Device Management WebCenter

ermöglicht die zentrale Verwaltung aller Router und der Geräte im lokalen Netz.

Das Device Management WebCenter bietet folgende Features:

Router:

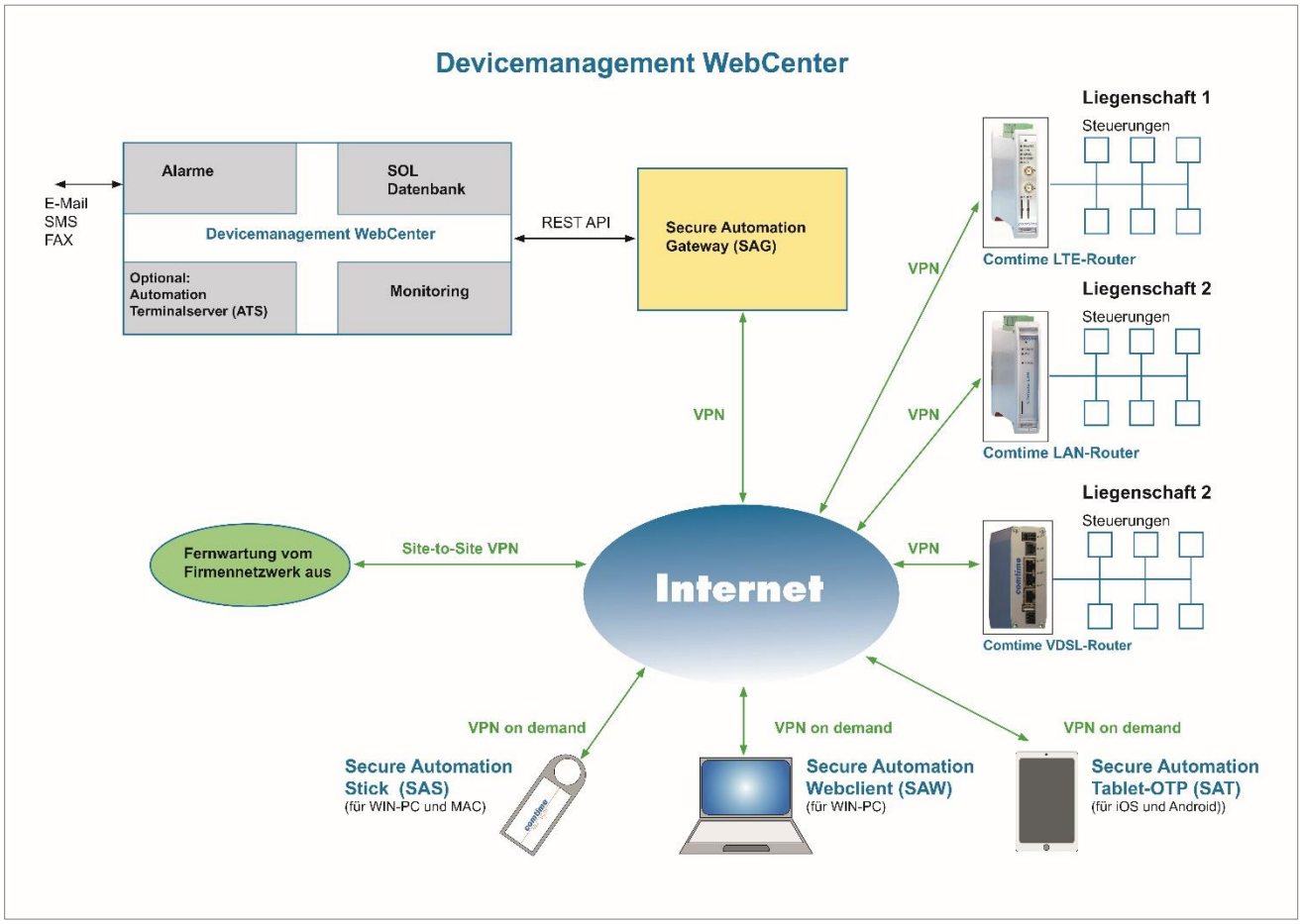
- Remote-Konfigurationsänderung der Router
- Remote-Firmware-Update der Router
- Remote die Zertifikate der Router einspielen bzw. die Zertifikate nach Ablauf erneuern
- Download der Konfigurationsdatei zur Offline-Konfiguration der Router via USB-Stick

