Whitepaper

SD-WAN: Software Defined Networking

Sie möchten Standorte wie zum Beispiel Filialen, Anlagen, Fahrzeuge, Sensoren und Geräte sicher, leistungsstark und womöglich länderübergreifend vernetzen, überwachen und steuern – unabhängig von Lage und Technologie. Ob eine oder tausende Infrastrukturen, das Netz soll einfach und flexibel betreibbar sein. Das birgt verschiedene Herausforderungen. Die grösste liegt in der Konfiguration einer grossen Anzahl von Verbindungen und Geräten. Bisher musste standardmässig jedes Gerät einzeln konfiguriert werden. Sollte also eine kleine Anpassung vorgenommen werden, musste dies für jedes Gerät einzeln erfolgen, was fehleranfällig ist und einen grossen Zeit- und Kostenaufwand mit sich bringt. Die Skalierbarkeit solcher Lösungen war daher in der Vergangenheit eher tief. Zudem sorgen schwankende Netzwerkqualitäten für instabile Konnektivität und Verbindungen über öffentliche Netze gehen mit Sicherheitsrisiken einher.

SD-WAN

Die Lösung hierfür heisst SD-WAN, also Software Defined Networking in einem Wide Area Network, einem Weitverkehrsnetzwerk. Mit unserer softwarebasierten Lösung können externe Standorte und Geräte sehr einfach und sicher an das Firmennetzwerk angebunden werden.

Vorteile einer SD-WAN-Lösung

Eine SD-WAN-Lösung eignet sich für verschiedene Szenarien innerhalb eines Unternehmens. Besonders vorteilhaft ist sie für die Vernetzung von:

- Mehreren Firmenstandorten oder -filialen
- Abgesetzten Anlagen, Maschinen, Kraftwerke, Solaranlagen, Windrädern, Sensoren usw.
- Mobilen Fahrzeugen (Lastwagen, öffentliche Verkehrsmittel, Baumaschinen usw.)
- Temporären Standorten (Verkehrsmittel, Verkaufswagen, Open Airs, Pop-Up-Stores etc.)
- Anbindung mehrerer Cloud-Anbieter
- Internet-of-Things (IoT)-Geräten

Anschluss unterschiedlicher Umgebungen und Anlagen

Einer der grössten Vorteile der SD-WAN-Lösung ist demnach die flexible Integration aller internen und externen Standorte in eine private und sichere Netzwerkinfrastruktur. Dabei können diese abgesetzten Netzwerke sowohl länderübergreifend als auch über weite Distanzen so angebunden werden, dass diese stets erreichbar und damit überwach- und steuerbar sind.

Zentrale Verwaltung und Automatisierung

Die Erschliessung vieler Remote-Standorte bedingt eine automatisierte und zentrale Verwaltung und Steuerung des Netzwerks. So können jederzeit Änderungen oder zusätzliche Umgebungen mühelos und unabhängig von ihrer Position oder Anbindungsart durchgeführt werden. Die Netzwerkerweiterung erfolgt dabei ohne komplexe manuelle Konfigurationen und ist dementsprechend hochskalierbar. Durch eine konsequente Automatisierung können Zeit- und Kostenaufwand eingespart und Fehlerquellen minimiert werden.

Zuverlässige Konnektivität

Indem wir mehrere parallele Verbindungen über Netzwerkanbieter herstellen, kann die Leistung und Zuverlässigkeit der Konnektivität gesteigert werden. Redundante Verbindungen optimieren den Datenverkehr und stellen sicher, dass ein stabiles Netzwerk auch in unbeständigen Kontexten gegeben ist.

Sicherheit

Die Verbindungen werden nach den höchsten Sicherheitsstandards authentifiziert und verschlüsselt. Dabei werden zentrale Richtlinien für den Datenschutz und die Compliance jederzeit eingehalten. Dennoch unterstützt die Lösung auch individuelle Anforderungen und funktioniert über die unterschiedlichsten Netzwerkressourcen (Mobilfunknetze, Mietverbindungen, Internet usw.).

