Funktionsprincip myREX24

VPN-portalen myREX24 fungerar som förmedlingscentral för VPN-kommunikationen mellan fjärrunderhåll och kundanläggning. Det är en central VPN-åtkomst för programmerare, maskin- och servicetekniker på ena sidan och REX routrar som åtkomstpunkt på maskinen på andra sidan.

Varje REX router tilldelas ett unikt företagskonto i myREX24-portalen. På så sätt är det säkerställt att bara bestämda användare har åtkomst till bestämda routrar på plattformen.

Även problemet med lokala brandväggar kan förbigås med VPN-portalen. De lokala brandväggarna är förbundna med routernas WAN-nätverk. En åtkomst till REX routern via Internet är för det mesta förbjuden. Utgående förbindeler är dock för det mesta tillåtna, routern använder dessa för att ”logga in sig” på den centrala VPN-ingången.

Förbindelseprincip

myREX24.net serverportal bygger på OpenVPN. Krypteringen hos OpenVPN bygger på OpenSSL.

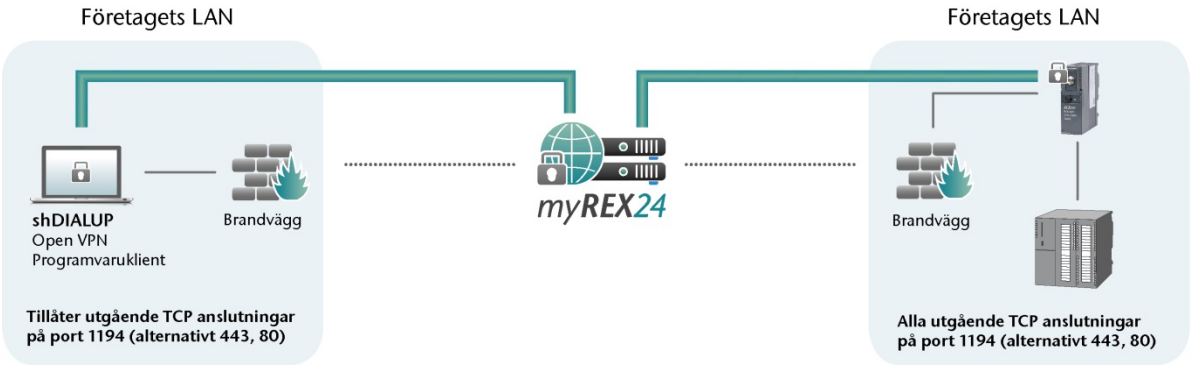
Upprättandet av förbindelsen till portalen sker alltid från två håll:

1. Från programmeraren som använder programvaran shDIALUP.

2. Från maskinsidan med en REX router.

På båda sidorna upprättas uteslutande utgående TCP förbindelser (OpenVPN port 1194, alternativt även port 443 eller port 80). Det är inte möjligt att använda UDP protokollet för förbindelser till myREX24.net serverportal.

Programmeraren använder som Internetåtkomst det lokala företagsnätverket som har en anslutning till Internet via en router och en brandvägg.



Maskinsidan är ansluten till Internet på samma sätt. REX Router är förbunden med kundnätverkets router via WAN-gränssnittet och upprättar via det en VPN anslutning till portalen. Som alternativ finns även routrar som kan logga in sig via en mobilanslutning (GPRS, UMTS).

