RELEASE NOTES SYSTEMSOFTWARE 7.4.2

Release Notes - Systemsoftware 7.4.2
Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.4.1/7.4.2**..

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

Bintec France
6/8 Avenue de la Grande Lande
F-33174 Gradignan
France

Telephone: +33 5 57 35 63 00
Fax: +33 5 56 89 14 05
Internet: www.funkwerk-ec.com

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.4.2 aufmerksam, um Probleme beim Update oder bei der Verwendung der Software zu vermeiden.

1.1 Gültigkeit

Systemsoftware 7.4.2 steht ausschließlich für folgende Geräte zur Verfügung und kann auf anderen Geräten nicht eingesetzt werden:

- **X2301**
- **X2302**
- **X2301w**
- **X2302w**
- **R232aw**
- **R232bw.**

Viele der hier beschriebene Funktionen finden sich für Geräte anderer Produktreihen in **Systemsoftware 7.4.1**.

1.2 Inkompatibilität

Konfigurationen, die unter **Systemsoftware 7.4.2** erstellt oder gesichert werden, sind zu Versionen unserer Systemsoftware vor **7.2.2** inkompatibel. Beachten Sie unbedingt 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 7.4.2** 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 7.4.2** wie gewohnt durch und starten Sie das Gateway neu.
   Das Gateway startet mit der neuen Software, die Boot-Konfiguration ist konvertiert und nicht mehr mit älteren Versionen der Systemsoftware kompatibel.

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 im-

portieren 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.

1 Wichtige Informationen

2 Neue Funktionen

Systemsoftware 7.4.2 enthält eine Reihe neuer Funktionen, die den Leistungsumfang gegenüber Systemsoftware 7.2.1 und 7.2.4 erheblich erweitern:

2.1 ADSL 2 und 2+

Mit Systemsoftware 7.4.2 unterstützt Ihr Gateway ADSL 2+.

Für die Verwendung mit ADSL 2 und ADSL 2+ müssen Sie neben der Systemsoftware auch die ADSL-Logik updaten. Sie finden die entsprechende Logik an gleicher Stelle wie die aktuelle Systemsoftware. Das Update der Logik erfolgt auf die gleiche Weise wie das der Systemsoftware, Sie sollten jedoch die alte ADSL-Logik zuvor aus dem Flash ROM löschen.

Alte ADSL-Logik löschen

Um eine nicht mehr benötigte Logik zu löschen, gehen Sie folgendermaßen vor (alle Befehle müssen auf der SNMP Shell aufgerufen werden):

1. Rufen Sie die Flash ROM Management Shell auf: `update -i`.
2. Lassen Sie sich alle gespeicherten Dateien anzeigen: `ls -l`.

Sie sehen etwas in dieser Art:

```
Flash-Sh > ls -l
Flags     Version Length  Date                Name ...
Vr-x-bc-B  7.4.02  3310775 2005/12/13 11:35:12 boss.bin
Vr---l--f  3.1.02   326138 2004/10/01 12:44:04 XEY-ADSLp.xey
Flash-Sh >
```

3. Löschen Sie die nicht benötigte Logik:
   `rm XEY-ADSLp.xey.`
4. Stellen Sie sicher, dass die Dartei gelöscht wurde: `ls -l`.

Sie sehen nun etwas in dieser Art:

```
Flash-Sh > ls -l
Flags     Version Length  Date                Name ...
Vr-x-bc-B  7.4.02  3310775 2005/12/13 11:35:12 boss.bin
Flash-Sh >
```

5. Führen Sie einen "reorg" aus, um die Datei endgültig aus dem Flash ROM zu entfernen: `reorg`.
6. Verlassen Sie die Flash ROM Management Shell: `exit`.

Sie haben die nicht mehr benötigte ADSL-Logik gelöscht und können nun die neue Logik installieren.

Sie sollten nach dem Update der Systemsoftware kontrollieren, ob der ***PARAMATER ADSL CONFIGURED MODE*** im Menü ***xDSL*** auf einem entsprechenden Wert steht. Er sollte entweder auf dem zu Ihrem Anschluss passenden Wert stehen (*ADSL 1*, *ADSL 2* oder *ADSL 2 Plus*) oder aber auf *multimode*.

Hinweis

Im *multimode*-Betrieb kann es bis zum Zustandekommen der ADSL-Verbindung geringfügig länger dauern, da ggf. alle möglichen Verbindungstypen versucht werden.

2.2 DSL-Debug-Applikation

Zur Kontrolle einer ADSL-Verbindung verfügt Systemsoftware 7.4.2 über eine Debug-Applikation, mit der relevante Parameter kontrolliert werden können.

Die grundlegende Verwendung ist folgendermaßen:

```
R232:> dsl
usage: dsl [-v] [<command> <arg1> <arg2> ... ]
Options:
        -v: incr verbose level, default is 0
Commands:
        status
        traininfo
        retrain
        ping            [-e|-s] [-c <count> ] <vpi> [<vci>]

use dsl <command> -? for more info
```

Weitere Informationen zu den abrufbaren Informationen folgen in der nächsten Fassung dieser Release Notes.

2.3 Dead Peer Detection

In der Kommunikation zweier IPSec-Peers kann es dazu kommen, dass einer der beiden z. B. aufgrund von Routing-Problemen oder aufgrund eines Neustarts nicht erreichbar ist. Dies ist aber erst dann feststellbar, wenn das Ende der SA Lifetime erreicht ist und ein Rekeying fehlschlägt. Bis zu diesem Zeitpunkt gehen die Datenpakete verloren. Um dies zu verhindern, gibt es verschiedene Mechanismen einer Erreichbarkeitsprüfung.

