Entsprechende Maßnahmen zur betrieblichen Risikominimierung liegen in der Verantwortung des Kunden, wenn der POC auf in Betrieb befindliche Standorte / Umgebungen eingebunden wird.
- Erhöhte initiale Aufwände und Zeiten zur erfolgreichen POC-Implementierung im Zuge einer Problem-; Fehleranalyse können nicht ausgeschlossen werden
- Der Nutzende muss entsprechendes IT-Knowhow zur Integration der Drei POC in dessen IT-Umgebung während der Herstell- und Testphase zur Verfügung stellen
- Außerhalb des POC liegende, oder nicht vorhersehbare Aufwände bzw. Support-Dienstleistungen werden lt. jenen in Kapitel 4.9 definierten Regelwerken in Rechnung gestellt.

Fazit: Ein POC schafft Klarheit, Vertrauen und eine solide Basis für die nächsten Schritte der Bestellung und Herstellung von Drei gelegten IML-Angebotes.

Die Beauftragung eines POCs erfolgt immer unabhängig einer möglichen Bestellung des im Zuge der Pre-Sales Phase gelegten Gesamtangebotes IML (Ihre Maßgeschneiderte Lösung), wobei üblicherweise jene mit dem POC-Angebot verbundene Kosten im Zuge der IML-Bestellung dann gegengerechnet würden.

4.3 Pilot Phase:

Nach der Bestellung erfolgt der Rollout der SD-WAN Lösung im ersten Schritt über eine Pilotphase.

Eine Pilotphase ermöglicht es dem Kunden, unsere Lösung in einem begrenzten, realen Umfeld zu testen, bevor sie flächendeckend eingeführt wird.

Der Pilot dient als Referenz der Ziel-Erfüllung lt. dem im IML definierten Scope und inkludiert eine entsprechende Abnahme, welche im Zuge der Projektierung vereinbart wird.

Der Pilot umfasst maximal 2-3 Standorte, mit einer vorab vereinbarten Beobachtungszeit von maximal 14 Tagen bis zum Übergang in den Regelbetrieb, sobald die Abnahme der Pilot-Standorte erfolgreich abgeschlossen wurde.

Der Pilot-Standort geht danach in den Regelbetrieb mit dem entsprechend mit Drei vereinbarten SLA lt. IML über.

Vorteile:

1. Praxisnahe Validierung: Die Drei Lösung wird unter realen Bedingungen erprobt, um ihre Funktionalität und Effektivität sicherzustellen.
2. Anpassungsmöglichkeiten: Erkenntnisse aus der Pilotphase ermöglichen Optimierungen vor dem vollständigen Rollout.
3. Risikoreduktion: Potenzielle Probleme oder Fehlkonzepte werden frühzeitig erkannt und behoben.
4. Schulungen: Nutzer können in kleinerem Rahmen geschult werden.
5. Datenbasierte Entscheidungen: Ergebnisse aus der Pilotphase liefern wertvolle Einblicke und schaffen eine solide Basis für die weitere Planung.

Fazit: Die Pilotphase ist ein wichtiger Zwischenschritt, um Risiken zu minimieren und die Erfolgswahrscheinlichkeit der Lösung im Zuge der darauffolgenden Rollout Phase zu maximieren.

4.4 Rollout Phase:

Der Rollout ist die Phase, in der eine Lösung nach erfolgreicher Prüfung (Abnahme der Piloten) flächendeckend implementiert wird.

Hier unterscheiden wir typischerweise in 2 Handhabungen:

- Rollout der Standorte in einer einzigen Projektierungsphase mit kurzen Durchlaufzeiten.
- Rollout In Tranchen aufgeteilt, welche in unterschiedlichen meist darauffolgenden, Projektierungsphasen realisiert wird (z.B: bei hoher Standortanzahl oder Durchlaufzeiten)

Vorteile:

1. Skalierung der Lösung: Nach erfolgreichem Test wird die Lösung vollständig eingeführt, um ihren Nutzen voll auszuschöpfen.
2. Effizienzsteigerung: Herstellprozesse werden automatisiert oder optimiert, was Zeit und Kosten spart.
3. Die Standort Einzelabnahme und Finale Abnahme, bestätigen die erfolgreiche Umsetzung und dessen Gesamtabschluss der im IML offerierten SD-WAN Lösung.