Die SD-WAN-Lösung von onway

Folgende Alleinstellungsmerkmale zeichnen die SD-WAN-Lösung von onway aus:

- Zero-Touch Deployment ***– Auspacken und Einstecken!***

  Die Geräte und Standorte sind ohne manuelle Konfiguration sofort einsatzbereit. Die Router verbinden sich automatisch mit dem zentralen Management-System, sobald sie an ein beliebiges Netzwerk angeschlossen worden sind und erhalten alle erforderlichen Einstellungen und Updates automatisch. Dadurch wird die Installation auch grosser Netzwerke stark vereinfacht und beschleunigt.

- Zentralisiertes Management ***– Verwaltung leicht gemacht!***

  Unsere zentralisierte Router-Management-Technologie ermöglicht eine effiziente Konfigurationsverwaltung inkl. Versionierung auf der zentralen onway-Cloud. Eine automatisierte Testumgebung validiert sämtliche Änderungen und gewährleistet dadurch einen reibungslosen Rollout. Eine intuitive Benutzeroberfläche vereinfacht das Management zusätzlich für die Administrator:innen.

- Security by Design ***– Von Grund auf sicher!***

  Wichtige Sicherheitsprinzipien sind bereits in das Design der Gesamtlösung integriert, wodurch nachträgliche Massnahmen wegfallen. So werden standardmässig alle eingehenden Netzwerkverbindungen blockiert, ausser sie werden ausdrücklich zugelassen. Die Verwendung von Zertifikaten ist obligatorisch, sodass nur authentifizierte Geräte und Benutzer:innen und Geräte Zugriff erhalten. Regelmässige Updates und Security Patches bieten zusätzlichen Schutz vor Bedrohungen.

- Failsafe-Updates von Konfigurationen und Software ***– Updates ohne Ausfallrisiko!***

  Die Aktualisierung von Konfigurationseinstellungen und Softwareversionen wird durch verschiedene Mechanismen geschützt. Nach einem Update prüfen die Router die Verbindung zum zentralen Management. Bei Fehlkonfigurationen und dadurch entstandene Unterbrechungen im Netzwerk werden die Router automatisch auf den letzten funktionierenden Zustand zurückgesetzt. Mittels einem Dual-Boot-System werden neue Images auf die gerade nicht aktive Partition geladen und dort zu starten versucht. Falls dies nicht klappt, wird automatisch auf die alte und funktionierende Partition zurück gewechselt. So wird sichergestellt, dass ein Update immer einwandfrei oder gar nicht durchgeführt wird. Der Zustand des Gerätes wird zudem durch einfach erkennbare Lauf- und Blinklichter am Gerät signalisiert. Damit kann man Fehler auch vor Ort anhand der angezeigten LED erkennen.
  Die Hardware ist «by design» auf raue Umgebungen ausgelegt und zertifiziert. Daher sind Hardwarefehler selten und die Software verfügt über umfangreiche Kontrollmechanismen. All das minimiert das Risiko von Ausfallzeiten oder Betriebsstörungen und erhöht die Zuverlässigkeit des Netzwerks.

- Aktive Steuerung der Übertragungsqualität (Dynamisches QoS)
  – Optimierung der Übertragungsqualität!

  Die zugrundeliegenden Netzwerkverbindungen sind von schwankender Qualität. Der Nutzverkehr muss daher aktiv gesteuert werden, damit kritische Anwendungen jederzeit kommunizieren können. Unter dem Begriff «dynamische Quality-of-Service (QoS)» wird eine Vielzahl von Mechanismen zur kontinuierlichen Bandbreiten- und Latenzmessung sowie zur Priorisierung und Glättung (Shaping) von Nutzerverkehr verstanden. Dank diesen Mechanismen wird kritischen Anwendungen stets die bestmögliche Qualität und Zuverlässigkeit gewährleistet.

- Dynamisches Reagieren auf Link-Changes (Mobilität, Unterbrüche usw.) in Echtzeit ***– Echtzeit-Reaktion auf Link-Changes!***