Bisher wurde lediglich der Heartbeat-Mechanismus unterstützt, um die Erreichbarkeit eines Peers zu überprüfen. Zunehmend hat sich nun DPD (RFC 3706) etabliert, das die Initiative zum Aktivieren der Erreichbarkeitsprüfung vollständig auf eine Seite verlagert und dazu ein Echo-Protokoll verwendet.

Systemsoftware 7.4.2 bietet zwei unterschiedliche Modi der DPD: DPD Triggered und DPD Idle. DPD Triggered überprüft die Erreichbarkeit des Peers nur, wenn tatsächlich Daten an ihn gesendet werden sollen, während DPD Idle die Überprüfung in bestimmten Intervallen unabhängig von anstehenden Datentransfers vornimmt. Somit können auch solche Peer Gateways, die keine Heartbeats, aber DPD unterstützen, regelmäßig auf ihre Erreichbarkeit überprüft werden.

Die Auswahl des DPD-Modus erfolgt bei der Konfiguration der Phase-1-Profile:

```
R232bw Setup Tool                 Funkwerk Enterprise Communications
GmbH
[PHASE1][EDIT]                                                MyGateway

Description (Idx 1)     : global (converted)
Proposal                : 2 (DES3/MD5)
Lifetime Policy         : Propose this lifetime, accept use all
                          Seconds: 7200    KBytes: 0
Group                   : 1 ( 768 bit MODP)
Authentication Method   : Pre Shared Keys
Mode                    : aggressive
Alive Check             : Dead-Peer-Detection (DPD)
Block Time              :  0
Local ID                :  central
Local Certificate       :  none
CA Certificates         :
Nat-Traversal           :  enabled

View Proposals >

               SAVE                           CANCEL
```

Der Parameter ***ALIVE CHECK*** verfügt zusätzlich zu den bekannten Werten für die Heartbeats über die Werte *Dead-Peer-Detection (DPD)* und *Dead-Peer-Detection (DPD), Idle Mode*, wobei *Dead-Peer-Detection (DPD*) für DPD Triggered steht. Wenn Sie eine der beiden Einstellungen auswählen, wird ausschließlich diese für die Erreichbarkeitsüberprüfung in Phase 1 eingesetzt. Wenn Sie *autodetect* wählen, verhält sich Ihr Gateway wie folgt:

- Wenn das Peer Gateway Heartbeats und DPD unterstützt, werden in Phase 1 Heartbeats verwendet.
- Wenn das Peer Gateway nur DPD unterstützt wird in Phase 1 DPD verwendet.
- Wenn das Peer Gateway nur Heartbeats unterstützt, werden in Phase 1 Heartbeats verwendet.

Da DPD für Phase 2 nicht definiert ist, findet sich in der Konfiguration der entsprechenden Profile die Option DPD nicht. Wenn der Wert ***ALIVE CHECK*** für Phase 2 auf *autodetect* steht und für Phase 1 DPD verwendet wird, findet in Phase 2 keine Erreichbarkeitsprüfung statt.

Zur Steuerung der DPD sind folgende neue Variablen eingeführt worden:

- ***IPSECGLOBDPDIDLETHRESHOLD***: Definiert das Intervall, nach dessen Ablauf eine Überprüfung vorgenommen wird. Im Idle Mode bedeutet dies, dass nach Ablauf des Intervalls die Überprüfung dann vorgenommen wird, wenn keine authentisierten Daten von der Gegenstelle empfangen worden sind - unabhängig davon, ob Daten versendet werden sollen. Im Triggered Mode überprüft das Gateway für jedes Paket, das über den Tunnel gesendet werden soll (d. h. nur, wenn Daten versendet werden sollen), ob schon länger als ***IPSECGLOBDPDIDLETHRESHOLD*** keine Daten empfangen worden sind. Ist das der Fall, wird die Erreichbarkeit des Peers überprüft. Der mögliche Wertebereich ist *1* bis *3600* Sekunden, der Defaultwert ist *15*.
- ***IPSECGLOBDPDMAXRETRIES***: Definiert die Anzahl der Versuche, die das Gateway macht, um den Peer zu erreichen (ein Wert von 3 Retries bedeutet dabei insgesamt 4 Anfragen). Erfolgt auf die letzte Anfrage keine Antwort, gilt der Peer als nicht mehr erreichbar und die zugehörigen SAs werden gelöscht. Der mögliche Wertebereich ist *1* bis *10* , der Defaultwert ist *3*.
- ***IPSECGLOBDPDRETRYTIMEOUT***: Definiert das Intervall zwischen den einzelnen Versuchen, den Peer zu erreichen. Der mögliche Wertebereich ist *1* bis *3600* Sekunden, der Defaultwert ist *2*.

Diese Variablen können nicht im Setup Tool konfiguriert werden.

2.4 Unterstützung für mehrere SSIDs

Mit Systemsoftware 7.4.2 unterstützen auch die Geräte der X230xw-Serie die Verwendung mehrerer SSIDs.

Die Konfiguration erfolgt wie gewohnt im Menü ***WLAN*** ➜ ***WIRELESS INTERFACES***.

2.5 WPA 2

Systemsoftware 7.4.2 unterstützt im WLAN-Betrieb WPA 2 sowohl mit Preshared Keys als auch über einen 802.1x Authentisierungsserver.