Fazit: Der Rollout markiert den Übergang von der Planung zur operativen Nutzung, wodurch die Vorteile der Lösung für alle Beteiligten dann spürbar werden.

4.5 Allgemeine bauliche Voraussetzungen.

Die Errichtung eines SD-WAN Services erfordert einen Aufstellungs- oder Betriebsraum am Standort, der sauber, trocken, staubfrei und ausreichend belüftet ist. Es ist vom Nutzenden sicherzustellen, dass ein Betriebstemperaturbereich von Temperaturbereich 0-40° C; Luftfeuchtigkeit 05-85%; nicht kondensierend eingehalten wird.

4.6 Service Implementierung & Einrichtung.

Drei installiert im Aufstellungsraum an einer geeigneten und für eine allfällige Störung leicht zugänglichen Stelle, eine CPE.

Der für die CPE erforderliche Platz ist an geeigneter Stelle zu Verfügung zu stellen, wobei die für die CPE erforderliche Stromversorgungen (230 VAC) und LAN-seitige Verkabelung vom Nutzenden bereitzustellen sind.

Liegt der Standort in einem erhöht blitzgefährdeten Gebiet, so ist vom Nutzenden der Einbau eines Überspannungsschutzes erforderlich.

Die CPE bildet den Abschluss des Übertragungsweges des SD-WAN Overlay Netzes von Drei, also den Netzabschlusspunkt.

Der Netzabschlusspunkt legt die Grenze der Verantwortung zwischen dem Nutzenden und Drei fest. Alle Netzeinrichtungen vor der CPE (auf der Netzseite /WAN), also die Access Technologien selbst liegen im Verantwortungsbereich von Drei, oder des jeweiligen 3rd Party Anbieters.
Alle Einrichtungen hinter dem Netzabschlusspunkt (LAN – Local Area Network) z.B. Server, Switches, Router, Cloud Services, aber auch DNS, DHCP etc., liegen im Verantwortungsbereich des Nutzenden.

4.7 Herstellung & Installation.

Die Herstellung des SD-WAN Services erfolgt entsprechend den üblichen Regeln für die Installation (Standardinstallation). Die Verkabelung erfolgt dementsprechend mit einem geschirmten Kabel und es ist darauf zu achten, dass in unmittelbarer Nähe der Verkabelung keine Fremd- und Störfelder (z.B. Trafostationen, Funkeinrichtungen) liegen.

Wird innerhalb von Gebäuden die Führung der Teilnehmeranschlussleitung in Verrohrungen oder Kabelkanälen gewünscht, oder ist dies aus anderen nicht von Drei zu vertretenden Gründen erforderlich (z.B. Auflage des Verfügungsberechtigten), so sind die entsprechenden Verrohrungen oder Kabelkanäle bereitzustellen.

Kosten für allenfalls notwendige Schutzmaßnahmen gegen Fremdspannungsbeeinflussung sind vom Kunden zu tragen.

Nachträgliche Änderungen nach der Inbetriebnahme gelten als BCCR (Business Customer Change Request) und werden im Rahmen des BCCR Handling Prozesses verrechnet.

4.7.1 Anschlüsse.

Der Kunde schließt seine Geräte (Router, Switch, Host, etc.) über entsprechende Netzwerk Anschlusskabel an den definierten Ethernet LAN-Port (Netzabschlusspunkt) an (RJ45, LWL nach Vereinbarung). Damit ist der Zugang zum SD-WAN Service hergestellt.

4.8 Generelle Support Leistungen.

Die Supportleistungen von Drei beinhalten ausschließlich den Support von Geräten und Software, die von Drei zur Verfügung gestellt werden und erstrecken sich auf Hardware- und Konfigurations-Support (Restore of the last known good Configuration).

Wenn nicht anders vereinbart, umfasst die Serviceleistung die Behebung aller Störungen und Fehler, die im Verantwortungsbereich von Drei oder von ihr beauftragten Dritten (Partner) liegen. Die Behebung von Fehlern und Störungen, die von Drei oder ihren Partnern vertreten werden, ist entgeltfrei.

