funkwerk
enterprise communications

Read Me
System Software 7.4.1 PATCH 9

This version of our system software is available for the following gateways:

- **X1000 II**
- **X1200 II**
- **X2300 Series**
- **X2100**
- **X2404**
- **X4000 Series**
- **X8500**
- **VPN Series**

It contains the following changes:

1.1 New start mode for IPSec peers

(ID 5294)

In order to ensure that a tunnel is activated immediately after the gateway is switched on, a new parameter has been introduced for peer configuration. The ***IPSec*** ➜ ***Configure Peers*** ➜ ***APPEND/EDIT*** ➜ ***Peer specific Settings*** menu now offers a choice between ***Start Mode*** *Always Up* and ***Start Mode*** *On demand*. If ***Start Mode*** *Always Up* is selected, the gateway attempts to establish a tunnel as soon as booting is completed.

1.2 Support for Additional IPSec Licenses

Additional IPSec licenses have been introduced that enable either 25 or 50 additional active tunnels. These licenses can be added up to the maximum number of tunnels supported by your device.

1.3 Trace - Support for IPSec Interfaces

(ID n/a)

The trace application now supports IPSec interfaces. source and destination IP filters can be used, the command syntax has not been changed.

1.4 RADIUS - Reload with two servers failed

(ID 6873)

If, when using two RADIUS servers, one was configured with reload interval (MIB variable ***RELOADINTERVAL*** in the MIB table ***RADIUSSERVERTABLE***) and the second without, no reload was carried out after changing from the server with reload interval to the server without reload interval.

The problem has been resolved.

1.5 IPSec - Dynamic peer not functional

(ID 7284)

If a dynamic peer was configured on a virtual interface, the configuration was not functional. A peer on a traffic list basis was functional.

The problem has been resolved.

1.6 Problems with the system after 194 days

(ID 7309)

It was still possible to log into the system after 194 days, but it was no longer possible to run commands and access the Setup Tool.

The problem has been resolved.

1.7 MS-CHAP Authentication error between Windows clients and router

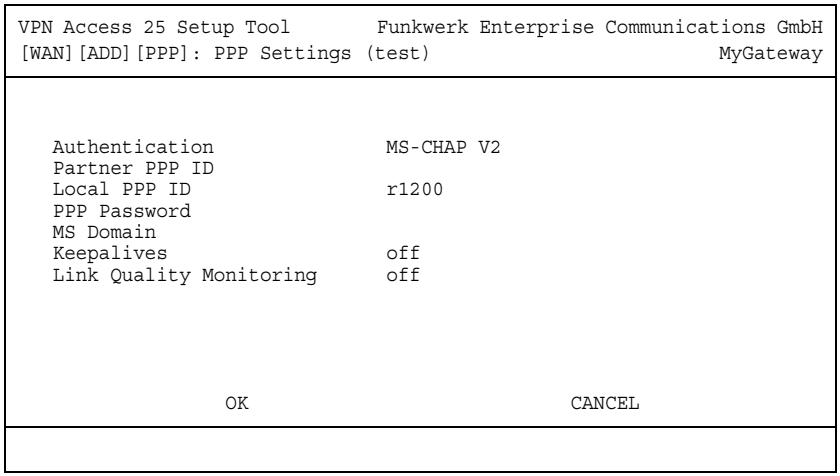
(ID 2318)

The authentication negotiation between Windows clients and the router sometimes failed for PPP or PPTP connections if the login name was used together with the domain name, for example, DEVELOPMENT\Developer.

The problem has been resolved.

In MS-CHAP V1 the entire identification name (domain and login name) is used for authentication.

In MS-CHAP V2 only the login name is used for authentication. The domain name is checked separately. To do so, the domain name must be entered in the new ***MS DOMAIN*** field. The field is only shown if ***AUTHENTICATION*** = *MS-CHAP*, *MS-CHAP V2* or *CHAP + PAP + MS-CHAP*.



1.8 HTTP - Black List Filter Introduced

ID n/a

In addition to the white list you can now also configure a web filter through a black list in the menu ***Security*** ➜ ***Cobion Orange Filter*** ➜ ***Configure Black List***.

1.9 Cobion Orange Filter – Path depth setting

VPN Access allows you to enter the maximum path depth for the Cobion Orange Filter when scanning a URL.

```
VPN Access 25 Setup Tool       Funkwerk Enterprise Communications GmbH
[SECURITY][ORANGE FILTER]: Static Settings                    MyGateway


        Admin Status        : disable
        Orange Filter Ticket: B1BT

        Ticket Status       :

        Filtered Interface  : none
        History Entries     : 64
        URL path depth      : 1

        Configure Black List >
        Configure White List >
        Configure Filters >
        View History >

                  SAVE                                  CANCEL
```

Use the ***URL PATH DEPTH*** field to enter the maximum path level accessed when checking a URL.

When you enter *0*, only the URL domain name is checked (e.g., *www.server.com*). This means that all pages on this Web server belong to the same category.

When *1* is entered, the first level of the URL path is scanned. For example, *www.server.com/info* and *www.server.com/games* are checked separately and can be assigned to two different categories.

The higher the setting, the longer it will take to load Internet pages because each URL has to be checked for multiple categories. If you enter a value that is too low, no distinctions are made between any categories of directories below the set depth. The actual classification on the Cobion filter servers is not affected by this, but the processing speed increases since the check is not made down to the maximum depth (32).