Zur Konfiguration finden sich im Menü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ **ADD** folgende zusätzlichen Felder:

Parameter	Wert
WPA/WPA2 mixed mode	Nur für ***SECURITY MODE*** = *WPA PSK* und *WPA 802.1x* Hier wählen Sie aus, ob Sie WPA (mit TKIP-Verschlüsselung) oder WPA2 (mit AES-Verschlüsselung) anwenden oder eine Aushandlung zulassen wollen. Mögliche Werte: ■ *WPA + WPA2* (Defaultwert) ■ *WPA only* ■ *WPA2 only.*

Parameter	Wert
WPA2 preauthentication	Nur für ***SECURITY MODE*** = *WPA 802.1x* mit ***WPA/WPA2 MIXED MODE*** = *WPA + WPA2* und *WPA2 only* Mit dieser Option erlauben Sie, dass sich angemeldete Clients vorab bei anderen Access Points in derselben Funkzelle authentifizieren. Dies ermöglicht einen deutlich schnelleren Wechsel des Clients zum nächsten Access Point ("Roaming"), da bei der Anmeldung die RADIUS-Authentisierung übersprungen werden kann. Die Vorab-Authentisierung ist nur möglich, wenn der Client mit WPA2 am Access Point angemeldet ist. Mögliche Werte: ■ *enabled*: der Access Point erlaubt Vorab-Authentisierung von Clients auf anderen Access Points. ■ *disabled* (Defaultwert): Anfragen von Clients zur Vorab-Authentisierung werden ignoriert.

Tabelle 2-1: Neue Felder im Menü ***WIRELESS LAN*** ➜ ***WIRELESS INTERFACES*** ➜ ***ADD/EDIT***

Da WPA 2 für Pre Shared Keys eine Schlüssellänge von 256 Bits vorsieht, ermöglicht das Feld ***PRESHARED KEY*** die Eingabe von 63 ASCII-Zeichen.

2.6 WLAN Wizard

Systemsoftware 7.4.2 unterstützt die Konfiguration von WLAN Interfaces mittels des bintec HTML Wizards.

Der HTML Wizard führt Sie durch die Konfiguration des WLAN Interfaces mit einer SSID. Eine ausführliche Online-Hilfe informiert Sie bei der Konfiguration über die notwendigen Einstellungen.

2.7 SIP- und MGCP-Proxy

Um IP-Telefonen über MGCP und SIP die Verbindung mit einem VoIP Provider zu ermöglichen, ist in Systemsoftware 7.4.2 ein entsprechender Proxy implementiert, der die dazu notwendigen NAT- und Firewall-Freigaben vornimmt.

Die Konfiguration der Proxies wird im Menü ***VoIP*** ➜ ***Application Level Gateways*** vorgenommen:

```
R232bw Setup Tool                 Funkwerk Enterprise Communications
GmbH
[VOIP][ALG]: Application Level Gateway configuration          MyGateway

 Terminal administration

          MGCP Terminal configuration >
          SIP Terminal configuration >


Description     Type     Status    Destination Port
-------------------------------------------------------------------------
MGCP-Provider   MGCP     enable          2427
SIP-Provider    MGCP     enable          5400




     ADD               DELETE              EXIT
```

Durch Auswahl eines bestehenden Proxies oder über ***ADD*** gelangen Sie in das Menü zur Konfiguration eines Proxies. Es enthält folgende Felder:

Parameter	Wert
Description	Hier geben Sie eine Beschreibung für den Proxy ein.
Proxy Type	Hier wählen Sie das Protokoll aus, das der Proxy weiterleiten soll. Zur Auswahl stehen: ■ *MGCP* ■ *SIP.*

Parameter	Wert
Adminstatus	Hier wählen Sie aus, ob der Proxy aktiviert werden soll. Zur Auswahl stehen: ■ *enable* (Defaultwert) ■ *disable.*
Destination Port	Hier geben Sie den Port ein, an dem der VoIP Provider die MGCP- bzw. SIP-Verbindungen annimmt. Pro Destination Port, zu dem sich die VoIP Clients aus dem LAN verbinden können sollen, müssen Sie einen Proxy anlegen. Die Ports können Provider-spezifisch sein. Defaultwert ist *2427*.

Tabelle 2-2: ***VoIP ➜ Application Level Gateways ➜ ADD***

In den Submenüs ***MGCP Terminal Configuration*** und ***SIP Terminal Configuration*** erhalten Sie einen Überblick über diejenigen MGCP bzw. SIP Clients, die aktuell eine Verbindung über Ihr Gateway aufgebaut haben oder bereits einmal eine Verbindung aufgebaut haben:

```
R232bw Setup Tool                 Funkwerk Enterprise Communications
GmbH
[VOIP][ALG][MGCP]: Application Level Gateway configuration   MyGateway

All known connected MGCP Terminals:


Ident    Alias    Status    IP-Address    Gateway
-------------------------------------------------------------------------



            DELETE                                  EXIT
```

Das Menü dient der Anzeige der bekannten Clients und der wesentlichen Verbindungsparameter. Sie können lediglich nicht mehr benötigte oder unerwünschte Einträge löschen.

Die Liste der bekannten Clients wird von Ihrem Gateway gespeichert, so dass nach einem Reboot die entsprechenden NAT- und Firewall-Einstellungen wiederhergestellt werden. So kann ein VoIP Client unmittelbar nach einem Reboot wieder von außen erreicht werden, auch wenn sich der Client noch nicht wieder beim Proxy angemeldet hat.