Fehler in den zentralen System-Komponenten (u.a. im Festnetz; Mobile Bereich bzw. der SD-WAN Cloud LMC) im Drei-Netzwerk werden von Drei bzw. Dritten (Partner) von Mo - So von 00.00 - 24.00 Uhr behoben.

Eine zu 100% Verfügbarkeit ist technisch generell nicht zu gewährleisten. Drei behält sich vor, aus Wartungs-, Sicherheits- oder Kapazitätsgründen die Dienstleistungen kurzzeitig auszusetzen oder zu beschränken.

4.9 Nicht im SLA gedeckte, kostenpflichtige Dienstleistungen.

Unter kostenpflichtige Service und Dienstleistungen fallen all jene Tätigkeiten, welche nicht im SLA oder im Lieferumfang des IML-Angebotes gedeckt sind. Diese werden gesondert anhand des entstandenen Aufwands als BCCR erfasst und über jenem im IML vereinbarten „Drei Managed Services“ Stundenpoolkontingent abgerechnet (siehe IML-Angebot).

Sollte kein Drei Managed Services Stundenpool vereinbart sein, oder das Stundenpoolkontingent überschritten / bereits aufgebraucht sein erfolgt die Abrechnung / die Stundenpool Aufstockung auf Rechnung gemäß „Allgemeine Stundensätze“ lt. IML-Angebot.

Darunter fallen u.a.:

- Mehraufwände und Standzeiten,
- Störungsbehebung mit Fremdverschulden,
- Kostenpflichtige Dienstleistungen,
- Arbeitsleistung außerhalb von Bürozeiten.

4.9.1 Mehraufwände und Standzeiten im Zuge der Vor-Ort Installation.

Darunter fallen Mehraufwände, mehrfache Vor-Ort Anfahrten wie Standzeiten im Zuge der Vor-Ort Installation, welche nicht auf Eigenverschulden von Drei zurückzuführen sind.

4.9.2 Störungsbehebung mit Fremdverschulden.

Wenn Drei zu einer Störungsbehebung gerufen wird und festgestellt, dass entweder keine Störung bei der Bereitstellung des Service vorliegt oder die Störung außerhalb des Verantwortungsbereiches von Drei liegt.

4.9.3 Kostenpflichtige Dienstleistungen.

Wenn nicht anders vereinbart fallen unter kostenpflichtige Dienstleistungen u.a.:

- Jegliche Vor-Ort Dienstleistungen, welche nicht im Zuge der SLA-Erfüllung oder einer Herstellung gedeckt sind.
- Jegliche Erweiterungen auf Ebene der Hard & Software, wie Lizenzen
- Abänderungen oder Anpassungen im Zuge der Herstell-; Rollout oder Betriebsphase, wenn diese außerhalb jenes im IML-Angebot definierten Lieferumfanges liegen
- Vor-Ort Messungen & Vor-Ort Begutachtungen
- Consulting & Beratungsleistungen
- Schulungen
- Konfigurationsänderungen und Integrationsdienstleistungen wie:
    - Firewall Definition & Einstellung, laufende Pflege der Firewall Settings
    - Migration von IT-Diensten wie Radius; Active Directory Server, sonstigen IT-Einbindungen und externe Applikationen
- „Root Cause“ bzw. Fehleranalysen, welche außerhalb der Drei Verantwortung liegen
- Spezielle Abnahme Verfahren, Redundanz Tests oder Ähnliches
- Leistungsoptimierung von Applikationen in der SD-WAN Lösung
- Zur Umsetzung nötige Mehraufwände im Zuge der Projektplanung (Projekt Management)

4.9.4 Arbeitsleistung außerhalb von Bürozeiten.

Generell gilt, das Arbeiten außerhalb jener in „Allgemeine Stundensätze“ (siehe IML-Angebot) liegenden Bürozeiten mit jenen darin definierten Aufschlägen abzugelten sind.

Dieser Aufschlag kommt aliquot auch für die Abrechnung über den Stundenpool im Zuge der BCCR-Umsetzung zum Tragen.

