

SD-WAN: Software Defined Networking



Vous souhaitez connecter, surveiller et contrôler de manière sécurisée, performante et éventuellement à l'échelle internationale des sites (tels que des succursales), des installations, des véhicules, des capteurs et des appareils, indépendamment de leur emplacement et de la technologie utilisée. Qu'il s'agisse d'une ou de milliers d'infrastructures, le réseau doit être facile et flexible à exploiter. Cela pose divers défis. Le plus important est la configuration d'un grand nombre de connexions et d'appareils. Auparavant, chaque appareil devait être configuré individuellement par défaut. Par conséquent, si un petit ajustement devait être effectué, il devait être effectué individuellement pour chaque appareil, ce qui est sujet aux erreurs et implique beaucoup de temps et d'argent. L'évolutivité de ces solutions a donc été plutôt faible dans le passé. De plus, les qualités fluctuantes des réseaux entraînent une connectivité instable et les connexions via les réseaux publics s'accompagnent de risques de sécurité.

SD-WAN

La solution s'appelle SD-WAN, c'est-à-dire Software Defined Networking dans un Wide Area Network, un réseau étendu. Avec notre solution logicielle, les sites externes et les appareils peuvent être connectés au réseau de l'entreprise de manière très simple et sécurisée.

Avantages d'une solution SD-WAN

Une solution SD-WAN est adaptée à divers scénarios au sein d'une organisation. Il est particulièrement avantageux pour la mise en réseau de :

- Plusieurs sites ou succursales de l'entreprise
- Systèmes à distance, machines, centrales électriques, systèmes solaires, éoliennes, capteurs, etc.
- Véhicules mobiles (camions, transports en commun, engins de chantier, etc.)
- Lieux temporaires (transports, camionnettes de vente, open air, pop-up stores, etc.)
- Connexion de plusieurs fournisseur·euse·s de cloud
- Appareils de l'Internet des objets (IoT)

Connexion de différents environnements et systèmes

L'un des plus grands avantages de la solution SD-WAN est donc l'intégration flexible de tous les sites internes et externes dans une infrastructure réseau privée et sécurisée. Ces réseaux distants peuvent ainsi être connectés, qu'il s'agisse de liaisons transfrontalières ou sur de longues distances, de manière à être constamment accessibles, surveillés et contrôlés.

Gestion centralisée et automatisation

Le développement de nombreux sites distants nécessite une gestion et un contrôle automatisés et centralisés du réseau. Cela signifie que des modifications ou des environnements supplémentaires peuvent être effectués sans effort à tout moment, quelle que soit leur position ou leur type de connexion. L'extension du réseau s'effectue sans configurations manuelles complexes et est donc hautement évolutive. Une automatisation cohérente permet d'économiser du temps et de l'argent et de minimiser les sources d'erreur.

Connectivité fiable

En établissant plusieurs connexions parallèles par l'intermédiaire de fournisseurs de réseau, les performances et la fiabilité de la connectivité peuvent être augmentées. Les connexions redondantes optimisent le trafic et assurent un réseau stable même dans des contextes volatils.

Sécurité

Les connexions sont authentifiées et cryptées selon les normes de sécurité les plus élevées. Les directives centrales en matière de protection des données et de conformité sont respectées à tout moment. Cependant, la solution prend également en charge les besoins individuels et fonctionne sur une grande variété de ressources réseau (réseaux mobiles, connexions de location, Internet, etc.).

La solution SD-WAN onway

Les arguments de vente uniques suivants distinguent la solution SD-WAN onway :

- Déploiement sans contact – **Déballiez et branchez-le !**

Les appareils et les emplacements sont prêts à l'emploi immédiatement sans configuration manuelle. Les routeurs se connectent automatiquement au système de gestion central dès qu'ils ont été connectés à un réseau et reçoivent automatiquement tous les paramètres et mises à jour nécessaires. Cela simplifie et accélère considérablement l'installation de réseaux, même de grande taille.