2.8 HTTP Update

Systemsoftware 7.4.2 unterstützt erstmals die Aktualisierung der Systemsoftware über eine HTTP-Verbindung.

Bisher konnte ein Update der Systemsoftware nur über einen TFTP Server oder die serielle Schnittstelle vorgenommen werden. Die update-Applikation ist so erweitert worden, dass auch HTTP-Verbindungen für ein Update genutzt werden können, z. B.:

```
update   http://www.funkwerk-ec.com/downloads/X2300/X2x00-s7401.x2c.
```

Darüber hinaus ist es möglich, ein HTTP-Update von einer Default Location zu machen: Mittels der Variablen ***biboExtAdmUpdatePath*** kann der Standardpfad zum jeweils aktuellen Release der Software festgelegt werden. Der Befehl, um von diesem Pfad eine neue Version der Systemsoftware zu laden ist dann

```
update http:
```

Das Gateway hängt an den in ***biboExtAdmUpdatePath*** definierten Pfad (sofern er mit einen "/" endet) folgende Elemente an:

- "<System Name>/<System Name>-b_current" für Standard-Images
- "<System Name>/<System Name>-s_current" für IPSec-Images

Hinweis

"System Name" ist nicht der Wert der MIB-Variablen ***SYSNAME***, sondern ein systeminterner Wert, der nicht geändert werden kann. Ggf. vorhandene Leerzeichen werden durch "-" ersetzt, also wird aus "X2300i compact" "X2300i-compact".

Auf dem für das Update vorgesehenen Webserver müssen entsprechende Symlinks angelegt werden, die auf das tatsächlich aktuelle Release Image verweisen (also z. B x2300i-compact-s_current -> X2x00-s7401.x2c). Der vorkonfigurierte Wert für ***BIBOEXTADMUPDATEPATH*** ist *http://www.funkwerk-ec.com/static/files/*.

Außerdem kann der `update`-Befehl mit zwei neuen Optionen aufgerufen werden:

- `-a` - Das Update wird ohne alle Abfragen durchgeführt. Hierfür wird ein inkrementelles Update ausgeführt, das die neue Systemsoftware direkt in den Flash ROM schreibt. Das Gerät darf während des Updates nicht ausgeschaltet werden.
- `-r` - Nach einem Update wird das Gateway rebootet, um die neue Systemsoftware zu aktivieren.

2.9 Scheduler -Erweiterung

Der Event Scheduler kann unter **Systemsoftware 7.4.2** nun auch alle Befehle (Applikationen) ausführen, die auf der SNMP Shell aufgerufen werden können.

Dazu hat das Menü ***SCHEDULE COMMANDS*** ➜ ***ADD*** folgende neue Felder bzw. Optionen erhalten:

Parameter	Wert
Execute Command	Der Parameter kann zur Ausführung eines Shell-Applikation den Wert *exec application* annehmen.
Appl. name	Hier geben Sie den Befehl ein, den der Scheduler ausführen soll, z. B. `update`.
Argum.list active	Hier können Sie Argumente (Optionen) eingeben, die der Scheduler mit dem Befehl ausführen soll, sobald der Schedule Event aktiv wird und der Befehl daraufhin ausgeführt werden soll.
Argum.list inactive	Hier können Sie Argumente (Optionen) eingeben, die der Scheduler mit dem Befehl ausführen soll, sobald der Schedule Event inaktiv wird und der Befehl daraufhin ausgeführt werden soll.

Tabelle 2-3: Neue Felder/Optionen im Menü ***SCHEDULE COMMANDS*** ➜ ***ADD/EDIT***

Darüber hinaus ist der Scheduler durch folgende Änderungen erweitert worden, die Konfiguration erfolgt auf der SNMP Shell:

- Mehrere Variablen (durch ";" getrennt) können vom Scheduler gesetzt werden.
- Entsprechend können auch mehrere Indexvariablen zur Identifikation des zu modifizierenden Eintrags angegeben werden.
- Der Scheduler kann einer MIB Table eine neue Reihe hinzufügen bzw. eine bestehende ersetzen. Dazu wird dem entsprechenden Tabellennamen ein "+" vorangestellt. Der Eintrag wird dann mit den Werten, die für ***VARINDEXVAL*** und ***ACTIVEVALUE*** bzw. ***INACTIVEVALUE*** eingegeben werden erstellt.

3 Änderungen

Folgende Änderungen sind an unserer Systemsoftware vorgenommen worden, um Leistung und Bedienbarkeit zu verbessern:

3.1 PPP-Neuimplementierung

Das PPP-Subsystem ist einer Neuimplementierung unterzogen worden, um den steigenden Anforderungen von Breitbandanwendungen und den damit verbundenen Erfordernissen gerecht zu werden. Im Zuge dieser Neuimplementierung sind eine Reihe von Fehlern beseitigt worden; die entsprechenden Beschreibungen finden Sie in "Gelöste Probleme" auf Seite 31

3.2 SIF-Verbesserungen

Die Stateful Inspection Firewall ist umfangreichen Verbesserungen unterzogen worden, um den steigenden Anforderungen von Breitbandanwendungen und den damit verbundenen Erfordernissen gerecht zu werden. Im Zuge dieser Verbesserungen sind eine Reihe von Fehlern beseitigt worden; die entsprechenden Beschreibungen finden Sie in “Gelöste Probleme” auf Seite 31

3.3 BLUP-Prozedur

Die BLUP-Prozedur ist dahingehend geändert worden, dass gleichnamige Images unserer Systemsoftware vor den Schreiben eines neuen Images aus dem Flash-Speicher gelöscht werden. Dies verhindert Update-Fehler wie z. B. mangelnden Platz im Flash-Speicher.