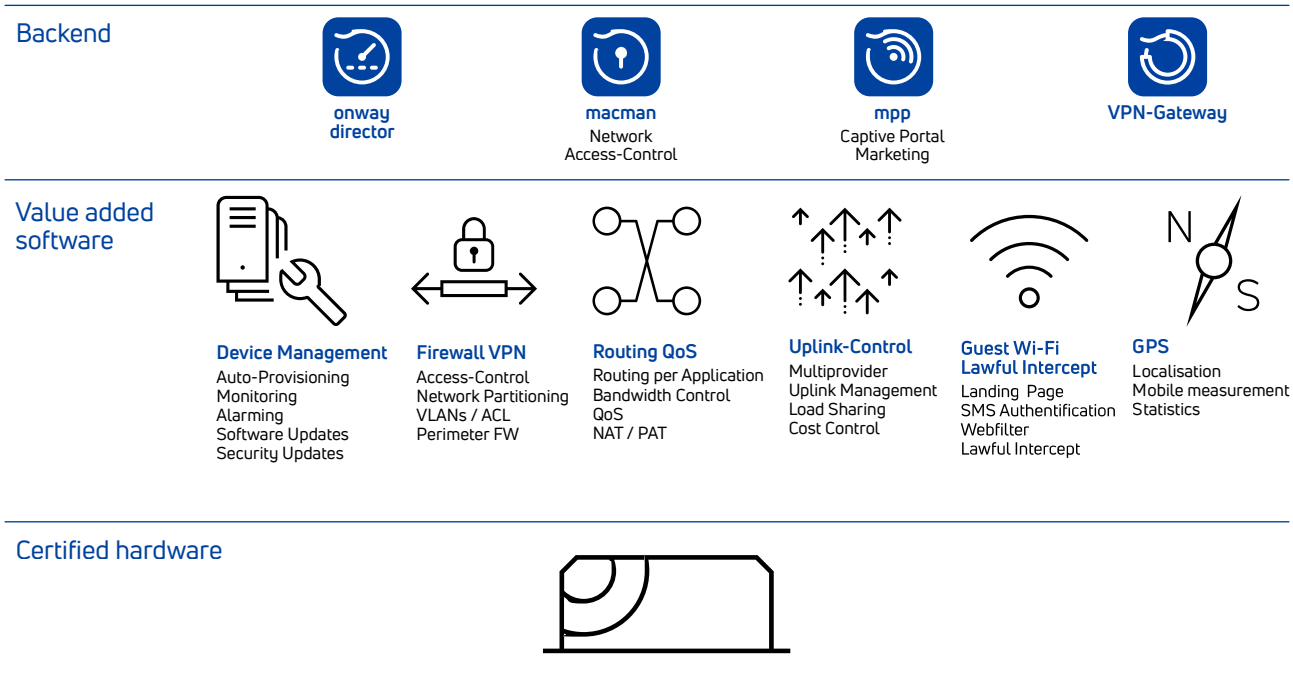
  Das System erkennt automatisch, wann eine Verbindung unterbrochen wird oder sich ändert und ergreift Massnahmen, um den Datenverkehr auf alternative Pfade umzuleiten oder die Verbindung wiederherzustellen. Dies geschieht anhand der transparenten Aggregation mehrerer Uplinks (Ethernet, Mobilfunk, WLAN etc.) und dynamischen Routing-Protokollen. Dadurch wird die Ausfallsicherheit verbessert und die Kontinuität der Netzwerkkommunikation auch bei Verbindungsunterbrüchen gewährleistet.

- Horizontale Skalierung mehrerer Router ***– Optimale Leistung durch parallele Router-Nutzung!***