- Gestion centralisée – **L'administration simplifiée !**

Notre technologie de gestion centralisée des routeurs permet une gestion efficace de la configuration, y compris la gestion des versions, sur le cloud central onway. Un environnement de test automatisé valide toutes les modifications et garantit ainsi un déploiement sans problème. Une interface utilisateur intuitive simplifie encore la gestion pour les administrateur·rice·s.

- La sécurité dès la conception – **Sécurisez dès le départ !**

D'importants principes de sécurité sont déjà intégrés dans la conception de la solution globale, ce qui élimine la nécessité de prendre des mesures ultérieures. Par défaut, toutes les connexions réseau entrantes sont bloquées, sauf si elles sont explicitement autorisées. L'utilisation de certificats est obligatoire, de sorte que seuls les appareils authentifiés et les utilisateur·rice·s y ont accès. De plus, des mises à jour régulières et des correctifs de sécurité offrent une protection supplémentaire contre les menaces.

- Mises à jour sécurisées des configurations et des logiciels

- **Mises à jour sans risque d'échec !**

La mise à jour des paramètres de configuration et des versions logicielles est protégée par différents mécanismes. Après une mise à jour, les routeurs vérifient la connexion à la gestion centrale. En cas de mauvaises configurations et d'interruptions du réseau qui en résultent, les routeurs sont automatiquement réinitialisés au dernier état de fonctionnement. À l'aide d'un système à double démarrage, les nouvelles images sont chargées sur la partition actuellement inactive et tentent de démarrer à cet endroit. Si cela ne fonctionne pas, il reviendra automatiquement à l'ancienne partition fonctionnelle. Cela garantit qu'une mise à jour est toujours effectuée sans problème ou pas du tout. L'état de l'appareil est également signalé par des feux de circulation et clignotants facilement reconnaissables sur l'appareil. Cela signifie que les défauts peuvent également être détectés sur place par la LED affichée.

Le matériel est conçu et certifié « by design » pour les environnements difficiles. Par conséquent, les pannes matérielles sont rares et le logiciel dispose de mécanismes de contrôle étendus. Tout cela minimise le risque de temps d'arrêt ou d'interruptions opérationnelles et augmente la fiabilité du réseau.

- Contrôle actif de la qualité de la transmission (Dynamic QoS)

- **Optimisation de la qualité de la transmission !**

Les connexions réseau sous-jacentes sont de qualité variable. Le trafic commercial doit donc être activement contrôlé afin que les applications critiques puissent communiquer à tout moment. Le terme « qualité de service dynamique (QoS) » fait référence à une variété de mécanismes permettant de mesurer en continu la bande passante et la latence, ainsi que de hiérarchiser et de lisser (façon-

ner) le trafic utilisateur. Grâce à ces mécanismes, les applications critiques sont toujours garanties de la meilleure qualité et fiabilité possibles.

- Réaction dynamique aux changements de liens (mobilité, interruptions, etc.) en temps réel – **Réaction en temps réel aux changements de liens !**