4.9.5 Professional bzw. Managed Service Erbringung.

In diesen Bereich fallen alle Leistungen der vorbeugenden Wartung, welche zusätzlich zum SLA als Managed Service angeboten werden können.

Dies beinhaltet u.a.:

- Support und Umsetzung bei Konfigurationsänderungen (über BCCR-Handling)
- Testen & Abnahme der neuen Konfigurationen / Änderungen
- Consulting & Planungsleistungen
- Lösungsdokumentation
- LifeCycle Pflege (Hardware und Software)
- Schulungen

4.10 Wartungsarbeiten.

4.10.1 Festnetz Access & Zentrale Komponenten.

- Wartungsfenster: 22.00 bis 06.00
- Vorankündigung: mind. 3 Werktage im Voraus

Wartungsarbeiten, die mit der von Drei zur Verfügung gestellten „Drei Festnetz Access“ bzw. die dahinterliegenden zentralen Komponenten (Festnetz Core Systeme bzw. SD-WAN LMC Cloud) Serviceunterbrechungen verbunden sind, werden in der Regel in vordefinierten Wartungsfenstern jeweils täglich in der Nacht zwischen 22.00 und 06.00 Uhr durchgeführt und mindestens 3 Werktage im Voraus telefonisch oder E-Mail angekündigt. Dabei werden Sie über Zeitpunkt und voraussichtliche Dauer des Serviceausfalls informiert. Das Ausmaß solcher serviceunterbrechenden Wartungsmaßnahmen beträgt maximal 12 Stunden pro Jahr.

Drei behält sich vor, die Zeiten der vordefinierten Wartungsfenster einseitig zu ändern und diese Änderung mindestens 2 Wochen vorher mitzuteilen.

Nach Absprache können auch andere Wartungszeiten vereinbart werden.

Für umfangreichere Arbeiten, die innerhalb der angeführten Wartungsfensters aus Zeitgründen nicht durchgeführt werden können bzw. für kurzfristig unaufschiebbare Arbeiten, die zur Abwendung von Betriebsausfällen (Hotfix; Workaround Lösungen) unbedingt notwendig sind, können von Drei Wartungszeiten auch außerhalb der Wartungsfenster beansprucht werden. Drei wird sich jedoch bemühen, solche Wartungsarbeiten nach den vorhandenen Möglichkeiten zu den mit Ihnen abgesprochenen Zeiten durchzuführen bzw. mindestens 3 Werktage im Voraus anzukündigen.

Serviceausfallszeiten, die durch vorangekündigte Wartungsarbeiten innerhalb der vordefinierten oder anderer vereinbarter Wartungsfenster begründet sind, zählen bei der Berechnung der Serviceverfügbarkeit nicht als nichtverfügbare Zeiten und gelten als suspendierte Zeiten.

4.10.2 Wartungsarbeiten SD-WAN Lösung.

- Wartungsfenster: Nach Vereinbarung
- Vorankündigung: mind. 3 Werktage im Voraus

Sollten spezifische Wartungsarbeiten der SD-WAN Lösung nötig sein, erfolgt dies in Abstimmung mit dem Kunden im Zuge der Managed Service Erbringung.

5. Service Level Agreement.

5.1 SLA-Varianten.

Die Umsetzung erfolgt anhand jener hier im SLA-Portfolio beschriebenen, mit den vereinbarten SLA-Varianten. Diese beziehen sich entweder auf den jeweiligen Standort, oder werden abhängig der eingesetzten Hardware-Komponenten im IML-Angebot vereinbart.

(z.B.: höhere SLA für „kritische“ Standorte oder im Einsatz befindliche, zentrale Komponenten)

Zur Auswahl stehen dabei derzeit folgende SLA-Varianten:

SLA-Standard: Drei Remote Support mit SLA-Garantien, welche die „Pick-up & Return“ Option zu Austausch von Defektgeräten inkludiert

SLA-Premium: Drei Support inklusive Field Service, mit Auswahl von unterschiedlichen SLA-Garantien mit vor Ort Support, falls sich über den Remote Support der Fehler nicht beheben lässt.