3.4 Zusätzliche SIF-Tabelle

Eine neue MIB-Tabelle (***IPSIFSTATS***) ist eingeführt worden, um die zur Verfügung stehenden statistischen Informationen zu erweitern. Sie enthält folgende Variablen:

```
x2301:> ipsifstat
ipSifStatCurrSessions( ro):                 0
ipSifStatCurrUdpSessions( ro):              0
ipSifStatCurrTcpSessions( ro):              0
ipSifStatCurrOtherSessions( ro):            0
ipSifStatCurrExpectedSessions( ro):         0
ipSifStatTotalUdpSessions( ro):             0
ipSifStatTotalTcpSessions( ro):             0
ipSifStatTotalOtherSessions( ro):           0
ipSifStatTotalExpectedSessions( ro):        0
x2301:ipSifStat>
```

3.5 HTML Wizard - Handhabung vereinfacht

Der HTML Wizard ist so verändert worden, dass die Javascript Capabilities des verwendeten Browsers zuverlässig erkannt werden. Außerdem ist die APPLY-Prozedur im Quick Mode vereinfacht worden.

3.6 IPSec - ID String Syntax erweitert

Die IPSec ID String Syntax ist um neue Delimiter erweitert worden, um den ID-Typ unabhängig von der Syntax explizit festlegen zu können:

- X500 distinguished name:
  <obj-name=obj-value, obj-ID=obj-value, ...>
- IPV4-Address:
  |123.456.789.012| mit oder ohne '|'
- IPV4 Address Range:
  |123.456.789.012-123.456.789.013| mit oder ohne '|'
- IPV4 Address Subnet:
  |123.456.789.012/255.255.255.0| mit oder ohne '|'
  oder:
  |123.456.789.012/24| mit oder ohne '|'
- Key-ID: Hexadezimal-String beliebiger Länge mit einer graden Anzahl an Digits:
  { 01 23 45 67 89 ab cd ef }
- Fully Qualified User Name (FQUN):
  user@domain mit obligatorischem '@'
- Fully Qualified Domain Name (FQDN):
  beliebiger Name ohne '@', der mit keiner anderen Syntax übereinstimmt.

3.7 IPSec - Lifetime-Konfiguration

Die Konfiguration der Phase-1- und Phase-2-Lifetimes ist geändert worden. Sie erfolgt nun per Profil. Die ***IPSECLIFETIMETABLE*** ist somit obsolet, alle erforderlichen Parameter werden in der ***IKEPROFILETABLE*** und in der ***IPSECPROFILETABLE*** gespeichert.

Bestehende Konfigurationen werden so konvertiert, dass alle bestehenden Profile mit den Werten aus der ***IPSECLIFETIMETABLE*** initialisiert werden, die in den entsprechende Profilen referenziert werden. Wenn ***IKE-/IPSECPROFILEFLIFEPOLICY*** auf *use_default_lifetime* gesetzt ist, werden alle Lifetime-Variablen (sofern verwendet) aus dem Default-Profil übernommen.

Darüber hinaus ist die Konfiguration der Profil-Lifetimes im Setup Tool verbessert worden. Sie wird nun über folgende Parameter gesteuert:

Feld	Wert
Lifetime Policy	Hier legen Sie fest, wie die Lebensdauer (Lifetime) festgelegt wird, die ablaufen darf, bevor die Phase-1-SAs erneuert werden müssen. Mögliche Werte: ■ *Use default lifetime settings* (Defaultwert): Es wird keine Lifetime vorgeschlagen, und gemäß RFC eine Lifetime von 8 Stunden angenommen. Abweichende Vorschläge des IPSec Peers werden angenommen und auch so verwendet. ■ *Propose this lifetime, accept and use all proposals*: Vorgeschlagen wird, die Schlüssel zu erneuern, wenn entweder der in ***SECONDS*** angegebene Wert abgelaufen ist oder der in ***KBYTES*** angegebene Wert verarbeitet wurde, je nachdem, welches Ereignis zuerst eintritt. Abweichende Vorschläge des IPSec-Peers werden angenommen und auch so verwendet.

Feld	Wert
Lifetime Policy (Forts.)	■ *Propose this lifetime, reject different proposals*: Vorgeschlagen wird, die Schlüssel zu erneuern, wenn entweder der in ***SECONDS*** angegebene Wert abgelaufen ist oder der in ***KBYTES*** angegebene Wert verarbeitet wurde, je nachdem, welches Ereignis zuerst eintritt. Abweichende Vorschläge des IPSec-Peers werden nicht angenommen. ■ *Use this lifetime, accept all proposals, notify*: Die Schlüssel werden erneuert, wenn entweder der in ***SECONDS*** angegebene Wert abgelaufen ist oder der in ***KBYTES*** angegebene Wert verarbeitet wurde, je nachdem, welches Ereignis zuerst eintritt. Abweichende Vorschläge des IPSec-Peers werden angenommen, jedoch nicht verwendet. Der IPSe-Peer wird mittels einer "Responder-Lifetime"-Benachrichtigung über die abweichenden Lifetime-Werte in Kenntnis gesetzt.
Seconds	Nur für ***LIFETIME POLICY*** = *Propose this lifetime, accept and use all proposals* oder *Propose this lifetime, reject different proposals* oder *Use this lifetime, accept all proposals, notify* Geben Sie die Lebensdauer für Phase-1-Schlüssel in Sekunden ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Defaultwert ist *900*.