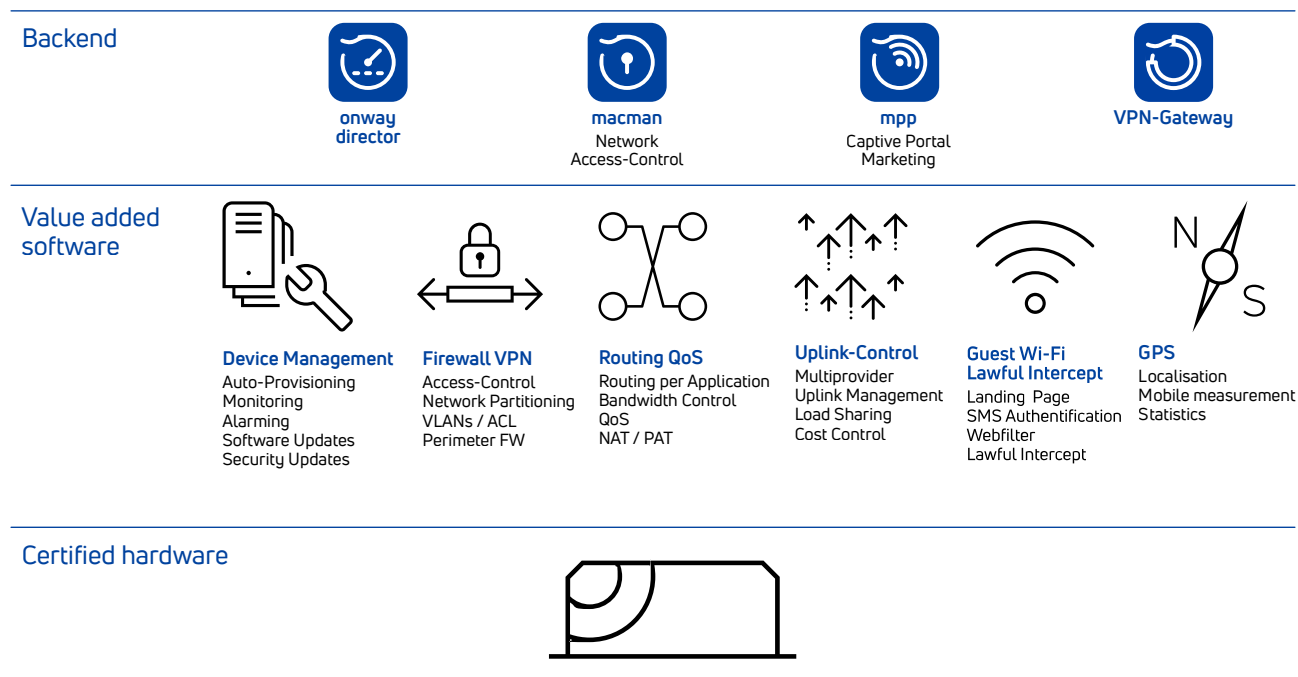
Le système détecte automatiquement lorsqu'une connexion est interrompue ou modifiée et prend des mesures pour rediriger le trafic vers d'autres chemins ou rétablir la connexion. Cela se fait à l'aide de l'agrégation transparente de plusieurs liaisons montantes (Ethernet, cellulaire, Wi-Fi, etc.) et de protocoles de routage dynamiques. Cela améliore la fiabilité et assure la continuité de la communication réseau, même en cas d'interruption de la connexion.

- Mise à l'échelle horizontale de plusieurs routeurs – **Performances optimales grâce à l'utilisation de routeurs parallèles !**

