funkwerk
enterprise communications

Read Me
Systemsoftware 7.4.1 PATCH 9

Diese Version unserer Systemsoftware ist für folgende Gateways verfügbar:

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

Sie enthält folgende Änderungen:

1.1 Neuer Start Mode für IPSec Peers

Um sicher zu stellen, dass ein Tunnel unmittelbar nach den Einschalten des Gateways aktiviert wird, ist für die Peer-Konfiguration ein neuer Parameter eingeführt worden. Das Menü ***IPSec*** ➜ ***Configure Peers*** ➜ ***APPEND/EDIT*** ➜ ***Peer specific Settings*** erlaubt jetzt die Auswahl zwischen dem ***Start Mode*** *Always Up* und dem ***Start Mode*** *On demand.* Wird ***Start Mode*** *Always Up* gewählt, versucht das Gateway, einen Tunnel sofort nach Beendigung des Bootvorgangs herzustellen.

1.2 Unterstützung zusätzlicher IPSec-Lizenzen

Es stehen nun zusätzliche IPSec-Lizenzen zur Verfügung, die entweder 25 oder 50 zusätzliche aktive Tunnel ermöglichen. Sie können zur maximal vom Gerät unterstützen Anzahl an Tunneln aufaddiert werden.

1.3 Trace - Unterstützung von IPSec Interfaces

(ID n/a)

Die Trace-Applikation unterstützt nun IPSec Interfaces. Dabei können Source- oder Destination-IP-Filter verwendet werden. Die Syntax für den Trace-Befehl ist unverändert.

1.4 RADIUS - Reload mit zwei Servern fehlgeschlagen

(ID 6873)

Wenn bei zwei RADIUS Servern der eine mit Reload Intervall (MIB-Variable ***RELOADINTERVAL*** in der MIB-Tabelle ***RADIUSSERVERTABLE***) konfiguriert wurde und der zweite ohne, so wurde beim Wechsel vom Server mit Reload Intervall zum Server ohne Reload Intervall keine Reload mehr durchgeführt.

Das Problem ist gelöst worden.

1.5 IPSec - Dynamischer Peer nicht funktionsfähig

(ID 7284)

Wenn ein Dynamischer Peer auf einem virtuellen Interface konfiguriert wurde, war die Konfiguration nicht funktionsfähig. Ein Peer auf Basis von Traffic-Listen war funktionsfähig.

Das Problem ist gelöst worden.

1.6 Probleme mit dem System nach 194 Tagen

(ID 7309)

Nach 194 Tagen konnte man sich auf dem System zwar weiterhin einloggen, aber keine Kommandos ausführen und das Setup Tool nicht aufrufen.

Das Problem ist gelöst worden.

1.7 MS-CHAP Authentifizierungsfehler zwischen Windows-Clients und Router

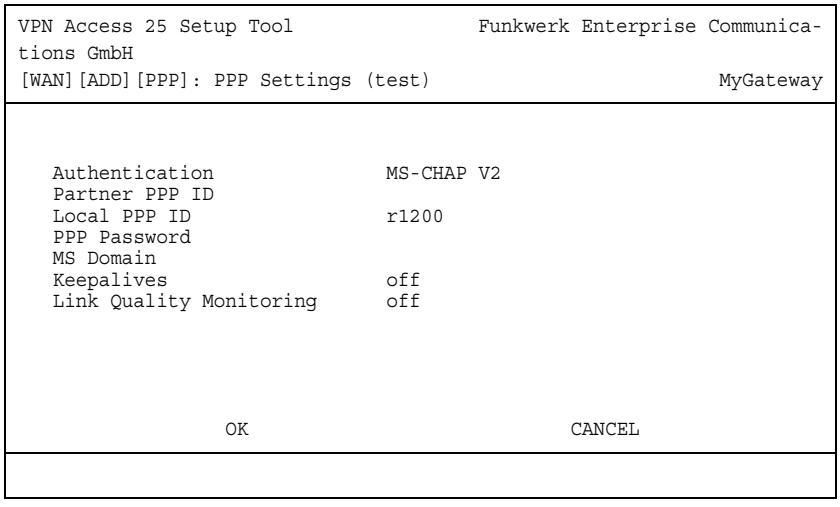
(ID 2318)

Die Authentifizierungsverhandlung zwischen Windows-Clients und dem Router konnte bei PPP- oder PPTP-Verbindungen fehlschlagen, wenn der Login-Name zusammen mit dem Domänennamen verwendet wurde, z. B. DEVELOPMENT\Developer.

Das Problem ist gelöst worden.

Bei MS-CHAP V1 wird der ganze Identifikationsname (Domänenname und Login-Name) für die Authentifizierung verwendet.