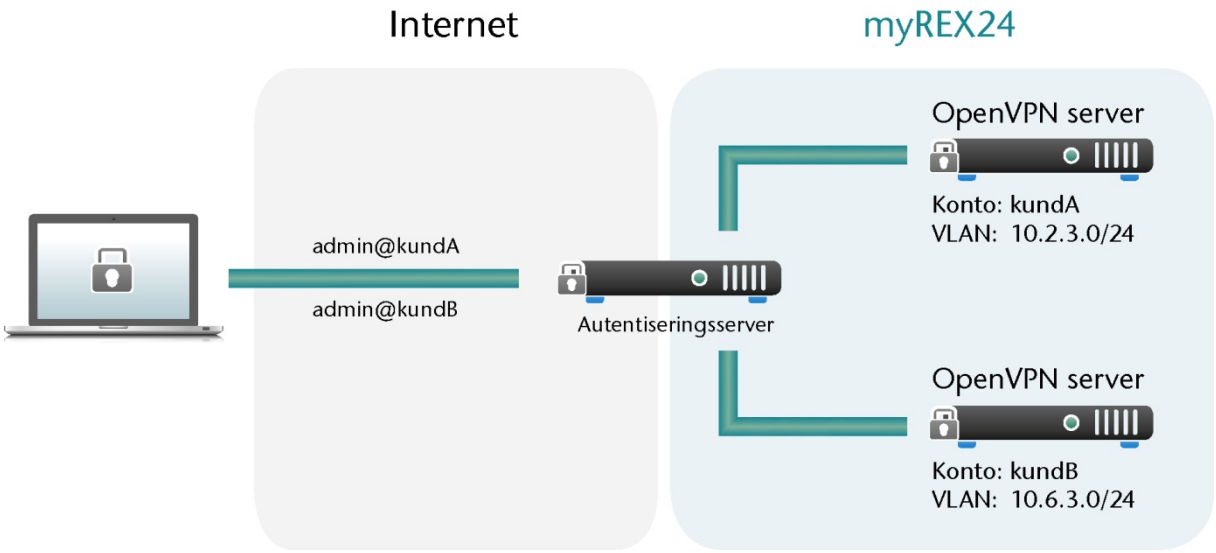
Maskinnätverket är förbunden med REX routern via LAN gränssnittet. VPN tunneln möjliggör åtkomst till alla enheter i REX routerns maskinnätverk på LAN sidan.

Fjärrunderhållssida

Programmeraren/fjärunderhållsteknikern upprättar med programvaran shDIALUP en förbindelse till portalservern via en utgående TCP- förbindelse på TCP port 1194 (alternativt port 443 eller 80). För att detta ska fungera måste den port som används vara öppen för utgående förbindelser i den lokala brandväggen och företagets brandvägg.

På samma sätt är det möjligt att upprätta en förbindelse via en HTTP Proxy. I så fall måste HTTP CONNECT metoden och en förbindelse via de ovan nämnda portarna tillåtas av Proxy.

Utifrån kontonamnet avgör autentiseringsservern till vilken OpenVPN server förfrågan måste sändas vidare. Vidarebefordran görs sedan via portalserverns routing funktion.



Den verkliga förbindelsen och kontrollen av säkerhetsparametrar görs av med kontots OpenVPN server och inte med autentiseringsservern.

När förbindelsen till portalen har upprättats hämtar shDIALUP nätverksadaptern via DHCP sin IP-adress för det virtuella nätverket från kontots OpenVPN server.

Programvaran shDIALUP lägger nu till routern för VPN nätverket i den lokala routertabellen och startar portalens översiktssida.

I översikten ser programmeraren vilka av hans REX routrar som redan har upprättat en förbindelse till portalen. Han klickar på knappen ”Anslut” vilket leder till att portalen frågar vilka av maskinnätverkets routrar som ska noteras och överlämnar dessa till programvaran shDIALUP som noterar routrarna i Pc:ns routertabell.

Därmed har förbindelsen upprättats.

Maskinsida

Upprättandet av förbindelsen sker på samma sätt som på programmerarens sida. OpenVPN är fast implementerad i routerns fasta programvara. WAN förbindelsen kan lösas via slutkundens nätverk eller via en mobil förbindelse.

En väsentlig skillnad på maskinsidan beror på möjligheten att man även vid behov kan utlösa upprättandet av förbindelsen till portalen individuellt. Det är praktiskt om VPN tunneln till portalen inte ska upprätthållas permanent. Beroende på enhetsvariant står olika möjligheter till förfogande för att utlösa upprättandet av förbindelsen:

- digitala ingångar
- dialout knapp
- SMS
- samtal

Konfiguration

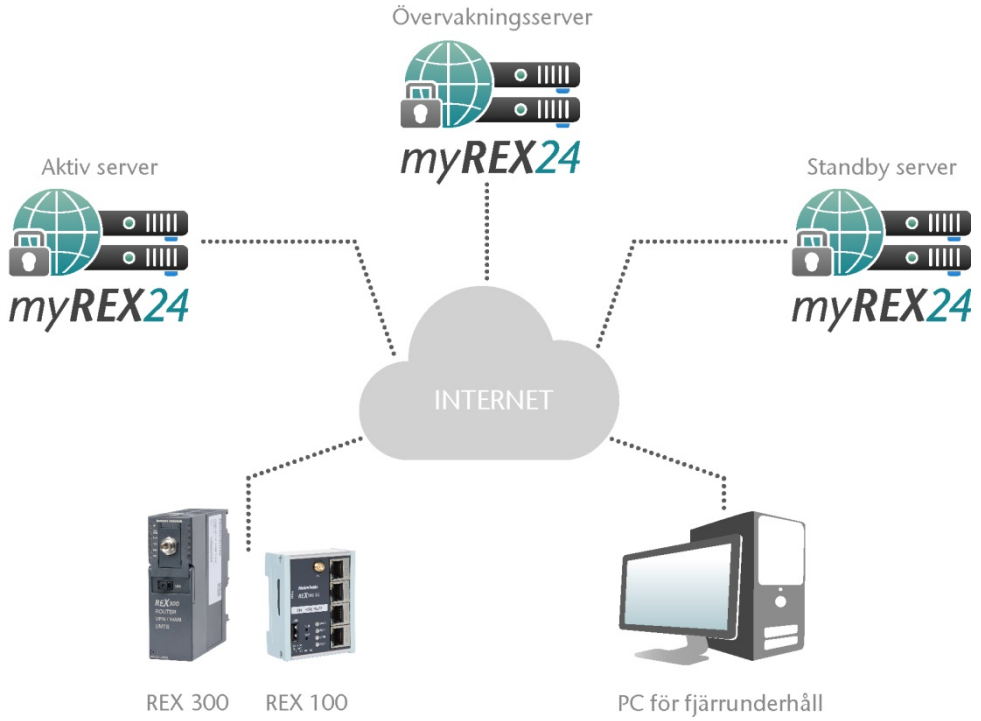
Konfigurationen av routern görs i myREX24 portalen och kan överföras till enheten på olika sätt. Vid sidan av överföring av konfigurationsfilen via USB-minne tillåter Configuration Transfer Manager (CTM) som ingår i portalen att man konfigurerar en router via en Internetanslutning. Dessutom är det möjligt att göra en direkt överföring av parametrarna med LAN.

Enheterna identifieras entydigt med hjälp av serienumret. Vid den första konfigurationen överförs OpenVPN inloggningsuppgifterna.

myREX24 portalens värdfunktioner

myREX24 portalens värdfunktioner ligger redundant i ett högsäkert datacentrum och kopieras ständigt till en standby server. En övervakningsserver övervakar driften och utlöser vid en felfunktion en omkoppling till standby-servern.

myREX24 portalens databas säkras dessutom cykliskt.



myREX24 säkerhetsegenskaper

- bygger på Open Source Standard ”OpenVPN”
- autentisering av servern med X.509 certifikat (RSA 1024-bit)
- autentisering av klienten med användarnamn/lösenord
- slumpartad OpenVPN lösenord med 15 tecken för varje REX router (kan ändras)
- Diffie-Hellmann kodutbyte med 1024 bit
- OpenVPN överföringskryptering med OpenSSL (TLS 1.0), Blowfish CBC (128-Bit), SHA1
- varje konto är tilldelat till en egen OpenVPN server (tilldelning via kontonamn)
- REX router ansluts fast till ett konto genom den första parametreringen
- värd placerad i högsäkert datacentrum
- redundant värdfunktion (upp till 99,9 % tillgänglighet)
- särskiljning av företags- och maskinnätverk i REX router (WAN/LAN)
- extra brandvägg i REX router mellan WAN och LAN
- hantering av användare och rättigheter i portalen
- rapporter om varje upprättad förbindelse
- permanenta säkerhetsuppdateringar av portalens programvara
- snabb reaktion vid rapporterade säkerhetsluckor

Ytterligare information

http://openvpn.net/index.php/open-source/documentation.html

http://www.openssl.org/related/ssl.html

https://www.bsi.bund.de → ”ICS Security Kompendium” & ”Fjärrunderhåll i industriell miljö”

https://www.allianz-fuer-cybersicherheit.de

Ändringar och misstag förbehållna för alla uppgifter.
För övrigt gäller våra allmänna affärsvillkor. Dessa finns att läsa på www.helmholz.de.

Aktuell per: 2015-10-07