Whitepaper

SD-WAN: Software Defined Networking

You want to network, monitor and control locations (such as branches), plants, vehicles, sensors and devices securely, efficiently and possibly across countries – regardless of location and technology. Whether one or thousands of infrastructures, the network should be easy and flexible to operate. This poses various challenges. The biggest one is the configuration of a large number of connections and devices. Previously, each device had to be configured individually by default. So, if a small adjustment was to be made, this had to be done individually for each device, which is error-prone and involves a great deal of time and money. The scalability of such solutions has therefore been rather low in the past. In addition, fluctuating network qualities cause unstable connectivity and connections via public networks are accompanied by security risks.

SD-WAN

The solution is called SD-WAN, i.e. Software Defined Networking in a Wide Area Network. With our software-based solution, external locations and devices can be connected to the company network very easily and securely.

Benefits of an SD-WAN Solution

An SD-WAN solution is suitable for various scenarios within an organization.
It is particularly advantageous for the networking of:

- Multiple company locations or branches
- Remote systems, machines, power plants, solar systems, wind turbines, sensors, etc.
- Mobile vehicles (trucks, public transport, construction machinery, etc.)
- Temporary locations (transport, sales vans, open airs, pop-up stores, etc.)
- Connecting multiple cloud providers
- Internet-of-Things (IoT) devices

Connection of different environments and systems

One of the biggest advantages of the SD-WAN solution is the flexible integration of all internal and external locations into a private and secure network infrastructure. These remote networks can be connected both across countries and over long distances in such a way that they are always accessible and can therefore be monitored and controlled.

Centralized management and automation

The development of many remote locations requires automated and central management and control of the network. This means that changes or additional environments can be carried out effortlessly at any time, regardless of their position or type of connection. The network expansion takes place without complex manual configurations and is accordingly highly scalable. Consistent automation can save time and costs and minimise sources of error.

Reliable connectivity

By establishing multiple parallel connections through network providers, the performance and reliability of connectivity can be increased. Redundant connections optimize traffic and ensure a stable network even in volatile contexts.

Security

The connections are authenticated and encrypted according to the highest security standards. Central guidelines for data protection and compliance are always adhered to. However, the solution also supports individual requirements and works over a wide variety of network resources (mobile networks, rental connections, Internet, etc.).

The onway SD-WAN Solution

The following unique selling points distinguish onway's SD-WAN solution:

- Zero-Touch Deployment ***– unpack and plug it in!***

  The devices and locations are ready for immediate use without manual configuration. The routers automatically connect to the central management system as soon as they have been connected to any network and receive all necessary settings and updates automatically. This greatly simplifies and accelerates the installation of even large networks.

- Centralized management ***– administration made easy!***

  Our centralized router management technology enables efficient configuration management including versioning on the central onway cloud. An automated test environment validates all changes and thus ensures a smooth rollout. An intuitive user interface further simplifies management for administrators.

- Security by Design ***– secure from the ground up!***

  Important security principles are already integrated into the design of the overall solution, eliminating the need for subsequent measures. By default, all incoming network connections are blocked, unless they are explicitly allowed. The use of certificates is mandatory, so only authenticated devices and users have access. In addition, regular updates and security patches provide additional protection against threats.

- Failsafe updates of configurations and software ***– updates without the risk of failure!***

  Updating configuration settings and software versions is protected by various mechanisms.
  After an update, the routers check the connection to the central management. In the event of misconfigurations and resulting interruptions in the network, the routers are automatically reset to the last working state. Using a dual-boot system, new images are loaded onto the currently inactive partition and attempted to start there. If this does not work, it will automatically switch back to the old and working partition. This ensures that an update is always carried out flawlessly or not at all.
  The status of the device is also signaled by easily recognizable running and flashing lights on the device. This means that faults can also be detected on site by the LED displayed.
  The hardware is designed and certified "by design" for harsh environments. Therefore, hardware failures are rare and the software has extensive control mechanisms. All of this minimizes the risk of downtime or operational disruptions and increases the reliability of the network.

- Active control of transmission quality (Dynamic QoS)
  – optimization of transmission quality!

  The underlying network connections are of fluctuating quality. Commercial traffic must therefore be actively controlled so that critical applications can communicate at all times. The term "dynamic

quality-of-service (QoS)" refers to a variety of mechanisms for continuous bandwidth and latency measurement as well as for prioritizing and smoothing (shaping) user traffic. Thanks to these mechanisms, critical applications are always guaranteed the best possible quality and reliability.

- Dynamically react to link changes (mobility, interruptions, etc.) in real time
  – real-time reaction to link changes!

