VPN Access 250, VPN Access 1000, X8500

Release Notes
Systemsoftware 7.9.1

Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.9.1**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Funkwerk Enterprise Communications GmbH haftet nur im Umfang ihrer Verkaufs- und Lieferbedingungen und übernimmt keine Gewähr für technische Ungenauigkeiten und/oder Auslassungen.

Die Informationen in diesem Dokument können ohne Ankündigung geändert werden. Zusätzliche Informationen sowie Änderungen finden Sie unter www.funkwerk-ec.com.

Als Multiprotokoll-Gateways bauen Bintec-Gateways in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Funkwerk Enterprise Communications GmbH übernimmt keine Verantwortung für Datenverlust, ungewollte Verbindungskosten und Schäden, die durch den unbeaufsichtigten Betrieb des Produkts entstanden sind.

Marken

Bintec und das Bintec-Logo sind eingetragene Warenzeichen der Funkwerk Enterprise Communications GmbH.

Erwähnte Firmen- und Produktnamen sind in der Regel Warenzeichen der entsprechenden Firmen bzw. Hersteller.

Copyright

Richtlinien und Normen

Bintec-Gateways entsprechen folgenden Richtlinien und Normen:

R&TTE-Richtlinie 1999/5/EC

CE-Zeichen für alle EU-Länder

Weitere Informationen finden Sie in den Konformitätserklärungen unter www.funkwerk-ec.com.

Wie Sie Funkwerk Enterprise Communications GmbH erreichen

Funkwerk Enterprise Communications GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.funkwerk-ec.com

Funkwerk Enterprise Communications
6 Avenue de la Grande Lande - CS 20102
33173 Gradignan cedex
France

Telephone: +33 (0)1 61 37 32 76
Fax: +33 (0)1 61 38 15 51
Internet: www.funkwerk-ec.com

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.9.1 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Systemsoftware 7.9.1 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **VPN Access 250**
- **VPN Access 1000**
- **X8500**.

1.2 Inkompatibilität

Konfigurationen, die unter **Systemsoftware 7.9.1** erstellt oder gesichert werden, sind unter Umständen zu einigen Versionen unserer Systemsoftware inkompatibel.

Beachten Sie dennoch die folgenden Hinweise zum Update und zu den Möglichkeiten eines Downgrades.

1.2.1 Vorbereitung und Update

Gehen Sie ggf. folgendemaßen vor, um ein Update auf **Systemsoftware 7.9.1** vorzubereiten und durchzuführen:

1. Sichern Sie die aktuelle Boot-Konfiguration. Verwenden Sie eine der folgenden Möglichkeiten:
   a) Geben Sie auf der SNMP Shell `cmd=save path=boot.alt` ein. Dies sichert die aktuelle Boot-Konfiguration im Flash ROM Ihres Gateways unter

dem Namen "boot.alt".
b) Starten Sie auf einem Rechner in Ihrem LAN einen TFTP-Server und exportieren Sie die aktuelle Boot-Konfiguration über das Menü ***CONFIGURATION MANAGEMENT*** des Setup Tools. Wählen Sie dazu:

- ***OPERATION*** = *put (FLASH -> TFTP)*
- ***TFTP SERVER IP ADDRESS*** = *<IP-Adresse des TFTP Servers im LAN>*
- ***TFTP FILE NAME*** = *boot.alt*
- ***NAME IN FLASH*** = *boot*

2. Führen Sie das Update auf **Systemsoftware 7.9.1** wie gewohnt durch und starten Sie das Gateway neu.
   Das Gateway startet mit der neuen Software, die bestehende Boot-Konfiguration wird verwendet.