Feld	Wert
KBytes	Nur für ***LIFETIME POLICY*** = *Propose this lifetime, accept and use all proposals* oder *Propose this lifetime, reject different proposals* oder *Use this lifetime, accept all proposals, notify* Geben Sie die Lebensdauer für Phase-1-Schlüssel als Menge der verarbeiteten Daten in KBytes ein. Der Wert darf jeder ganzzahlige Wert von *0* bis *2147483647* sein. Defaultwert ist 0.

3.8 IPSec - Unterstützung von Schlüssellängen pro Proposal

Systemsoftware 7.4.2 unterstützt die Konfiguration von Schlüssellängen auf Proposal-Ebene. Sie kann aktuell noch nicht mittels des Setup Tool konfiguriert werden, die relevanten Variablen finden sich in ***IKEPROPOSALTABLE*** und ***IPSECPROPOSALTABLE***.

3.9 Rijndael in AES umbenannt

Die Bezeichnung des bislang als Rijndael bekannten Algorithmus ist zu AES geändert worden, um der größeren Verbreitung dieser Bezeichnung Rechnung zu tragen.

3.10 Neue Optionen in der Flash Management Shell

Der Befehl `ls` zeigte bislang nicht den Patch Level einer im Flash-Speicher abgelegten Datei an. Mittels der Option `-e` kann dieser nun angezeigt werden:

```
Flash-Sh > ls -eal
Flags    Version        Length                Date Name ...
Vr-x-bc-B  7.4.02      3071906 2005/10/21  9:09:31 boss.bin
Vr---l--f  3.0.14.000   268818 2004/12/14 20:09:05 XEY-ADSLp.xey
Vr---l--f  3.0.14.249   266802 2005/10/12  7:27:48 XEY-ADSLp.xey
Flash-Sh >
```

3.11 SNMP Foreign Agent entfernt

Vor **Systemsoftware 7.4.2** war es möglich, die Adresse eines anderen SNMP Agents anzugeben. Diese Funktion wurde kaum genutzt und führte beim Lauschen auf der Adresse *0.0.0.0* zu Problem. Sie ist entfernt worden.

3.12 MRU für PPPoA-Interfaces

Wenn ein Interface für PPPoA Permanent Mode konfiguriert ist, wird das MRU dem entsprechenden Eintrag in der ***BIBOADMDEVICETABLE*** entnommen. Ist das Interface für PPPoA On Demand Mode konfiguriert, wird der Wert auf *4096* Bytes gesetzt. Wenn jedoch für ***PPPEXTIFMRU*** ein anderer Wert als *0* konfiguriert ist, hat diese Einstellung den Vorrang.

3.13 Zusätzliche Debug-Optionen

Wenn ein Treiber einen Burst an Syslog-Meldungen erzeugt, wird auf der Konsole die Meldung `trap queue 0x12345678 full` ausgegeben, und eine Anzahl von Syslog-Meldungen wird nicht mehr angezeigt. Dies geschieht, wenn die Anzahl der Syslog-Meldungen die Grenze der Trap Queue überschreitet.

Diese ist in den meisten Fällen auf *32768* Meldungen beschränkt. **Systemsoftware 7.4.2** führt die Option `-l <size>` ein, mit der die Größe der Trap Queue auf maximal *256000* vergrößert werden kann.

Bislang war es nicht möglich, den Inhalt der ***BIBOADMSYSLOGTABLE*** komfortabel anzuzeigen. **Systemsoftware 7.4.2** führt die Option `-s` ein, die anstelle der neuen Syslog-Meldungen in Echtzeit die in der ***BIBOADMSYSLOGTABLE*** gespeicherten in der gleichen Formatierung anzeigt.

3.14 ADSL Monitoring verbessert

SNR Margin und Attenuation wurden bislang nicht in die MIB geschrieben und daher im ADSL-Monitoring-Menü des Setup Tools nicht angezeigt. Dies ist geändert worden: SNR Margin, Attenuation und Output Power werden (in dB/10) in die MIB geschrieben. Im ADSL-Monitoring-Menü werden ATUC -und ATUR-Status ebenfalls korrekt angezeigt.

3.15 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.

4 Gelöste Probleme

Die folgenden Probleme sind in Systemsoftware 7.4.2 gelöst worden:

4.1 Wichtig: IPSec-Verwundbarkeit beseitigt

Funkwerk Gateways waren von einer ISKAMP-Verwundbarkeit betroffen, die bei http://www.ee.oulu.fi entdeckt worden war (siehe http://www.ee.oulu.fi/research/ouspg/protos/testing/c09/isakmp/). Sie vesagten in den Testfällen #16, #427, #1681 und #2970.

Diese Schwachstelle ist beseitigt worden.

4.2 SIF - Verbesserte Leistung

(ID 2800)

Unter bestimmten Umständen konnte die CPU-Auslastung bei der Verwendung der SIF signifikant ansteigen und eine Reduktion der gesamten Gateway-Leistung verursachen.

Das Problem ist gelöst worden.

4.3 RADIUS - Accounting Messages

(ID n/a)

Wenn RADIUS Accounting für eine PPP-over-L2TP-Verbindung genutzt wurde und der RADIUS Server nur durch den L2TP-Tunnel erreichbar war, so erreichte die ACCOUNTING-OFF-Nachricht den RADIUS server nicht, wenn der Benutzer das entsprechende Interface deaktivierte.

Das Problem ist gelöst worden.