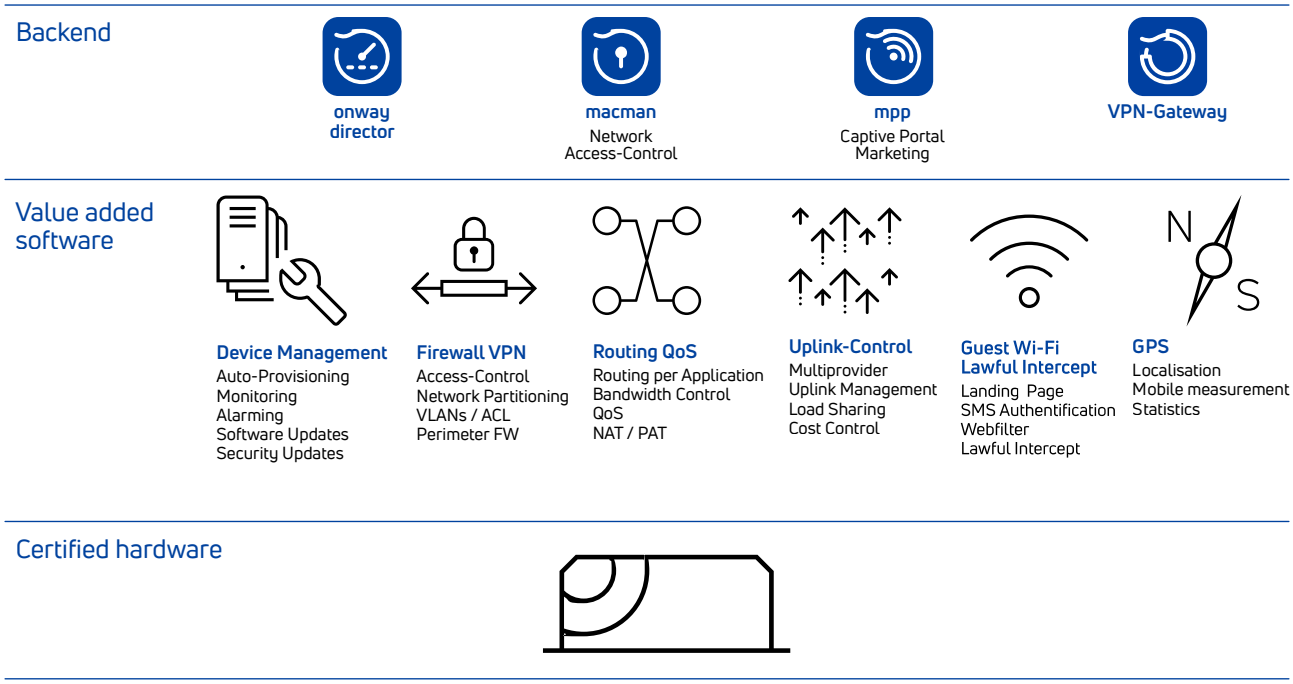
  The system automatically detects when a connection is interrupted or changes and takes action to redirect traffic to alternative paths or re-establish the connection. This is done using the transparent aggregation of multiple uplinks (Ethernet, cellular, Wi-Fi, etc.) and dynamic routing protocols. This improves reliability and ensures continuity of network communication even in the event of connection interruptions.

- Horizontal scaling of multiple routers
  – optimal performance through parallel router use!