1.2.2 Downgrade

Wenn Sie ein Downgrade durchführen wollen, gehen Sie folgendermaßen vor:

1. Ersetzen Sie die aktuelle Boot-Konfiguration mit der zuvor gesicherten. Verwenden Sie eine der folgenden Möglichkeiten:
   a) Geben Sie auf der SNMP Shell `cmd=move path=boot.alt pathnew=boot` ein. Dies überschreibt die aktuelle Boot-Konfiguration mit der zuvor gesicherten. Die "boot.alt" genannte Konfiguration wird dabei aus dem Flash ROM gelöscht (wenn Sie diese im Flash erhalten wollen, verwenden Sie `cmd=copy` anstelle von `cmd=move`).
   b) Starten Sie auf einem Rechner in Ihrem LAN einen TFTP-Server und importieren Sie die zuvor gesicherte Konfiguration über das Menü ***CONFIGURATION MANAGEMENT*** des Setup Tools. Wählen Sie dazu:
   - ***OPERATION*** = get (TFTP -> FLASH)
   - ***TFTP SERVER IP ADDRESS*** = *<IP-Adresse des TFTP Servers im LAN>*
   - ***TFTP FILE NAME*** = *boot.alt*
   - ***NAME IN FLASH*** = *boot*
2. Führen Sie das Downgrade auf die gewünschte Softwareversion durch.
3. Rebooten Sie das Gateway. Es startet nun mit der zuvor gesicherten Boot-Konfiguration und der älteren Version der Systemsoftware.

2 Neue Funktionen

Systemsoftware 7.9.1 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.8.7 erheblich erweitern:

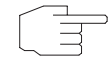
2.1 Zeitzonenwahl für automatische Zeitumstellung

Ab Systemsoftware 7.9.1 erfolgt auf Ihrem Gerät die Umstellung von Sommer- auf Normalzeit im Herbst und von Normal- auf Sommerzeit im Frühling am jeweiligen Umschalttag automatisch.

Im Setup Tool Menü ***System*** ➜ ***Time and Date*** können Sie im neuen Feld ***System Time Zone*** die gewünschte Zeitzone für Ihr System wählen (z. B. *Europe*/*Berlin*). Wenn für die gewählte Zeitzone Sommer- und Normalzeit festgelegt sind, erfolgt die Zeitumstellung am Umschalttag automatisch.

Hinweis

Beachten Sie, dass die automatische Zeitumstellung unerwünschte Auswirkungen auf Ereignisse haben kann, die im Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** konfiguriert sind.



Hinweis

Beachten Sie, dass die automatische Zeitumstellung bei der Umschaltung von Sommer- auf Normalzeit dazu führen kann, dass bei aufgezeichneten Ereignissen Zeitstempel doppelt auftreten.

2.2 ISAKMP Configuration Method (IKE Config Mode) im Client Modus

Mit Hilfe der ISAKMP Configuration Method (kurz IKE Config Mode) können Sie einen mobilen PC-Arbeitsplatz (bintec Secure IPSec Client) über IPSec an die Firmenzentrale anbinden.

Die IP-Adresse und auf Wunsch weitere Daten wie Domänen- und Serverparameter für DNS und WINS werden dem Client vom IPSec Gateway auf Anfrage zur Verfügung gestellt. Diese Methode ermöglicht die Zuteilung einer dynamischen IP-Adresse z. B. aus dem internen Adressbereich der Firmenzentrale (siehe Release Notes 7.8.7).

Ab **Systemsoftware 7.9.1** können Sie Ihr Gerät nicht nur wie bisher als Server sondern auch als Client für den IKE Config Mode konfigurieren; bisher konnten Sie als Client z. B. einen NCP Secure Client verwenden.

Um Ihr Gerät als Client für den IKE Config Mode zu konfigurieren, wählen Sie ***IPSec*** ➜ ***Configure Peers*** ➜ **EDIT** ➜ ***Interface IP Settings*** ➜ ***Basic IP-Settings*** und setzen Sie ***IP Transit Network*** = *IKE Config Client Mode*.