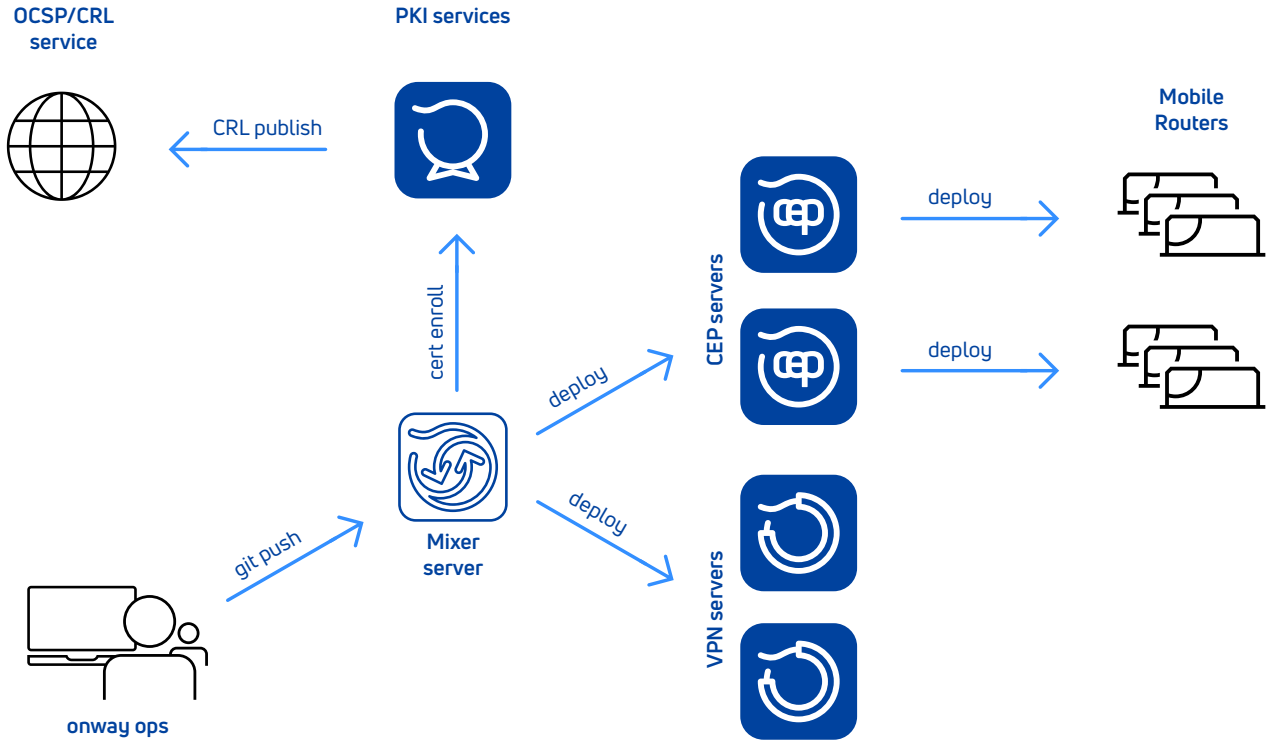
  Es können mehrere Router parallel betrieben und dadurch die Überlastung einzelner Router vermieden werden. Dies ermöglicht eine nahtlose Anpassung an steigende Anforderungen, ohne dass es zu Engpässen oder Leistungseinbussen kommt.

- Kostengünstige Hardware ***– Hochwertige Hardware, niedrige Kosten!***

  Unsere Hardware ist in verschiedenen Konfigurationen erhältlich; von klein bis gross. Damit bieten wir Lösungen für jeden Zweck zu attraktiven Preisen.



Das folgende Bild zeigt die Architektur der onway SD-WAN-Lösung. Nachfolgend beschreiben wir die wichtigsten Funktionen der verschiedenen Komponenten.



Mixer

Der Mixer ist die zentrale Oberfläche zum Erstellen und Ändern von Konfigurationen für mobile Router/Server und VPN-Gateways. Die Konfiguration basiert auf dem IaC-Ansatz (Infratructure as Code), das heisst die Router-Konfiguration wird in hardware-unabhängiger YAML-Notation geschrieben. Diese wird auf dem Mixer validiert und auf die Zielhardware angepasst. Der Mixer interagiert mit der PKI, um Zertifikate zu registrieren, die für die IPsec-Authentifizierung erforderlich sind. Nachdem die vollständige Konfiguration generiert wurde, überträgt der Mixer die Konfiguration an den CEP oder direkt an die VPN-Gateways.

GEP (Global Entry Point)

Der Hauptzweck des GEP besteht in der Zeitsynchronisierung mit den onway-Routern, um zertifikatsbasierte Authentifizierung und ZeroTouch-Bereitstellung zu ermöglichen. Zudem werden Router über den GEP den entsprechenden Kundeninstallationen zugeordnet. Dazu leitet der GEP den Router an den entsprechenden Customer Entry Point (CEP) weiter. Der GEP wird von onway gehostet und verwaltet.

CEP (Customer Entry Point)

Der CEP ist für die Bereitstellung der vom Mixer empfangenen Konfiguration auf onway-Routern und die Aktualisierung von Router-Images verantwortlich. Zudem ermöglicht der CEP einen jederzeitigen Fernzugriff auf *Standorte* über ein gesichertes Protokoll der Managementebene namens BRUSH. CEPs werden in der Regel von onway bereitgestellt und verwaltet und daher in der onway-Cloud gehostet, können aber auch beim Kunden platziert werden.