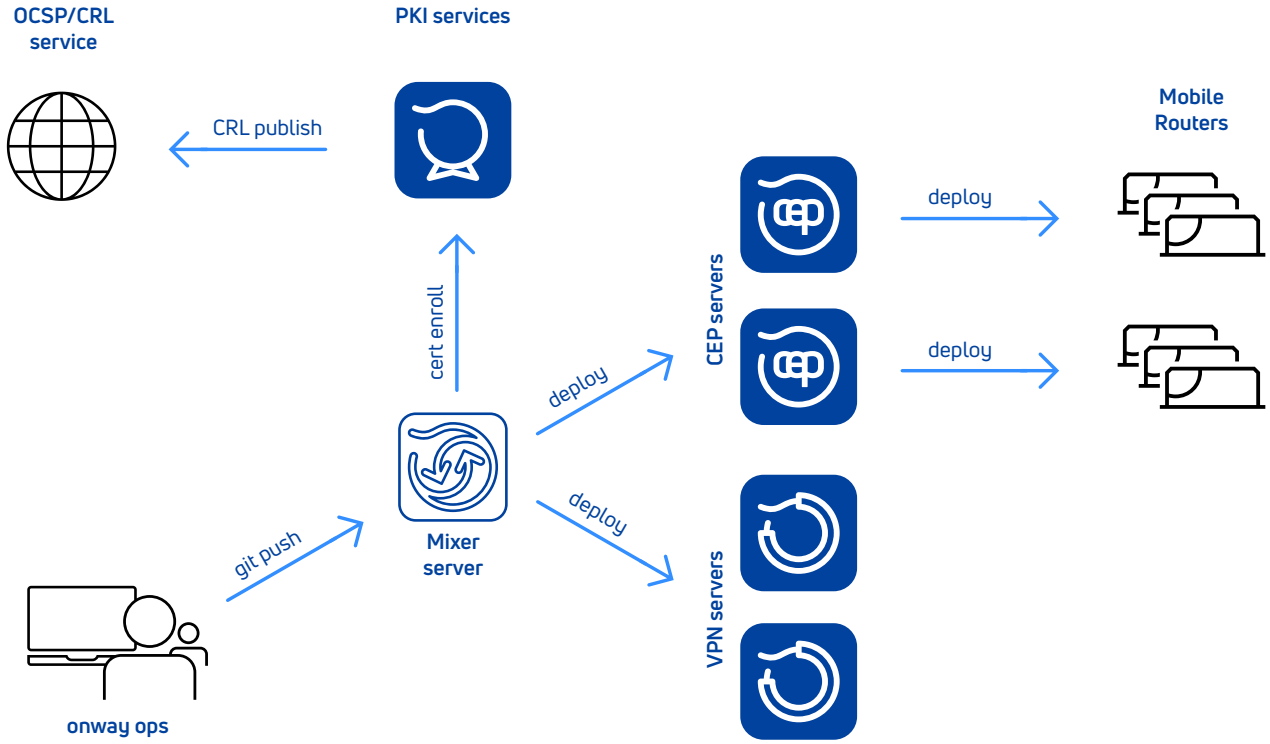
  Several routers can be operated in parallel, thus avoiding overloading individual routers. This enables seamless adaptation to increasing requirements without bottlenecks or performance losses.

- Cost-effective hardware ***– high quality hardware, low cost!***

  Our hardware is available in different configurations; from small to large. This means that we offer solutions for every purpose at attractive prices.



The following image shows the architecture of the onway SD-WAN solution. Below we describe the main functions of the various components.



Mixer

The Mixer is the central interface for creating and modifying configurations for mobile routers/ servers and VPN gateways. The configuration is based on the IaC (Infratructure as Code) approach, which means that the router configuration is written in hardware-independent YAML notation. This is validated on the mixer and adapted to the target hardware. The mixer interacts with the PKI to enroll certificates required for IPsec authentication. After the full configuration is generated, the mixer transmits the configuration to the CEP or directly to the VPN gateways.

GEP (Global Entry Point)

The primary purpose of the GEP is to synchronize time with the onway routers to enable certificate-based authentication and ZeroTouch provisioning. In addition, routers are assigned to the corresponding customer installations via the GEP. To do this, the GEP forwards the router to the appropriate Customer Entry Point (CEP). The GEP is hosted and managed by onway.

CEP (Customer Entry Point)

The CEP is responsible for deploying the configuration received from the mixer to onway routers and updating router images. In addition, the CEP enables remote access to sites at any time via a secure protocol of the management level called BRUSH. CEPs are typically provisioned and managed by onway and therefore hosted in the onway cloud but can also be placed at the customer›s premises.

VPN-Gateway / concentrator

The VPN gateway enables encrypted communication between the central locations and the onway routers. VPN gateways are located at onway and/or at the customers, their partners or suppliers, depending on the use case.