Netzwerk:

Monitoring der CT-Router und der Steuerungen in den einzelnen Liegenschaften

- Alarmierung via E-Mail, SMS oder Fax, wenn ein Router offline ist oder eine Anlage eine Störung meldet
- Standortübergreifende Erfassung von Alarmen und Zähler-/Messwerten in einer zentralen SQL-Datenbank
- Schnittstellen zu Energiemanagementsystemen, GLT-Servern, Abrechnungssystemen, ERP, Leitwarten, Ticketsystemen usw.

Übersicht Graphik - Device Management WebCenter mit den CT-Routern



Netzwerk Komponenten

Router

Die Comtime VPN-Router gibt es in verschiedenen Varianten:

- Festnetzrouter: LAN, ADSL, VDSL
- Mobilfunk: 5G, LTE, UMTS, GPRS

Die Router werden so konfiguriert, dass nach dem Einschalten ein VPN-Tunnel oder eine sichere HTTPS Verbindung zum zentralen Secure Automation Gateway (SAG) aufgebaut wird.

Das Device Management WebCenter ermöglicht die zentral verwalten der Router.

Die Konfigurationsdateien (aus Sicherheitsgründen verschlüsselt) für die Router können direkt vom Device Management WebCenter heruntergeladen und über Webbrowser oder per USB-Stick offline eingespielt werden.

Secure Automation Gateway (SAG)

Das SAG stellt die zentrale Komponente des *Secure Automation Systems* dar. Es dient als VPN-Gateway, Fernwartungsserver, Authentisierungsserver, Berechtigungssystem, Router-Management, PKI sowie als zentraler Managementserver für alle Komponenten. Das SAG ist als virtuelle Appliance (lauffähig auf VMware®, Hyper-V®, XenServer®, Oracle VirtualBox®) oder als Hardware-Appliance erhältlich. Die virtuelle Appliance wird je nach Anforderung entweder beim Kunden oder in einem Rechenzentrum gehostet. Bei Bedarf kann über einen VPN-Tunnel zwischen dem Secure Automation Gateway (SAG) und dem Firmennetzwerk (Site-to-Site VPN) ein sicheres und Hersteller-unabhängiges Fernwartungssystem realisiert werden.

Weitere Komponenten:

Secure Automation Stick (SAS)

Der SAS erlaubt es, von extern sicher auf beliebige Anlagenvisualisierungen oder Steuerungen zuzugreifen. Dieser spezielle USB-Stick benötigt keinerlei Installation oder Adminrechte und hinterlässt auf dem Windows® Gastsystem keine Spuren, da er in einer abgeschirmten Umgebung läuft.
Die Konfiguration des Sticks erfolgt zentral über das SAG.

Secure Automation Webclient (SAW)

Der SAW ist die USB-sticklose Variante des *Secure Automation Sticks (SAS)* mit identischen Features.

Secure Automation Tablet-OTP (SAT)

Mit dem SAT ist ein hochsicherer Zugriff auf Automationsanlagen von Tablets oder Smartphones aus möglich. Beim iPad®/iPhone® wird dazu der im iOS® integrierte VPN-Client verwendet, erweitert um eine zweistufige Authentisierung mit einem OTP-Token. Bei Android®-Tablets/-Smartphones wird die Original OpenVPN-App unterstützt, ergänzt um eine Zwei-Faktor-Authentisierung mit OTP-Token.