SD-WAN: SLA Portfolio Übersicht			Service Level Parameter & Targets				Involvierte Support Levels				
SLA Varianten		**SLA Service Target**	**Support Verfügbarkeit**	**Max. Antwortzeit**	**max. Vor Ort Eintreffzeit OSrT**	**Repair & Return Zeit**	Hersteller Garantie	1st Level Support	2nd Level Support	3rd Level Support	FS (Field Services)
SLA Standard	+ Incident Management + PickUP & Return + garantierte Ersatzgerätelieferung (N2BD)	8x5xN2BD	Mo-Fr: 09:00 bis 17:00	6h	X	Versand: N2BD	√	√	√	√	X
SLA Premium OSrT	+ Incident Management + FieldService + max. VorOrt Eintreffzeit (OSrT)	8x5xNBD	Mo-Fr: 09:00 bis 17:00	4h	NBD	√ Im FS Umfang	√	√	√	√	√
		8x5x4		4h	4h	√ Im FS Umfang	√	√	√	√	√
		10x6x4	Mo-Sa: 08:00 bis 18:00	2h	4h	√ Im FS Umfang	√	√	√	√	√
		24x7x4	24/7/365	2h	4h	√ Im FS Umfang	√	√	√	√	√

Legende: Abkürzungen zum Leistungsumfang
d (days) = Support Tage pro Woche
h = (hours) = Stundenanzahl
NBD = (Next Business Day) = Am nächsten Werktag
N2BD = Next two (2) Business Days = Am übernächsten Werktag
OSrT (Onsite Reponse Time) = maximale Vor Ort Eintreffzeit

Abbildung 16: Generelle Übersicht - Drei SD-WAN.

5.2 Kurzbeschreibung “PickUP & Return” Service.

Die Pick Up & Return Variante inkludiert eine Abholung des Defektgerätes über Drei. So handhabt der Kunde die nötige Demontage, und die Montage und Inbetriebnahme des Ersatzgerätes weiterhin selbst.

Die Abholung des Defektgerätes wie der Rückversand zum Standort erfolgt über Hutchison Drei Austria GmbH (oder dessen Service Partner) auf dessen Kosten, innerhalb einer garantierten Rückversandzeit.

- die kostenfreie Rückholung des Ersatzgerätes am Standort
- einem garantierten Ersatzgeräte Versand innerhalb von 2 Werktagen (N2BD) nach Fehleranalyse und Beauftragung des Ersatzgerätes über Drei

5.3 Kurzbeschreibung “Field Service (FS)”.

Das hier inkludierte Field Service (FS) beinhaltet die Ersatzteillieferung zum Zeitpunkt des Vor-Ort Einsatzes, die Demontage & Montage wie die erneute Inbetriebnahme des Ersatzgerätes am Standort.

Dies inkludiert auch das dazu nötige Repair & Return Service und die Logistik des Defektgerätes zum Hersteller. In der gewählten SLA-Variante sind auch garantierte Vor-Ort Eintreffzeiten inkludiert.

5.4 SLA-Standard N2BD

Der SLA-Standard umfasst die Dienstleistung der Fehleranalyse und Behebung über den Remote Support von Drei, inkludiert eine garantierte Reaktionszeit nach der Störungsmeldung durch den Kunden. Im Defektfall der Hardware wird ein Ersatzgerät geliefert, und das Defektgerät über einen von Drei beauftragten Lieferdienst abgeholt.

- 24/7 Störungsannahme: per E-Mail an unsere Business Support

- Support Zeiten: Werktags Mo – Fr. von 09:00 bis 17:00
- Garantierte Reaktionszeiten: Innerhalb von 6h nach Störungsmeldung während Support Zeiten
- Inkludiert das:
    - Incident Management aller Störungsmeldungen
    - Remote Support zur Fehlerdiagnose & Störungsbehebung
- Ersatzgeräteversand: innerhalb von 2 Werktagen (N2BD)
- Managed Service Dienstleistungen mit Abrechnung nach Aufwand über Stundenpool
    - BCCR-Handling & Umsetzung zu Bürozeiten
    - Planung, Handhabung und Umsetzung
    - Konfigurationsänderungen
    - Beratung & Consulting

Nicht inkludiert: Field Service typische Dienstleistungen wie Demontage und Montage; Test-, Konfiguration wie Inbetriebnahme des Ersatzgerätes.