4.4 Keepalive Monitoring - Setup-Tool-Fehler

(ID 3358)

Die Konfiguration des Keepalive Monitoring für IPSec Interfaces (mit einem INdex von *100001* und höher) schlug mit der Fehlermeldung "Integer value too large" fehl, wenn man den Interface Index für ***FIRSTIFINDEX*** eingab.

Das Problem ist gelöst worden.

4.5 QoS - TOS Error

(ID 4148)

Da ein TOS-Wert nicht wie vorgesehen behandelt wurde, konnte es zu inkonsistentem QoS-Verhalten kommen.

Das Problem ist gelöst worden.

4.6 Ethernet - Fehler in der Switch-Konfiguration

(ID 4181)

Nach dem Zurücksetzen einer Port-Trennung entstanden in der ***IPROUTETABLE*** überflüssige Einträge.

Das Problem ist gelöst worden.

4.7 PPP - Blockade

(ID 4071)

Bei Verbindung mit einem fehlkonfigurierten LNS konnte eine PPP-over-L2TP-Verbindung mit einem Shorthold von *-1* nicht realisiert werden. Nach einer Reihe von Verbindungsversuchen war das PPP-Subsystem blockiert.

Das Problem ist gelöst worden.

4.8 QoS - Verbessertes Weighted Fair Queuing

(ID n/a)

Die Verwendung von WFQ in QoS-Konfigurationen konnte zu unvorhersehbarem Verhalten des Gateways (und auch zu Stack Traces) führen.

Das Problem ist gelöst worden.

4.9 Setup Tool - Absturz während IP-Konfiguration

(ID 4180)

Wenn anstelle einer IP-Adresse ein Host-Name bei der IP-Konfiguration eingegeben wurde, kam es zu einem Absturz des Gateways beim Versuch, den Namen aufzulösen.

Das Problem ist gelöst worden.

4.10 NAT - Überflüssige MIB-Einträge

(ID 4210)

Die Änderung des NAT-Status eines Interfaces führte zu zusätzlichen, überflüssigen Einträgen in der ***PPPEXTIFTABLE***.

Das Problem ist gelöst worden.

4.11 ATM - Datenverkehr blockiert

(ID 4242)

Wenn beide Tx Queues (hohe und niedrige Priorität) eines SAR DMA Channels gleichzeitig benutzt wurden, konnte die Transmit-Tätigkeit einer der beiden Tx-Queues einfrieren.

Das Problem ist gelöst worden.

4.12 RPoA - IP-Advanced-Settings-Menü fehlt

(ID 4275)

Bei der Konfiguration eines RPoA-Interfaces, fehlte der Link zum IP-Advanced-Settings-Menü, wenn das Profil noch nicht gesichert worden war.

Das Problem ist gelöst worden.

4.13 QoS - Reboot bei Änderung der Priorität

(ID 4287)

Eine Änderung von Werten für ***QOSPOLICYPRIORITY*** konnte bei Einträgen, die mit dem gleiche Interface assoziiert waren, zu einem Neustart des Gateways führen.

Das Problem ist gelöst worden.

4.14 SNMP - Dezimale Notation für OIDs

(ID n/a)

Mit Hilfe des Befehls `x` auf der SNMP Shell können OIDs in dezimaler Notation eingegeben werden. Dies führte zu Fehlern bei der Identifikation des gemeinten MIB-Eintrags.

Das Problem ist gelöst worden.

4.15 ATM - Neustart bei VPI/VCI-Änderung

(ID 4323)

Bei der Änderung der Einstellungen für VPI und VCI entweder im Setup Tool oder auf der SNMP Shell kam es zu einem Neustart des Gateways.

Das Problem ist gelöst worden.

4.16 IPSec - Hinzufügen einer Post IPSec Rule nicht möglich

(ID 4586)

Sobald eine Post IPSec Rule konfiguriert worden war, stürzte das Gateway bei dem Versuch ab, eine weitere hinzuzufügen.

Das Problem ist gelöst worden.

4.17 PPTP - Kompatibilität

(ID 4337)

Der Aufbau einer PPTP-Verbindung zu einem DrayTek-Gerät schlug fehl.

Das Problem ist gelöst worden.

4.18 RIP - Endlosantworten

(ID 4338)

Obwohl das Gateway Acknowledgements für Triggered RIP Replies erhielt, wurden die Replies weiterhin gesendet, so dass keine anderen RIP-Routen mehr veröffentlicht werden konnten.

Das Problem ist gelöst worden.

4.19 Debug - NAT-Meldungen unterdrückt

(ID 4268)

Syslog-Meldungen des NAT wurden irrtümlich unterdrückt, wenn man z. B. `debug all` aufrief.

Das Problem ist gelöst worden.

4.20 QoS - Interfaces im Monitoring ignoriert

(ID 4328)

Einige Interfaces mit aktiviertem QoS wurden nicht in den entsprechenden Monitoring-Menüs angezeigt.

Das Problem ist gelöst worden.

4.21 TDRC - Port Range unzureichend

(ID 4317)

Bei der Konfiguration eines Dienstes für TDRC (TCP Download Rate Control) ließ der Parameter ***TCP SERVICE PORT*** nur Portnummern bis *999* zu. Der korrekte Wertebereich ist *1* bis *65535*.

Das Problem ist gelöst worden.

4.22 Setup Tool - IPSec Remote Type nicht konfigurierbar

(ID 3934

Der Typ der entfernten Seite einer Post-IPSec-Traffic-Konfiguration konnte nicht konfiguriert werden.