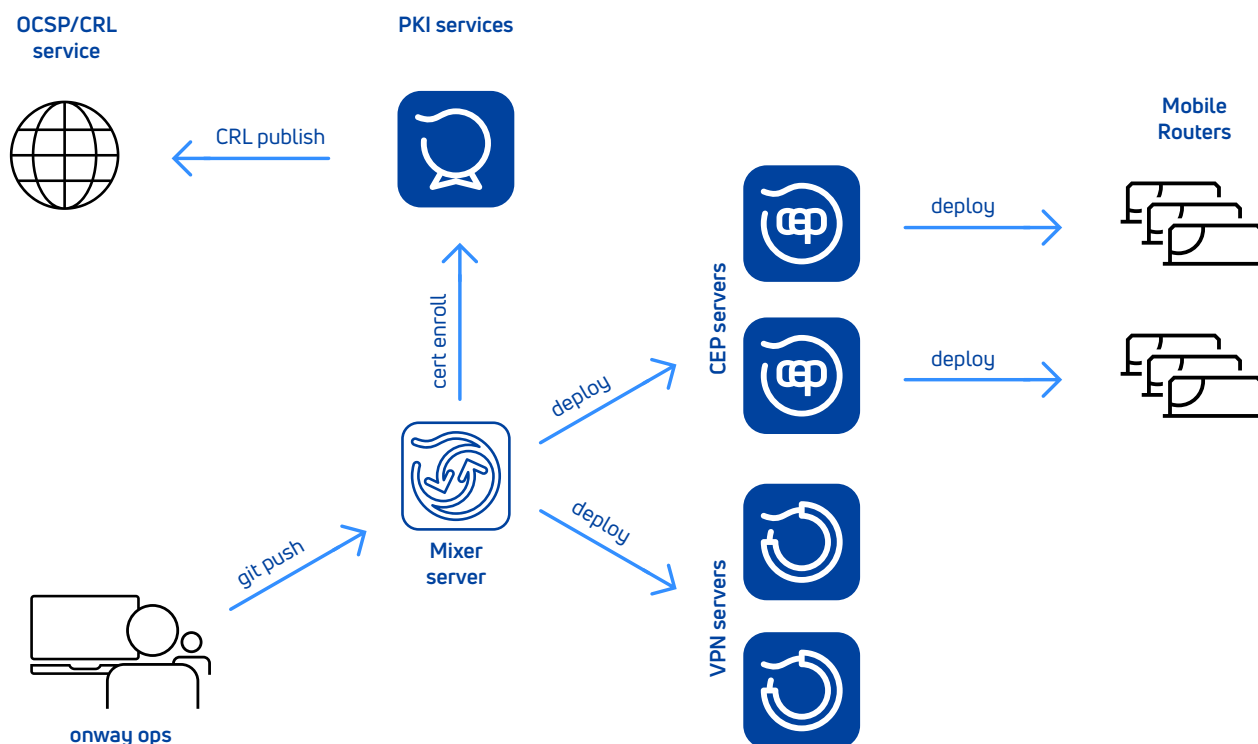
Plusieurs routeurs peuvent être utilisés en parallèle, ce qui évite de surcharger les routeurs individuels. Cela permet une adaptation sans faille aux exigences croissantes sans goulets d'étranglement ni pertes de performance.

- Hardware rentable – **Hardware de haute qualité, faible coût !**

Notre hardware est disponible en différentes configurations ; du petit au grand. Cela signifie que nous proposons des solutions pour chaque usage à des prix attractifs.



L'image suivante montre l'architecture de la solution SD-WAN onway. Nous décrivons ci-dessous les principales fonctions des différents composants.



Mixer

Le Mixer est l'interface centrale pour la création et la modification des configurations des routeurs/serveurs mobiles et des VPN-Gateways. La configuration est basée sur l'approche IaC (Infrastructure as Code), ce qui signifie que la configuration du routeur est écrite en notation YAML indépendante du hardware. Celui-ci est validé sur le Mixer et adapté au hardware cible. Le Mixer interagit avec l'infrastructure PKI pour inscrire les certificats requis pour l'authentification IPsec. Une fois la configuration complète générée, le Mixer transmet la configuration au CEP ou directement aux VPN-Gateways.



GEP (Global Entry Point)

Le principal objectif du GEP est la synchronisation temporelle avec les routeurs onway, afin de permettre l'authentification basée sur des certificats et le déploiement Zero Touch. De plus, les routeurs sont associés aux installations clients correspondantes via le GEP. Pour cela, le GEP redirige le routeur vers le point d'entrée client (CEP) approprié. Le GEP est hébergé et géré par onway.



CEP (Customer Entry Point)

Le CEP est responsable du déploiement des configurations reçues du Mixer sur les routeurs onway et de la mise à jour des images des routeurs. De plus, le CEP permet un accès à distance permanent aux sites via un protocole sécurisé de niveau de gestion appelé BRUSH. Les CEP sont généralement fournis et gérés par onway et sont donc hébergés dans le onway cloud, mais ils peuvent également être installés chez le client.



