The operating principle of myREX24 V2

The VPN portal myREX24 V2 serves as a mediation server for VPN communication between the provider of remote maintenance and the customer facility. On the one hand, it provides central VPN access for programmers and machine and service technicians, and on the other hand, it serves as an access point of the machine for the REX routers. The myREX24 V2 portal can also be used for the protocolling and visualization of machine data, which can be read in from the machine via the REX router.

Each REX router is unambiguously assigned to a company account in the myREX24 V2 portal. Any number of users with access rights can be administered in the account. This ensures that only authorized users have access to the approved router on this platform.

Likewise, the problem of local firewalls is bypassed with the VPN portal. Local firewalls are connected to the WAN network of the router. Access from the Internet to the REX router is usually prohibited. Outgoing connections are often allowed or can be easily and securely realized. The router then in this way “dials” into its account on the central VPN server.

Connection principle

The myREX24 Server Portal was implemented on the basis of OpenVPN. The encryption of OpenVPN is based on OpenSSL.

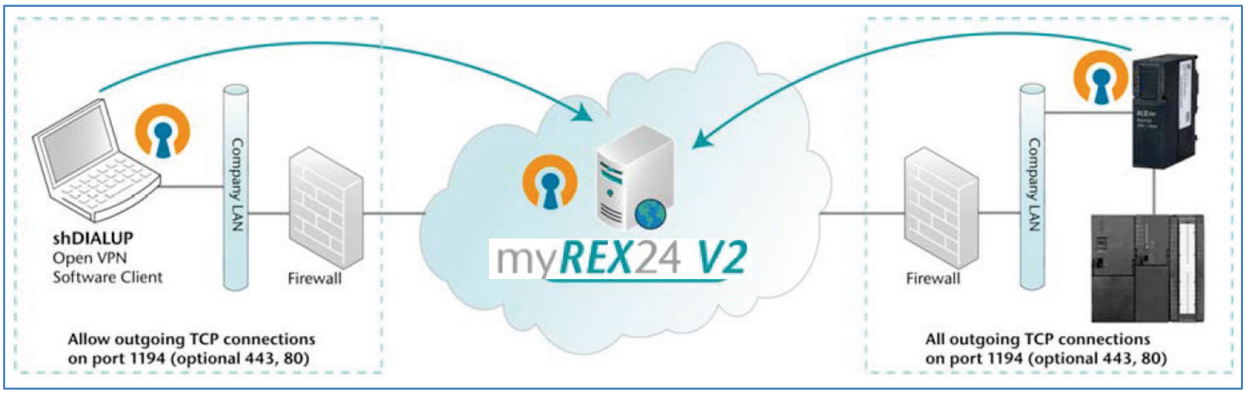
Establishing the connection to the portal is always carried out from two sides:

1. The side of the service technician who uses the shDIALUP software

2. The machine side with a REX router.

On both sides only outgoing TCP connections are established (OpenVPN port 1194, optionally port 443 or port 80). The use of the UDP protocol for connections to the myREX24 Server Portal is not possible.

The service technician uses the local company network as Internet access; this is connected to the Internet using a router and a firewall.


shDIALUP
Open VPN
Software Client
Company LAN
Firewall
Allow outgoing TCP connections
on port 1194 (optional 443, 80)
myREX24 V2
Firewall
Company LAN
All outgoing TCP connections
on port 1194 (optional 443, 80)

The machine side is connected to the Internet in the same way. Using the WAN interface, the REX router is connected to the customer’s router network, establishing a VPN connection to the portal through it. Alternatively, routers are also available that can log in over a mobile connection (3G, LTE).