2.3 Befehl cert get mit HTTPS

Ab Systemsoftware 7.9.1 ist der Befehl *cert get* **zum Import von Zertifikaten über HTTPS verfügbar.**

2.4 Scheduler - Platzhalter für Seriennummer verfügbar

Mit Systemsoftware 7.9.1 können Sie im Scheduler in Befehlen die Zeichenfolge SN als Platzhalter für die Seriennummer benutzen.

Sie können z. B. im Setup Tool Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** ➜ **ADD** das Feld ***Set value active*** = *get_all;http://10.9.1.2/tftp:file SN.cf* setzen, um die Konfigurationsdateien mehrerer Gateways zu holen.

2.5 DynDNS Provider www.dnsexit.com verfügbar

Mit Systemsoftware 7.9.1 ist der DynDNS Provider www.dnsexit.com verfügbar.

2.6 IPSec - Mehrere Benutzer über denselben Peer

Ab Systemsoftware 7.9.1 kann ein IPSec-Peer so konfiguriert werden, dass sich mehrere Benutzer über diesen IPSec-Peer einwählen können.

Wählen Sie dazu das Setup Tool Menü ***IPSec*** ➜ ***Configure Peers*** ➜ **EDIT** ➜ **Peer specific Settings** und setzen Sie ***Special Peer Type*** = *Dynamic Client* Wir empfehlen Ihnen zusätzlich im Menü ***IPSec*** ➜ ***Configure Peers*** ➜ **EDIT** ➜ ***Interface IP Settings*** ➜ ***Basic IP-Settings*** das Feld ***IP Transit Network*** = *IKE Config Server Mode* zu setzen.

2.7 Setup Tool - ISDN Statistik

Ab Systemsoftware 7.9.1 ist im Setup Tool Menü *MONITORING AND DEBUGGING* ➜ *ISDN MONITOR* über den Befehl *S* die Statistik auch für beendete Anrufe verfügbar und nicht wie bisher nur für aktuelle Anrufe.

2.8 Neue MIB-Variable HttpRedirect

Mit Systemsoftware 7.9.1 ist in der MIB-Tabelle *IPEXTIFTABLE* die neue MIB-Variable *HTTPREDIRECT* verfügbar.

Mit der Variablen ***HTTPREDIRECT*** können Sie HTTP-Anfragen auf einer Schnittstelle entweder mit dem Wert *local* auf den lokalen HTTP Dämon oder mit dem Wert *proxy* auf den lokalen Content Filter umleiten.

3 Änderungen

Folgende Änderungen sind in Systemsoftware 7.9.1 vorgenommen worden, um Leistung und Bedienbarkeit zu verbessern:

3.1 Java SNMP Browser entfernt

Ab **Systemsoftware 7.9.1** ist der Java SNMP Browser entfernt.

3.2 Funktionalität Credits entfernt

Ab **Systemsoftware 7.9.1** ist die Funktionalität Credits entfernt.

3.3 Preshared Keys - Warnung hinzugefügt

Folgende Warnung wurde in **Systemsoftware 7.9.1** hinzugefügt, um den Benutzer aufzufordern, die Standardeinstellung des Preshared Key zu ändern: "Ändern Sie unbedingt den Standard Preshared Key! Solange der Key nicht geändert wurde, ist ihr Gerät nicht gegen einen unautorisierten Zugriff geschützt!"

3.4 SIF Alias Namen für Schnittstellen geändert

Ab **Systemsoftware 7.9.1** sind die SIF Alias Namen für Schnittstellen verbessert, um Missverständnissen vorzubeugen. Es kann jetzt zwischen folgenden Kategorien unterschieden werden: LAN, WLAN, IPSec, Leased, Bundle und Bridge. Beispielsweise heißt die bisherige Schnittstelle *LAN_PEER_2_R4100_1* ab sofort *IPSEC_PEER_2_R4100_1*.