1.10 Setup Tool - Menu Extended Interface Settings not Displayed

(ID 3988)

The menu ***WAN Partner*** ➜ ***Advanced Settings*** ➜ ***Extended Interface Settings*** was not displayed. Some settings for a WAN Partner could, therefore not be made.

The problem has been resolved.

1.11 RIP - Triggered Update with Wrong Metric

(ID 7542)

A Triggered Update could contain routes with a metric of *0* which is not allowed.

The problem has been resolved.

1.12 OSPF - Only one IP Address Supported

(ID 7724)

If OSPF was activated in interface *1000* (*en1-0*), the propagation of more than one LAN route was not possible.

The problem has been resolved.

1.13 OSPF - Authentication with MD5 not Possible

(ID 2843)

Authentication with MD5 was not possible in OSPF.

The problem has been resolved.

1.14 IPSec - Time To Live Problems

(ID 7612, 7486)

Due to TTL values being changed when routing via an IPSec interface, there were unexpected traceroute and errors in RIP.

The problem has been resolved.

1.15 Setup Tool - Mistakable Formulation

(ID 3127)

If during a configuration in ***ATM*** ➜ ***OAM*** oder ***ATM QoS*** values were specified that had not been defined as a VCC in am ATM profile, the mistakable value *no VCC defined* was displayed for the field ***VIRTUAL CHANNEL CONNECTION (VCC)*** after leaving and reentering the menu.

The problem has been resolved.

1.16 ATM - Tracer Shows Wrong Message

(ID n/a)

For the deactivation of ATM F4/F5 OAM CC Cells a wrong message type was displayed in the tracer.

The problem has been resolved.

1.17 IPSec - Panic

(ID 8395, 8349, 7956, 7556, 7218, 7213, 7175, 7080, 7072)

After an error in the handlung of a peer state, the message 'improper state 5' (or similar) was sometimes printed to the console. A panic would follow. The error occurred with different peer states (***IPSECPEEROPERSTATUS***):

- awaiting_callback (33)

- ip_lookup (35)

- going_up (36)

- wait_if (37)

- wait_publish (38)

- wait_localip (39)

The problem has been resolved.

1.18 PPP - Link Status not Recognized

(ID n/a)

If for an arbitrary reason the layer 1 of a leased line was terminated, it could occur that the connection was still considered alive.

The problem has been resolved.

1.19 DNS - Interface not activated

(ID 7205)

A PPP interface specified for Domain Forwarding (***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS***) was not activated by DNS requests.

The problem has been solved

1.20 Multicast - Multicast Packets not Received

(ID 7048)

If a multicast connection is re-established after a connection failure, multicast packets are not forwarded to the network behind the gateway.

The problem has been solved

1.21 Scheduler - Malfunction

(ID n/a)

The scheduler treated MIB entries correctly only as long as they were not deleted (as e.g. dynamic entries usually are). Even if the same entry was recreated, the scheduler ignored it.

The problem has been solved

1.22 DNS - Stacktrace

(ID 7151)

Under certain circumstances, DNS requests could lead to a panic and a reboot of the gateway.

The problem has been solved

1.23 PPP - Incomplete CLID Check

(ID 6528)

Incomplete CLID checks could lead to calls being accepted even if the Calling Party Number was incorrect.

This problem has been solved.

1.24 IP - PPP Connection not Initialized

(ID 5522)

If an ETHoA connection was supposed to initiate a PPP dial connection, this did not take place.

The problem has been resolved.

1.25 PPP - Panic with Inband Authentication

(ID 6851)

With inband authentication there could be sporadic reboots.

The problem has been solved

1.26 PPP - Callback changes

(ID n /a)

If either *yes (PPP negotiation)* or *yes (PPP negotiation, callback optional)* has been chosen for Callback, the Callback is carried out even if no Callback Control has been negotiated - provided that an MSN has been specified for the Callback.

1.27 SIF - TFTP Transfer Failed

(ID 6366)

TFTP file transfers could fail due to a malfunction of the SIF.

This problem has been solved.

1.28 System Reboot

(ID n/a)

During connection establishment, there could be a gateway reboot.

This problem has been solved.

1.29 PPP - Connection Failed

(ID 6099)

Connections to remote side gateways that do not completely comply with the relevant RFCs failed because of incompatible IPCP behavior.

This problem has been solved.

1.30 TACACS+ - Privilege Level Conflict

(ID 6358)

Due to a conflict between the privilege level configuration of the gateway and that of the TACACS+ server, specific permission levels could not be accessed properly.

This problem has been solved by making ***PRIVLVLONLOGIN*** in the ***TACACSPSERVERTABLE*** configurable.

1.31 Restoring the IPSec and X.25 licenses with Easy Licensing failed

(ID 5447)

Easy Licensing did not restore all licenses contained on the device at the time of delivery. The licenses for IPSec and X.25 were missing.

The problem has been resolved.

1.32 PPP - Panic During Leased Line Configuration

(ID 5778)

During the configuration of the IP settings of a leased line WAN Partner, there were occasional panics.

This problem has been solved.

1.33 IPSec - Unnecessary Rekeying

(ID n/a)

If for a Phase 2 Lifetime a limit in kilobytes was specified, rekeying could take place without that value having been reached.

This problem has been solved.