5.5 SLA-Premium OsRT: Incident Management & Field Service Support (FS).

Unser Premium SLA erweitert den SLA Standard Umfang um den Vor-Ort -Support im Defektfall der Hardware, welche im Störfall vom Kunden abgerufen werden kann.

Drei koordiniert das Field Service Team, wenn ein Vor-Ort Einsatz zur Fehlerbehebung im Defektfall der Hardware durch den Support von Drei als nötig erachtet wurde.

Im SLA Premium Umfang kann zwischen unterschiedlichen Support Zeit & SLA Garantien gewählt werden:

- 8x5xNBD
- 8x5x4
- 10x6x4
- 24x7x4

In allen SLA Premium Varianten sind folgende Leistungen gleich und inkludiert:

- 24/7 Störungsannahme: per E-Mail an unsere Business Support
- Support Zeiten: anhängig zur gewählten SLA-Variante (Details siehe unten)
- Field Service (FS) Zeiten: anhängig zur gewählten SLA-Variante (Details siehe unten)
- Incident Management aller Störungsmeldungen
- Remote Support zur Fehlerdiagnose & Störungsbehebung
- Managed Service Dienstleistungen mit Abrechnung nach Aufwand über Stundenpool
    - BCCR-Handling & Umsetzung zu Bürozeiten
    - Planung, Handhabung und Umsetzung
    - Konfigurationsänderungen
    - Beratung & Consulting
- FS-Vor-Ort Support: Vor Ort Support & HW Austausch direkt am Standort
- Repair & Return Service: Ersatzteil Handhabung über Field Service & Drei Logistik

5.5.1 SLA Premium OsRT: Incident Management & Field Service (8x5xNBD)

Diese SLA Premium Variante inkludiert folgende SLA Service Targets

- Support Zeiten: Werktags Mo – Fr. von 09:00 bis 17:00
- Field Service (FS) Zeiten: Werktags Mo – Fr. von 09:00 bis 17:00
- Garantierte OsRT: Innerhalb des nächsten Werktages nach Aktivierung (NBD)
- Maximale Reaktionszeit: 4h

5.5.2 SLA Premium OsRT: Incident Management & Field Service (8x5x4)

Diese SLA Premium Variante inkludiert folgende SLA Service Targets

- Support Zeiten: Werktags Mo – Fr. von 09:00 bis 17:00
- Field Service (FS) Zeiten: Werktags Mo – Fr. von 09:00 bis 17:00

- Garantierte OsRT: 4h
- Maximale Reaktionszeit: 4h

5.5.3 SLA Premium OsRT: Incident Management & Field Service (10x6x4)

Diese SLA Premium Variante inkludiert folgende SLA Service Targets

- Erweiterte Support Zeiten: Werktags Mo – Sa. von 08:00 bis 18:00
- Field Service (FS) Zeiten: Werktags Mo – Sa. von 08:00 bis 18:00
- Garantierte OsRT: 4h nach Aktivierung
- Maximale Reaktionszeit: 2h

5.5.4 SLA Premium OsRT: Incident Management & Field Service (24x7x4)

Diese SLA Premium Variante inkludiert folgende SLA Service Targets

- Erweiterte Support Zeiten: Werktags Mo – So. von 00:00 bis 24:00
- Field Service (FS) Zeiten: Werktags Mo – So. von 00:00 bis 24:00
- Garantierte OsRT: 4h nach Aktivierung
- Maximale Reaktionszeit: 2h