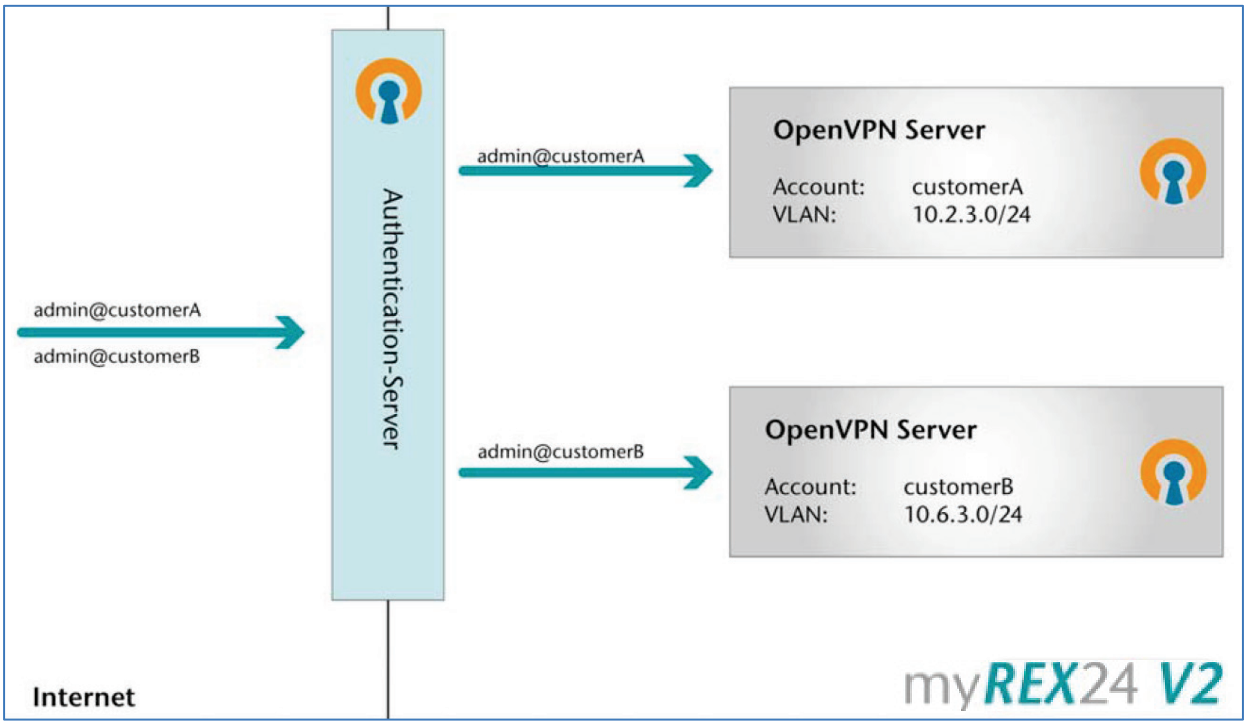
The machine network is connected via the LAN interface of the REX router. The VPN tunnel allows access to all devices in the network of machines of the REX router on the LAN side.

Remote maintenance side

The programmer / remote maintenance technician establishes a connection to the portal server via an outbound TCP connection on TCP port 1194 (optionally port 443 or 80) using the software shDIALUP. For this, the port used for outbound connections must be open in the local firewall and the corporate firewall.

Likewise, a connection is possible through an HTTP proxy; for this, the HTTP CONNECT method and a connection via the above-mentioned ports must be permitted by the proxy.

Based on the account name, the authentication server determines the OpenVPN server to which the request must be forwarded. Forwarding is then performed by the routing function of the portal server.



The actual connection and negotiation of security parameters occurs with the OpenVPN server of the account and not with the authentication server.

After successfully connecting to the portal, the shDIALUP network adapter obtains its IP address via DHCP for the virtual network of the OpenVPN server of the account.

The shDIALUP software now enters the routes for the VPN network in the local route table and launches the portal overview page.

In the overview, the programmer sees which of his REX routers have already established a connection to the portal. He clicks the “Connect” button, causing the entered routes of the machine network to be queried from the portal server and forwarded to the shDIALUP software, which enters the routes in the routing table of the PC.

The establishment of the connection is now complete.

Machine side

The connection is established in the same manner as on the programmer's side. OpenVPN is permanently implemented in the firmware of the router. The port for the outgoing connection can be permanently predefined (1194, 443, 80).

The Internet connection can be realized through the network of the end customer or through a mobile wireless connection. The address of the portal is permanently stored in the configuration.

A major difference on the machine side arises from the possibility of triggering the establishment of the connection to the portal individually as needed. This is useful when the VPN tunnel to the portal is not intended to be permanently maintained. Depending on the device model, different ways of triggering the establishment of the connection are available:

- Digital inputs
- Dialout button
- SMS

Access rights in the account

Users and clients with extensive access rights can be administered in the account. Access to the router can be regulated device, project or client-based.