VPN-Gateway / Konzentrator

Das VPN-Gateway ermöglicht eine verschlüsselte Kommunikation zwischen den zentralen Standorten und den onway-Routern. VPN-Gateways befinden sich je nach Anwendungsfall bei onway und/oder bei den Kunden, ihren Partnern oder Zulieferern.

onway-Router

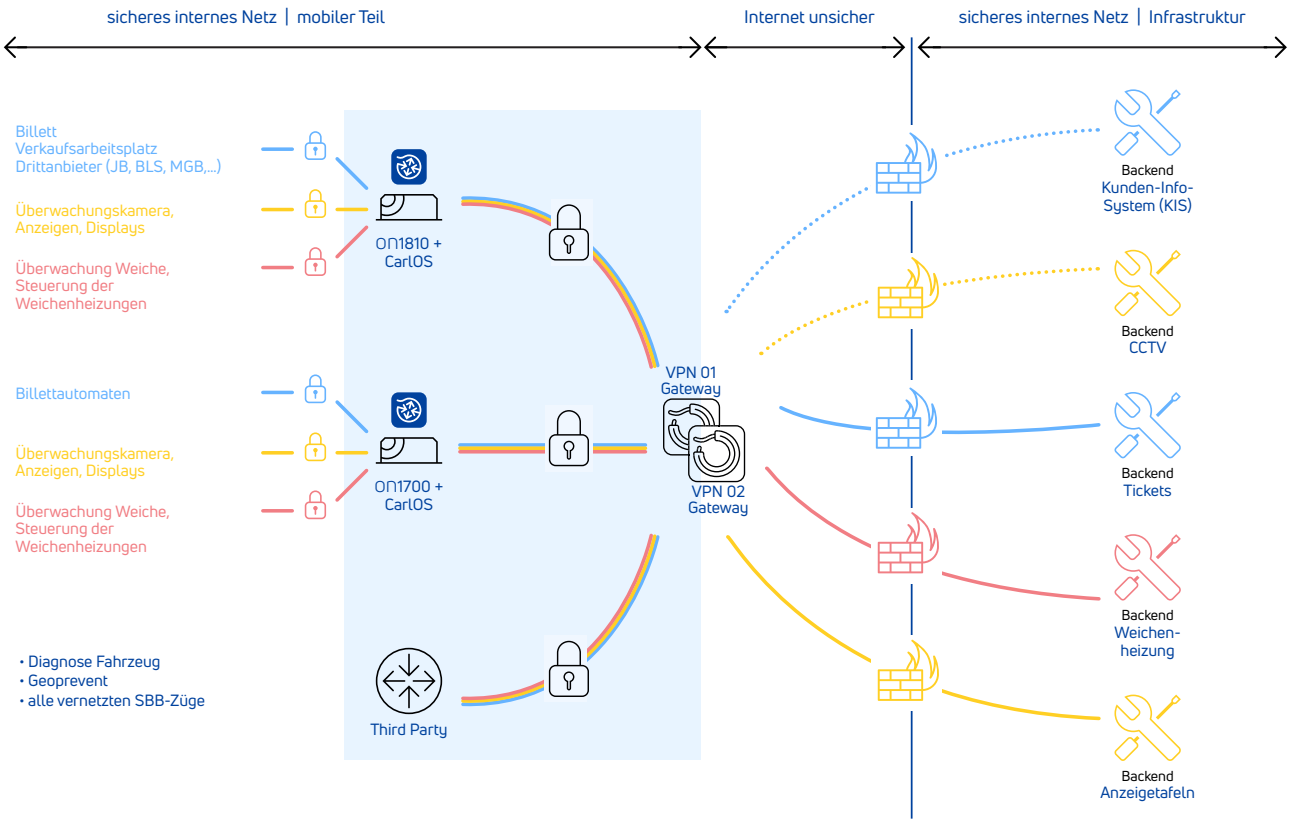
Mobile onway-Router können auch an ungeschützten Standorten eingesetzt werden. Sie basieren standardmässig auf einer Zero-Trust-Architektur und schützen das private Netz vor unerlaubten Zugriffen. Sie ermöglichen die Kommunikation gleichzeitig über mehrere Uplinks.
Dank konstanten Signal-, Verlust- und Latenzmessungen passen sie sich dynamisch an schnell wechselnde Umstände an.