Bei MS-CHAP V2 wird nur der Login-Name für die Authentifizierung verwendet. Der Domänenname wird separat überprüft. Dazu ist der Domänenname ggf. in das neue Feld ***MS DOMAIN*** einzugeben. Das Feld wird nur angezeigt, wenn ***AUTHENTICATION*** = *MS-CHAP*, *MS-CHAP V2* oder *CHAP* + *PAP* + *MS-CHAP*.



1.8 HTTP - Black-List-Filter eingeführt

(ID n/a)

Zusätzlich zur White List ist nun auch die Konfiguration eines Web-Filters über eine Black List im Menü ***Security*** ➜ ***Cobion Orange Filter*** ➜ ***Configure Black List*** möglich.

1.9 Cobion Orange Filter - Eingabe der Pfadtiefe

Mit VPN Access können Sie angeben, bis zu welcher Pfadtiefe eine URL durch den Cobion Orange Filter überprüft werden soll.

```
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
```

Im Feld ***URL PATH DEPTH*** geben Sie an, bis auf welche Ebene der Pfad einer URL geprüft werden soll.

Wird *0* eingegeben, wird nur der URL-Domänenname geprüft, z. B. *www.server.com*. Somit sind alle Seiten dieses Webservers in einer Kategorie.

Wenn Sie *1* eingeben, wird die erste Ebene des URL-Pfades geprüft. So werden z.B. *www.server.com/info* und *www.server.com/games* separat geprüft und könnten in zwei verschiedene Kategorien eingeordnet werden.

Je höher der Wert ist, den Sie hier eingeben, desto länger kann das Laden von Webseiten dauern, da jede URL in verschiedenen Kategorien geprüft werden muss. Ist der Wert zu niedrig gewählt, werden eventuell vorhandene Kategorisierungen von Verzeichnissen unterhalb der eingestellten Tiefe nicht mehr unterschieden. Die tatsächliche Kategorisierung auf den Cobion Filter Servern wird dadurch nicht beeinflusst, sondern nur zu Gunsten der Geschwindigkeit nicht bis zur maximalen Tiefe (32) ausgewertet.

1.10 Setup Tool - Menü Extended Interface Settings nicht angezeigt

(ID 3988)

Das Menü ***WAN Partner → Advanced Settings → Extended Interface Settings*** wurde nicht angezeigt. Daher konnten einige Einstellungen an einem WAN PArtner nicht vorgenommen werden.

Das Problem ist gelöst worden.

1.11 RIP - Triggered Update mit falscher Metrik

(ID 7542)

Ein Triggered Update konnte Routen mit der nicht erlaubten Metrik *0* enthalten.

Das Problem ist gelöst worden.

1.12 OSPF - Nur eine IP-Adresse unterstützt

(ID 7724)

Wenn auf dem Interface *1000* (*en1-0*) OSPF aktiviert wird, wird die Veröffentlichung von mehr als einer LAN-Route unterbunden.

Das Problem ist gelöst worden.

1.13 OSPF - Authentisierung mit MD5 nicht möglich

(ID 2843)

Die Authentisierung mittels MD5 war im OSPF nicht möglich.

Das Problem ist gelöst worden.

1.14 IPSec - Time-To-Live-Probleme

(ID 7612, 7486)

Aufgrund der Veränderung der TTL-Werte beim Routing über ein IPSec Interface konnte es zu unerwarteten Traceroute-Ergebnissen und zu Fehlern beim RIP kommen.

Die Probleme sind gelöst worden.

1.15 Setup Tool - Missverständliche Formulierung

(ID 3127)

Wenn bei der Konfiguration von ***ATM*** → ***OAM*** oder ***ATM QoS*** Werte eingestellt wurden, die noch nicht in einem ATM-Profil als VCC definiert waren, wurde nach Verlassen des Menüs bei einem erneuten Öffnen für das Feld ***Virtual Channel Connection (VCC)*** der missverständliche Wert *no VCC defined* ausgegeben.

Das Problem ist gelöst worden.

1.16 ATM - Tracer zeigt falsche Meldungen

(ID n/a)

Für die Deaktivierung von ATM F4/F5 OAM CC Cells wurde ein falscher Meldungstyp im Tracer angezeigt.

Das Problem ist gelöst worden.

1.17 IPSec - Panic

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

Nach einem Fehler in der Behandlung des Peer-Status kam es auf der Konsole zu Fehlermeldungen wie "improper state 5" und zu einem Neustart des Gateways. Der Fehler konnte mit unterschiedlichen Peer-Status (***IPSECPEEROPERSTATUS***) auftreten:

- awaiting_callback (33)

- ip_lookup (35)

- going_up (36)

- wait_if (37)

- wait_publish (38)

- wait_localip (39)

Das Problem ist gelöst worden.