onway router

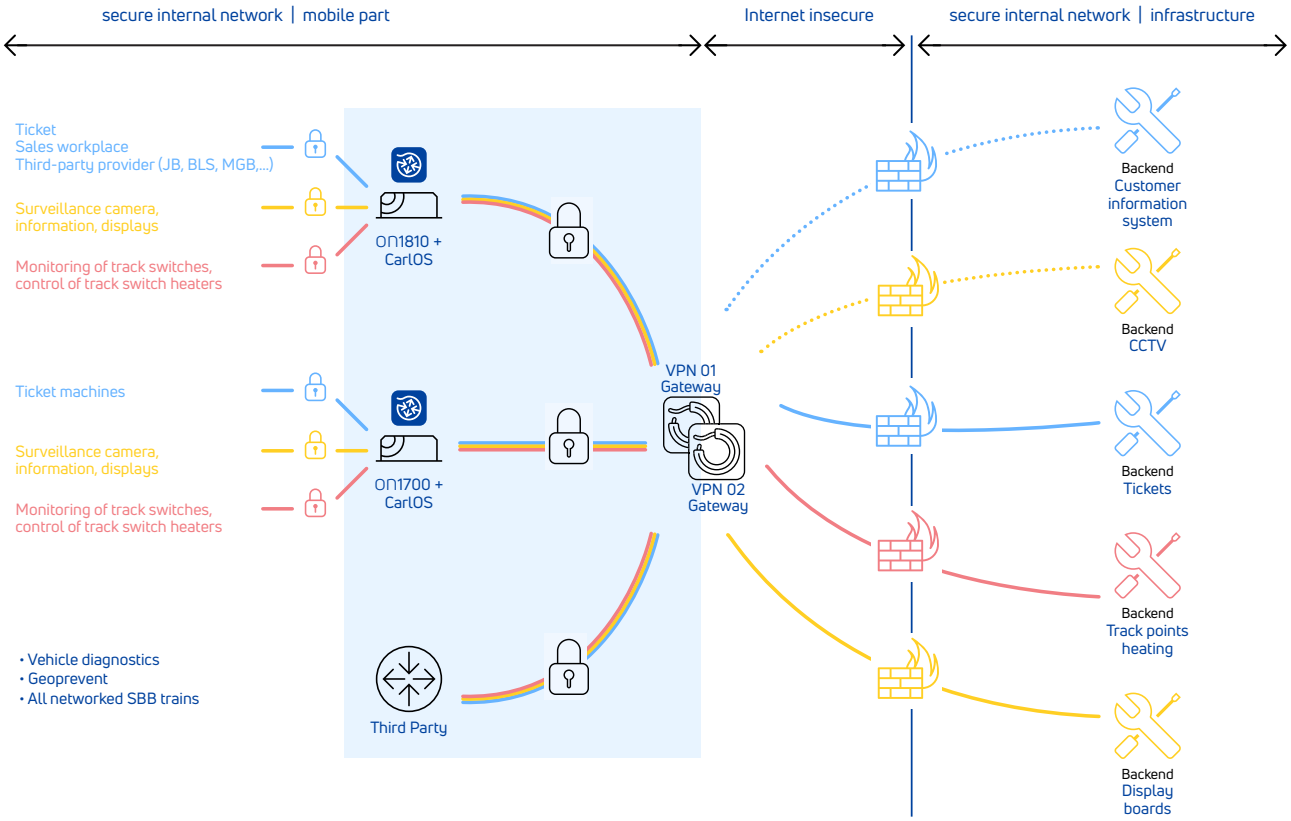
Mobile onway routers can also be used in unprotected locations. They are based on a zero-trust architecture by default and protect the private network from unauthorized access. They allow communication at the same time via multiple uplinks. Thanks to constant signal, loss and latency measurements, they dynamically adapt to rapidly changing circumstances.

Our solution using the example of SBB

As part of a GATT/WTO tender for up to 10,000 routers, SBB opted for our SD-WAN complete solution in 2022, consisting of mobile routers, central VPN concentrators and our management system. Our routers serve as secure network access points for the increasingly digitalised SBB infrastructure via various technologies (mobile communications, WLAN, WAN). In this case, different internal SBB networks must be connected to the central network via the same VPN tunnel and securely separated by means of multi-VRF separation. onway is taking over the maintenance, operation and support of the entire infrastructure for an initial period of nine years with an option for extension.

Project Requirements

SBB needs various services for its independent departments. Digital services were also partly implemented by partner companies and their products, with SBB always having sovereignty. Our SD-WAN solution integrated all applications and partners into centralized and automated management, as the graphic below shows.



- ## Surveillance

  SBB uses IP-capable cameras for video surveillance. With our SD-WAN solution, we can provide both connectivity and power for these cameras from the router at the same time. This creates a compact solution for monitoring SBB facilities. By using dual modems, we were also able to increase capacity and bandwidth to transmit high-resolution video in real time.

- ## Ticket machines

  To pay for tickets by credit card, obtain gift vouchers or top up prepaid mobile phones at SBB ticket machines, the corresponding data or communication transmission is required. This is now taken over by our routers.

- ## Switch Heaters

  The numerous switches along the SBB railway lines are particularly sensitive and critical points in the track layout. Under the influence of moisture and freezing temperatures, there is a risk that flexible rail components could freeze. Therefore, the switch heaters must be able to be activated or deactivated as needed. Our routers are used here to ensure automatic control.

- ## Digital Display Boards

  Overhead display boards are essential at train stations for travellers to receive key information such as departure times, delays, and schedule changes. Our solution ensures the seamless delivery of these real-time updates at both smaller and larger stations, keeping passengers consistently informed.

- ## Notification for upcoming maintenance

  SBB operates diagnostic vehicles that analyse the rails and automatically detect any necessary maintenance work. The resulting large amount of data is transmitted quickly and securely to the landside thanks to the onway routers.

- ## Seamless Train-to-Ground Connectivity

  The approximately one thousand SBB trains that use train-to-ground networks are connected to central systems on the ground via our VPN gateways.

- ## Third-Party Sales Points

  To allow sales workstations at other providers to access the SBB ticketing system, SBB relies on onway routers, which enable this secure access. Communication is carried out either via mobile networks or through a wired internet connection.