Unsere Lösung am Beispiel der SBB

Im Rahmen einer GATT/WTO-Ausschreibung für bis zu 10 000 Router hat sich die SBB im Jahr 2022 für unsere SD-WAN-Gesamtlösung entschieden, bestehend aus mobilen Routern, zentralen VPN-Konzentratoren sowie unserem Management-System. Unsere Router dienen dabei als abgesicherte Netzzugangspunkte für die zunehmend digitalisierte SBB-Infrastruktur über verschiedene Technologien (Mobilfunk, WLAN, WAN). Dabei müssen unterschiedliche interne Netze der SBB über den gleichen VPN-Tunnel mit dem zentralen Netzwerk verbunden und mittels Multi-VRF-Separierung sicher getrennt werden. Die onway übernimmt die Wartung, den Betrieb und den Support der gesamten Infrastruktur für vorerst neun Jahre mit Option auf Verlängerung.

Projekt-Anforderungen

SBB benötigt verschiedene Services für ihre eigenständigen Abteilungen. Digitale Services wurden zum Teil auch durch Partnerfirmen und deren Produkte realisiert, wobei die Hoheit stets bei der SBB lag. Unsere SD-WAN-Lösung bindet alle Anwendungen und Partner in die zentrale und automatisierte Verwaltung ein, wie die untenstehende Grafik zeigt.



- ## Videoüberwachung

  Zur Videoüberwachung nutzt die SBB IP-fähige Kameras. Mit unserer SD-WAN-Lösung können wir vom Router aus gleichzeitig die Konnektivität wie auch die Stromversorgung für diese Kameras bereitstellen. Dadurch entsteht eine kompakte Lösung für die Überwachung der SBB-Anlagen. Durch den Einsatz von Dualmodems konnten wir zudem die Kapazität und Bandbreite erhöhen, um auch hochauflösende Videos in Echtzeit zu übertragen.

- ## Billettautomaten

  Um an den Billettautomaten der SBB die Fahrkarten per Kreditkarte zu begleichen, Geschenkgutscheine zu beziehen oder Prepaid-Handys aufzuladen, braucht es die entsprechende Daten- respektive Kommunikationsübermittlung. Diese wird nun von unseren Routern übernommen.

- ## Weichenheizungen

  Die zahlreichen Weichen entlang der Bahnstrecken der SBB stellen besonders empfindliche und neuralgische Punkte im Gleisverlauf dar. Unter dem Einfluss von Feuchtigkeit und frostigen Temperaturen besteht die Gefahr, dass flexible Schienenteile einfrieren. Daher müssen die Weichenheizungen bedarfsweise aktiviert oder deaktiviert werden können. Unsere Router kommen hier zum Einsatz, um die automatische Steuerung zu gewährleisten.

- ## Digitale Anzeigetafeln

  Überkopf-Anzeigetafeln sind an Bahnhöfen unverzichtbar für Reisende, um grundlegende Informationen wie Abfahrtszeiten, Verspätungen und Fahrplanänderungen zu erhalten. Unsere Lösung gewährleistet an kleineren und grösseren Bahnhöfen eine reibungslose Bereitstellung dieser Updates in Echtzeit, damit Passagier:innen stets informiert sind.

- ## Benachrichtigung für anstehende Wartungsarbeiten

  Die SBB betreibt Diagnosefahrzeuge, welche die Schienen analysieren und allfällig nötige Wartungsarbeiten automatisch detektieren. Die dabei entstehende grosse Datenmenge wird dank den onway-Routern schnell und sicher auf die Landseite übertragen.

- ## Nahtlose Zug-Land-Vernetzung

  Die ungefähr tausend Züge der SBB, die Zug-Land-Netzwerke nutzen, werden über unsere VPN-Gateways mit den zentralen Systemen auf der Landseite verbunden.

- ## Verkaufsplätze von Drittanbietern

  Damit Verkaufsarbeitsplätze bei anderen Anbietern auf das SBB-Ticketing-System zugreifen können, setzt SBB auf die onway-Router, die diesen gesicherten Zugang ermöglichen. Die Kommunikation erfolgt entweder via Mobilfunk oder über einen kabelgebundenen Internetschluss.