VPN-Gateway / Concentrateur

Le VPN Gateway permet une communication chiffrée entre les sites centraux et les routeurs onway. Les VPN Gateways se trouvent, selon le cas d'utilisation, chez onway et/ou chez les clients, leurs partenaires ou leurs fournisseur·euse·s.



Routeur onway

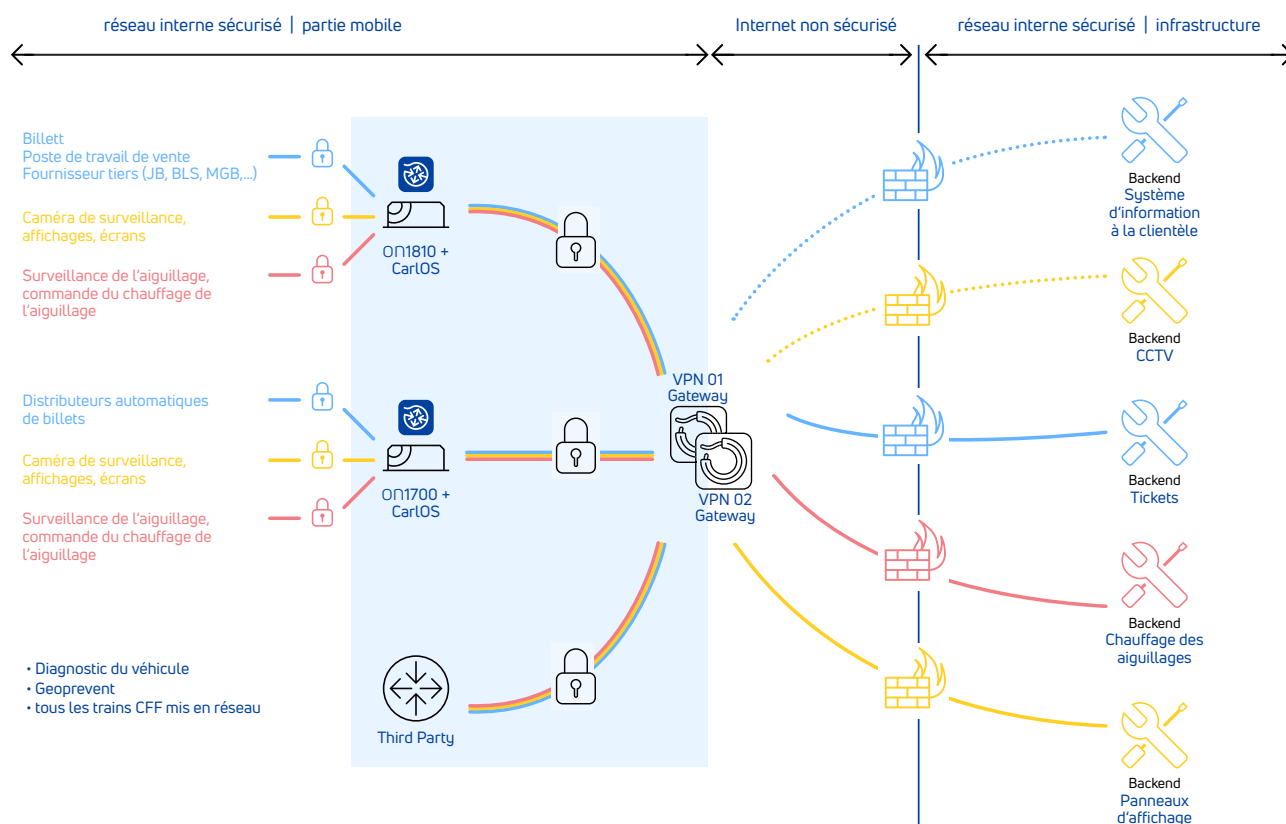
Les routeurs mobiles onway peuvent également être utilisés dans des sites non sécurisés. Par défaut, ils reposent sur une architecture Zero Trust et protègent le réseau privé contre les accès non autorisés. Ils permettent la communication simultanée via plusieurs liaisons montantes. Grâce à des mesures constantes du signal, des pertes et de la latence, ils s'adaptent dynamiquement aux conditions changeantes.