3.5 Setup Tool - QoS - Wertebereich vergrößert

Im Setup Tool Menü ***QoS*** ➜ ***Interfaces and Policies*** ➜ **Edit** ➜ ***QoS Scheduling and Shaping*** wird mit der Einstellung ***Queueing and Scheduling Algorithm*** = *priority queueing (PQ)* und ***Specify Traffic Shaping*** = ***yes*** das Feld ***Maximum Transmit Rate (Bits per Second)*** angezeigt. Der Wertebereich dieses Feldes wurde von *100000000* auf *1000000000* vergrößert.

3.6 Bei ausgehenden Rufen der eigenen Rufnummer Parameter mitgeben

Um bei ausgehenden Rufen der eigenen Rufnummer bestimmte Parameter nach Q.931 "mitgeben" zu können, kann in der MIB-Tabelle ***biboDialTable*** die MIB-Variable ***Screening*** auch für ausgehende Rufe verwendet werden. Darüber hinaus steht für diesen Zweck die neue MIB-Variable ***TypeOfLocalNumber*** zur Verfügung.

4 Gelöste Probleme

Die folgenden Probleme sind in Systemsoftware 7.9.1 gelöst worden:

4.1 Setup Tool - Stacktrace wegen Speicherverlust

(ID n/a)

Clients mit falschem Preshared Key versuchten sich immer wieder zu verbinden und verursachten daher einen Stacktrace wegen Speicherverlust.

Das Problem ist gelöst.

4.2 Setup Tool - Stacktrace wegen falscher Lifetime Policy

(ID 12531)

Wenn im Setup Tool bei Konfiguration von IPSec bei einer Eingabe im Feld ***LIFETIME POLICY*** der vorgegebene Wertebereich von *0 .. 4294967295* überschritten wurde, folgte ein Stacktrace. Dabei machte es keinen Unterschied, ob die Eingabe in Sekunden oder in KByte erfolgte.

Das Problem ist gelöst.

4.3 PIM - Stacktrace

(ID n/a)

Beim Herunterfahren von PIM trat ein Stacktrace auf, wenn die entsprechende Schnittstelle nicht verfügbar war.

Das Problem ist gelöst.

4.4 PPP-Verbindungen fehlgeschlagen

(ID 11303)

In seltenen Fällen konnte es dazu kommen, dass der Aufbau einer PPP-Verbindung scheiterte und das Interface blockierte, bis es manuell zurückgesetzt oder neu gestartet wurde.

Das Problem ist gelöst.

4.5 IPSec - Probleme beim Aufbau der Phase 2

(ID 12163)

Beim Aufbau der Phase 2 einer IPSec-Verbindung konnte es zu Problemen aufgrund der Auswahl der Quelladresse kommen.

Das Problem ist gelöst.

4.6 IPSec - trace zeigte UDP Pakete nicht an

(ID 12455)

Bei einem trace eines IPSec Tunnels wurden die Datenpakete nicht angezeigt, die vom Router mit hoher Priorität gesendet wurden.

Das Problem ist gelöst.

4.7 IPSec - IKE Config Mode - Eintrag in MIB-Tabelle ipDynaAddrTable falsch

(ID 12471)

Im IKE Config Mode enthielt die MIB-Tabelle ***ipDynaAddrTable*** den Eintrag ***ifIndex*** = *10001* (an Stelle von ***ifIndex*** = *100002* für den IPSec Peer).

Das Problem ist gelöst.

4.8 IPSec - Keine Verbindung mit Zertifikat

(ID 11313)

Mit IPSec konnte über RADIUS keine Verbindung aufgebaut werden, wenn ein Zertifikat benutzt wurde, in welchem der Parameter User-Name eine Länge von 64 Zeichen überschritt.

Das Problem ist gelöst.

4.9 Speichern der Konfiguration fehlgeschlagen

(ID 12251)

Es konnte vorkommen, dass bei wenig freiem Speicherplatz im Flash eine Boot-Konfiguration nicht korrekt gespeichert werden konnte und keine Fehlermeldung erschien.