1.18 PPP - Link-Status nicht erkannt

(ID n/a)

Wenn aus einem beliebigen Grund der Layer 1 einer Festverbindung abbrach, konnte es vorkommen, dass die Verbindung weiterhin als aktiv betrachtet wurde.

Das Problem ist gelöst worden.

1.19 DNS - Schnittstelle nicht aktiviert

(ID 7205)

Durch eine DNS-Anfrage wurde ein dafür im Domain Forwarding (***IP*** ➜ ***DNS*** ➜ ***FORWARDED DOMAINS***) vorgesehenes PPP Interface nicht aktiviert.

Das Problem ist gelöst worden.

1.20 Multicast - Kein Empfang von Multicast-Paketen

(ID 7048)

Wenn nach einer Unterbrechung der Verbindung, die Multicast-Verbindung wieder hergestellt wird, werden Multicast-Pakete nicht in das Netzwerk hinter dem Gateway weitergeleitet.

Das Problem ist gelöst worden.

1.21 Scheduler - Fehlfunktion

(ID n/a)

Der Scheduler bearbeitete Einträge in der MIB nur solange korrekt, wie diese nicht gelöscht wurden (wie z. B. bei dynamischen Einträgen der Fall). Wenn der gleiche Eintrag erneut erstellt wurde, wurde er nicht beachtet.

Das Problem ist gelöst worden.

1.22 DNS - Stacktrace

(ID 7151)

Unter bestimmten Umständen konnten DNS-Anfragen zu einem Stacktrace (mit Neustart des Gateways) führen.

Das Problem ist gelöst worden.

1.23 PPP - Unvollständige CLID-Überprüfung

(ID 6528)

Unvollständige CLID-Überprüfung konnte dazu führen, dass Rufe auch dann angenommen wurden, wenn die Calling Party Number falsch war.

Das Problem ist gelöst worden.

1.24 IP - PPP-Verbindung nicht initiiert

(ID 5522)

Wenn eine ETHoA-Verbindung eine PPP-Wählverbindung auslösen sollte, geschah dies nicht.

Dieses Problem ist gelöst worden.

1.25 PPP - Panic bei Inband-Authentifizierung

(ID 6851)

Bei einer Inband-Authentifizierung konnte es zu sporadischen Neustarts des Gateways kommen.

Das Problem ist gelöst worden.

1.26 PPP - Änderung im Callback

(ID 6659)

Wenn für einen Callback entweder *yes (PPP negotiation)* oder *yes (PPP negotiation, callback optional)* ausgewählt ist, wird der Callback auch dann

ausgeführt, wenn keine Callback Control ausgehandelt worden ist, sofern eine MSN für den Callback konfiguriert ist.

1.27 SIF - TFTP-Transfer fehlgeschlagen

(ID 6366)

TFTP-Dateitransfers konnten aufgrund eines Fehlers in der SIF fehlschlagen.

Das Problem ist gelöst worden.

1.28 System Neustart

(ID n/a)

Während eines Rufaufbaus konnte es zu einem Systemneustart kommen.

Das Problem ist gelöst worden.

1.29 PPP - Verbindungsaufbau fehlgeschlagen

(ID 6099)

Verbindungsaufbauten mit Gegenstellen, die sich nicht vollständig RFC-konform verhalten, schlugen aufgrund von Inkompatibilität im IPCP fehl.

Das Problem ist gelöst worden.

1.30 TACACS+ - Privilege-Level-Konflikt

(ID 6358)

Aufgrund eines Konfliktes zwischen der Privilege-Level-Konfiguration des Gateways und des TACACS+ Servers, konnten bestimmte Berechtigungsebenen nicht korrekt erreicht werden.

Das Problem ist gelöst worden, indem in der ***tacacspServerTable*** die Variable ***PrivLvlOnLogin*** konfigurierbar gemacht worden ist.

1.31 Wiederherstellen der IPSec und X.25 Lizenzen mit Easy Licensing fehlgeschlagen

(ID 5447)

Mit Easy Licensing wurden nicht alle Lizenzen wiederhergestellt, die im Auslieferungszustand auf dem Gerät vorhanden waren. Es fehlten die Lizenzen für IPSec und X.25.

Das Problem ist gelöst worden.

1.32 PPP - Panic bei Konfiguration einer Standleitung

(ID 5778)

Bei der IP-Konfiguration eines WAN Partners für Standleitungen konnte es zu einer Panic kommen.

Das Problem ist gelöst worden.

1.33 IPSec - Unnötiges Rekeying

(ID n/a)

Wenn für eine Phase-2-Lifetime eine Grenze in Kilobytes angegeben war, fand auch dann ein Rekeying statt, wenn der Wert noch nicht erreicht war.

Das Problem ist gelöst worden.