Notre solution à l'aide de l'exemple des CFF

Dans le cadre d'un appel d'offres du GATT/OMC portant sur un maximum de 10 000 routeurs, les CFF ont opté en 2022 pour notre solution complète SD-WAN, composée de routeurs mobiles, de concentrateurs VPN centraux et de notre système de gestion. Nos routeurs servent de points d'accès sécurisés au réseau pour l'infrastructure des CFF de plus en plus numérisée via différentes technologies (communications mobiles, WLAN, WAN). Dans ce cas, les différents réseaux internes des CFF doivent être connectés au réseau central via le même tunnel VPN et séparés en toute sécurité par une séparation multi-VRF. onway prend en charge la maintenance, l'exploitation et le support de l'ensemble de l'infrastructure pour une période initiale de neuf ans, avec une option de prolongation.

Exigences du projet

Les CFF ont besoin de différents services pour leurs départements indépendants. Les services numériques ont également été en partie mis en œuvre par des entreprises partenaires et leurs produits, les CFF ayant toujours la souveraineté. Notre solution SD-WAN a intégré toutes les applications et tous les partenaires dans une gestion centralisée et automatisée, comme le montre le graphique ci-dessous.



- Surveillance

Pour la vidéosurveillance, les CFF utilisent des caméras compatibles IP. Avec notre solution SD-WAN, nous pouvons fournir simultanément la connectivité et l'alimentation pour ces caméras directement depuis le routeur. Cela crée une solution compacte pour la surveillance des installations des CFF. Grâce à l'utilisation de modems doubles, nous avons également pu augmenter la capacité et la bande passante afin de transmettre des vidéos haute définition en temps réel.

- Distributeurs de billets

Pour payer des billets par carte de crédit, obtenir des chèques-cadeaux ou recharger des téléphones portables prépayés aux distributeurs de billets CFF, la transmission de données ou de communication correspondante est nécessaire. Celui-ci est maintenant pris en charge par nos routeurs.

- Chauffages d'aiguillages

Les nombreux aiguillages le long des voies ferrées des CFF représentent des points particulièrement sensibles et critiques du tracé des rails. Sous l'effet de l'humidité et des températures glaciales, il existe un risque que les parties flexibles des rails gèlent. C'est pourquoi les chauffages d'aiguillages doivent pouvoir être activés ou désactivés en fonction des besoins. Nos routeurs sont utilisés ici pour garantir le contrôle automatique.

- Tableaux d'affichage numériques

Les tableaux d'affichage suspendus sont indispensables dans les gares pour les voyageurs afin d'obtenir des informations essentielles telles que les horaires de départ, les retards et les modifications de programme. Notre solution garantit une mise à jour fluide de ces informations en temps réel dans les petites et grandes gares, afin que les passagers soient toujours informés.

- Notification de maintenance à venir

Les CFF exploitent des véhicules de diagnostic qui analysent les rails et détectent automatiquement les travaux d'entretien éventuels. La grande quantité de données générée est rapidement et en toute sécurité transmise vers la terre grâce aux routeurs onway.

- Connectivité fluide entre le train et la terre

Le millier de trains CFF qui empruntent les réseaux train-terre sont reliés aux systèmes centraux côté ville par le biais de nos Gateways VPN.

- Points de vente de tiers

Pour que les postes de vente d'autres fournisseur-euse-s puissent accéder au système de billetterie des CFF, les CFF utilisent les routeurs onway, qui permettent cet accès sécurisé. La communication s'effectue soit par réseau mobile, soit par une connexion Internet câblée.