Das Problem ist gelöst.

4.10 Multicast nicht funktionsfähig

(ID n/a)

Es konnte vorkommen, dass Multicast nicht funktionierte, weil es mehrmals aktiviert wurde.

Das Problem ist gelöst.

4.11 Multicast - Weiterleiten von Paketen fehlgeschlagen

(ID n/a)

In Szenarien mit Source Specific Multicast (SSM) schlug das Weiterleiten von Paketen fehl.

Das Problem ist gelöst.

4.12 Multicast auf IPSec-Schnittstellen fehlgeschlagen

(ID n/a)

Auf IPSec-Schnittstellen konnten keine Multicast-Pakete übertragen werden.

Das Problem ist gelöst.

4.13 Multicast - Timer Problem

(ID n/a)

Es konnte vorkommen, dass auf einer Schnittstelle sehr viele Queries und Reports versendet bzw. empfangen wurden.

Das Problem ist gelöst, die Timer sind angepasst worden.

4.14 RADIUS Reload funktionierte nicht

(ID n/a)

Ein nicht funktionierender RADIUS Dialout Reload verursachte eine Endlosschleife von Get Requests.

Das Problem ist gelöst.

4.15 Setup Tool - Scheduler - Falsches Intervall nach Änderung

(ID 12096)

Wenn im Setup Tool Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** ➜ **ADD** beispielsweise für das Feld ***Set value active*** = *1800* gesetzt wurde, während vorher *10* gesetzt war, so wurde nach Speicherung der Änderung noch einmal der Wert *10* verwendet und erst beim nächsten Mal *1800*.

Das Problem ist gelöst.

4.16 Setup Tool - Port 1 fälschlicherweise auf disabled gesetzt

(ID 12567)

Wenn bei einem Gerät im Auslieferungszustand das Setup Tool Menü ***Ethernet Switch*** ➜ ***Switch Configuration*** gewählt und mit **Save** verlassen wurde, wurde Port 1 auf disabled gesetzt und es gab keine Möglichkeit, dies zu ändern.

Das Problem ist gelöst.

4.17 Setup Tool - Standleitung - Fehler bei Auswahl der Timeslots

(ID 11323)

Wenn im Setup Tool Menü ***PRI2-4*** das Feld ***ISDN Switch Type*** = *leased line, chan. B1..B31* gesetzt ist und unter ***PRI2-4*** ➜ ***Bundle Confguration*** ➜ ***ADD*** das Feld ***Bundle Type*** = *PPP Multilink* gewählt ist, so sind in diesem Menü alle Timeslots standardmäßig gewählt, auch wenn sie mit **Save** gespeichert werden. Wenn ein Timeslot, z. B. Timeslot 11, aus der Auswahl entfernt wurde und der Cursor zum folgenden Timeslot bewegt wurde, waren alle Timeslots aus der Auswahl entfernt.

Das Problem ist gelöst.

4.18 Setup Tool - IPSec - Blockierte Verbindung

(ID 12115)

Wenn im Setup Tool Menü ***IPSEC*** ➜ ***CONFIGURE PEERS*** ➜ **APPEND** ➜ ***IPSEC CALLBACK*** die Felder ***ISDN CALLBACK*** = *both*, ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes* und ***MODE*** = *use B channel* gesetzt waren, traten Probleme mit Callback auf und es konnte unter Umständen keine Verbindung aufgebaut werden.

Das Problem ist gelöst.

4.19 Falsche Einträge in der MIB-Tabelle ipHostAccessClientTable

(ID n/a)

In der MIB-Tabelle ***IPHOSTACCESSCLIENTTABLE*** blieben nach einem Reboot versehentlich einige Einträge bestehen.

Das Problem ist gelöst, die Einträge werden bei einem Reboot gelöscht.