It is also possible to regulate the access rights to components in the LAN network (control systems, panels, PCs) at the user level. A VPN connection with the machine can then be limited to certain devices.

Configuration of routers

The configuration of the router is carried out in the myREX24 V2 portal and can be transmitted through different paths to the device. In addition to transfer of the configuration file via USB stick or by way of a local LAN connection, the configuration can also be updated via an existing VPN connection.

The devices are uniquely identified by their serial number. For the initial configuration, the OpenVPN access data are transferred. Changing the configuration is subsequently only possible with the appropriately signed configuration records. Reading out or decoding of the configurations is thus no longer possible following the initial configuration.

Secured web access

Access to the website of the myREX24 V2 portal is now only possible via the HTTPS-encoded connection. The "v2.myrex24.net" website is secured with a certificate that is also tested by the shDIALUP software.

Firmware updates

The router firmware can be updated via USB stick or by way of an existing VPN connection from the portal. The firmware update files are encoded and only correctly signed firmware files are accepted for the update.

Data storage

The data administered and collected by the portal is found in the portal's own SQL database. The data is separated strictly by account.

As an option, the connection of an external SQL database for the protocolled data points of the routers or of the machines is possible, or the realization of a completely autarkically running portal server ("myREX24 virtual server").

Access to the myREX24 portal by Helmholz employees (data protection)

In the back end of the myREX24 V2 portal, new accounts can be created, deleted, the account options administered, users deleted, or passwords reset.

For purposes of customer support, technical managing directors, support staff and portal developers from Helmholz, as well as 2 external developers have access to the back end of the myREX24 V2 portal.

Access by external developers is controlled by Helmholz and is activated and blocked as needed.

All persons having access to the back end of the myREX24 portal (internal or external) are obligated to secrecy by accessory or bilateral non-disclosure agreements.

If access to the myREX24 portal by Helmholz employees or by external developers conflicts with your data protection regulations, the myREX24 portal software can also be hosted on a server provided by Helmholz (in-house or with a host of your choice).

On an own server, only you have access to the back end and can disable access by Helmholz when you require no support. You can also carry out the loading of patches and updates. Should you require support, access to the back end through software, such as TeamViewer is possible. You then have control over the work of our support staff.

Your end customer can also operate their own myREX24 V2 portal, which can be operated self-contained independently of Helmholz following commissioning.

Should you be interested in your own server solution, please contact us and ask about the "myREX24 virtual server".

Hosting of the myREX24 portal

The myREX24 portal is redundantly hosted in a European high security data center and constantly replicated to a standby server. A monitoring system monitors operation. The databases of the myREX24 portal are also secured cyclically.

myREX24 V2 security features

- Based on open source standard “OpenVPN”
- Authentication of the server by X.509 certificate (RSA 1024-bit)
- Client authentication by user name/password
- Password rules for user authentication can be set
- 2-factor authentication methods (SMS, e-mail, telephone call, Google authentication)
- Random 15-digit password for each REX OpenVPN router (can be changed)
- Diffie-Hellman key exchange with 1024-bit
- OpenVPN transmission encryption with OpenSSL (TLS 1.0), Blowfish CBC (128-bit), SHA1
- Only HTTPS access to the web front end of the portal is possible
- A separate OpenVPN server is assigned to each account (allocation via account name)
- REX routers are hard-connected with one account in the initial configuration
- Hosted in a high security data center of a European hoster:
    - PCI-DSS certification
    - Certification according to ISO/IEC 27001
    - Certification according to SOC 1 TYPE II and SOC 2 TYPE II
    - Redundant hosting (up to 99.5% availability)
- Separation of business and machine network in the REX router with internal firewall
- User and rights management system in the portal
- Extensive reporting (connection history, configuration changes, activity protocol)
- “myREX24 virtual server” for independent, autonomous and stand-alone operation
- Constant security updates of the portal software
- Rapid response when security vulnerabilities are reported

Additional 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” & “Fernwartung im industriellen Umfeld”

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

Changes and errors are excepted in regard to all information. Our General Terms and Conditions also apply. These can be found at www.helmholz.de.

Version: 23.05.2017