6. Begrifflichkeiten und Kurzbeschreibung der Support Handhabung von Drei.

1st Level Support	Der 1st Level Support erfolgt durch den Service Desk von Drei: Es werden alle eingehenden Anfragen und Störungsmeldungen entgegengenommen, registriert und eine Erstanalyse durchgeführt. Abhängig davon wird die Anfrage entweder direkt an die zuständige Fachabteilung weitergeleitet, oder im Falle eines technischen Problems direkt vom Service Desk bearbeitet. Aufgrund des Fehlerreports wird mit der Wiederherstellung des Drei Service begonnen und versucht, es ehestmöglich wiederherzustellen. Ist die Fehlerursache zu diesem Zeitpunkt eindeutig erkennbar wird eine Entstörung in die Wege geleitet. Kann der Customer Incident nicht direkt im 1st Level Support gelöst werden, wird dieser an den 2nd Level Support übergeben.
2nd Level Support	Aufgrund der Informationen des 1st Level Support im Customer Incident wird mit der detaillierten Fehleranalyse und dessen Behebung begonnen. Bei Bedarf wird zur Unterstützung der 3rd Level Support einbezogen. Ist keine ursächliche Lösung des Incident möglich, übergibt bei Bedarf der 2nd Level diesen zur weiteren Bearbeitung an das Problem Management. Lieferanten können bei Bedarf auch durch den 2nd Level beauftragt werden.
3rd Level Support	Der 3rd Level Support erfolgt durch die System Engineers und der Netzwerkplanung, welche auch auf Spezialisten bei den Lieferanten, Service Partnern und Herstellerfirmen zugreifen kann.
Business Customer Change Request (BCCR)	Ist eine vom Kunden gewünschte technische Änderung einer bestehenden Konfiguration oder eines Service. Abhängig vom Aufwand kann ein Change Request kostenpflichtig sein. Bei standardisierten Change Requests erfolgt die Abrechnung nach Aufwand entsprechend den gültigen Drei Stundensätzen oder dem mit dem Kunden vereinbarten Stundenpool. Bei komplexen BCCR-Anfragen erhält der Kunde vor Implementierung des CR# eine Abschätzung, um die Umsetzung des BCCRs zu bestellen.
Hardware Pick up & Return Service	Bezeichnet eine Reparaturdienstleistung. Dabei wird das defekte IT/TK Equipment zur Reparatur geschickt und erhält ein funktionales Equipment retour.
Incident	Incident: Ist die ungeplante Unterbrechung oder Einschränkung des Service.
Incident Lösung	Drei schließt nach der erfolgreichen Wiederherstellung des Service das Incident Ticket. Der Zeitpunkt der Schließung des Incident Tickets gilt als Störungsende.
Störungsannahme	Jener Zeitraum, in der eine Störung per E-Mail automatisiert entgegengenommen und registriert wird.
Support Zeiten	Jene Zeiträume, in der unsere Support Abteilungen (1st und 2nd Level Support) telefonisch oder per E-Mail zur Verfügung stehen. Innerhalb dieser Zeit werden alle Fälle aktiv bearbeitet, und die Wiederherstellung Ihre Services umgesetzt.
Remote Support (Fernzugriff)	Unter dem Remote Support versteht man den räumlich getrennten Zugriff auf IT/TK-Systeme zur Fehleranalyse sowie zu Wartungs- und Reparaturzwecken beim Kunden
Reaktionszeit	Ist der Zeitraum, zwischen der Incident Eröffnung und dem Beginn der ersten Fehleranalyse bzw. Rückmeldung an den Kunden.
Field Service (FS) (Vor-Ort-Support)	Ein Techniker unterstützt vor Ort (z.B.: Infrastruktur- oder Standorte) in der Fehleranalyse sowie bei Wartungs- und Reparaturmaßnahmen, sofern diese nicht über einen Fernzugriff möglich sind.

Field Service Zeiten	Jene Zeiträume, in der eine Wiederherstellung Ihre Services im Bedarfsfall Vor-Ort erfolgt und innerhalb dessen wir Tickets im Field Service Bereich aktiv bearbeitet werden. Field Services wird von unserem 2nd Level Support dann involviert, sollte ein Remote Support keine Wiederherstellung Ihre Services ermöglichen (z.B.: Austausch einer defekten CPE-Hardware)
Vor-Ort-Eintreffzeit	Ist der Zeitraum, zwischen der Incident Eröffnung unseres 2nd Level Supports bei unserem Field Service und dem Eintreffen des Field Service Technikers am Standort.