Das Problem ist gelöst worden.

4.23 GRE - Speicherverlust

(ID 4301)

GRE-Sessions, die nicht vom PPTP-Subsystem gesteuert wurden, konnten zu einem Speicherverlust führen, wenn SIF, Load Balancing oder TDRC verwendet wurden.

Das Problem ist gelöst worden.

4.24 SIF - Activity Monitor Pakete blockiert

(ID 4384)

Lokal vom Systemprotokolldienst erzeugte Meldungen wurden trotz einer Accept-Regel blockiert.

Das Problem ist gelöst worden.

4.25 MIB - Enums umbenannt

(ID 4365)

Einige MIB-Enums begannen mit Großbuchstaben, was nicht standardkonform ist.

Das Problem ist gelöst worden.

4.26 Syslog - Stack Trace

(ID n/a)

Gelegentlich wurde ein Stack Trace ausgegeben, wenn der Systemprotokolldienst auf bestimmte Traps zugreifen wollte.

Das Problem ist gelöst worden.

4.27 Ethernet - Fehler in virtuellen MAC Adressen

(ID 4175)

Bei der Erstellung der virtuellen MAC-Adressen für ETHoA-Interfaces wurden versehentlich mit der dem Ethernet-Interface zugeordneten identische Adressen erzeugt.

Das Problem ist gelöst worden.

4.28 IPSec - Certificate Server nicht löschbar

(ID 4428)

Wenn ein Eintrag in der ***CERTSERVERTABLE*** angelegt worden war (sei es mittels des Setup Tools oder der SNMP Shell), war es nicht mehr möglich, diesen Eintrag zu löschen.

Das Problem ist gelöst worden.

4.29 NAT - Session-Beschränkung nicht korrekt angewendet

(IFD n/a)

Eine Begrenzung der maximalern Anzahl an NAT-Sessions durch einen Eintrag für ***IPEXTIFNATMAXSESSIONS*** hatte nicht das erwartete Ergebnis: Es wurde eine zusätzliche Session zugelassen.

Das Problem ist gelöst worden.

4.30 TCP - Geringer Durchsatz mit High Speed xDSL

(ID 4348)

Die Download-Rate, die auf xDSL-Verbindungen mit hoher Bandbreite (6 Mbit/s und mehr) tatsächlich erreicht wurde, war niedriger als erwartet.

Das Problem ist gelöst worden.

4.31 WLAN - Anlegen neuer WLAN Interfaces nicht möglich

(ID n/a)

Das Anlegen eines neuen WLAN Interfaces war bei Verwendung der SNMP Shell oder eines SNMP Managers nicht möglich. Dies war nur mit dem Setup Tool möglich.

Das Problem ist gelöst worden.

4.32 SNMP - Fehlermeldung "Decode failed"

(ID 4235)

Unter bestimmten Voraussetzungen wurden alle UDP-Pakete, die aus den mit dem Gateway verbunden Netzen kamen, wie SNMP-Antworten behandelt, was dazu führte, dass das Gateway bei Aufruf der MIB einen Fehler anzeigte.

Das Problem ist gelöst worden.

4.33 PPP - MRU Einstellungen wurden ignoriert

(ID 4588)

Für PPPoE-Interfaces wurde die MRU-Konfiguration ignoriert, da der Wert auf *1492* Bytes fest eingestellt war.

Das Problem ist gelöst worden.

4.34 IPSec - Zertifikats- / CRL-Download fehlgeschlagen

(ID 4598)

Der automatische Download eines Zertifikats oder einer CRL von einem Server aus der ***CERTSERVERTABLE*** schlug fehl, da die Anfrage auf einen falschen Port geschickt wurde.

Das Problem ist gelöst worden.

4.35 PPPoE - Rufrichtung falsch

(ID n/a)

Die Richtung eines ausgehenden PPPoE-Rufs wurde auf *incoming* gesetzt.

Das Problem ist gelöst worden.

4.36 HTML Wizard - Falsches Bild

(ID n/a)

Auf den SIF Konfigurationsseiten war ein falsches GIF eingefügt.

Das Problem ist gelöst worden.

4.37 PPP - Probleme bei der Authentifizierung in zwei Schritten

(ID 4667)

Bei der PPP-Authentifizierung in zwei Schritten konnte es gelegentlich zu Verbindungsschwierigkeiten kommen.

Das Problem ist gelöst worden.

4.38 Setup Tool - Absturz bei der WAN-Partner-Konfiguration

(ID 4391)

Wurde die WAN-Partner-Konfiguration mit ***SAVE*** bestätigt, konnte dies zu einem Stack Trace und zu einem Neustart des Gateways führen.

Das Problem ist gelöst worden.

4.39 WLAN - Konfiguration des Frenquenzbereichs

(ID 4764)

Das Feld ***USAGE AREA*** wurde für 2,4 und für 5 GHz Interfaces angezeigt, solllte aber nur für 5 GHz Interfaces zur Verfügung stehen.

Ausserdem wurde bei der Auswahl eines beliebigen anderen Wertes als *default* in ***USAGE AREA*** und anschliessender Bestätigung mit ***SAVE*** der ausgewählte Wert nicht gespeichert.

Das Problem ist gelöst worden.

4.40 WLAN - Auswahl des Kanals

(ID 4713)

In einigen Versionen unserer Systemsoftware war die Auswahl der Option *auto* für das Feld ***CHANNEL*** in der WLAN-Konfiguration nicht möglich. Dieses war nicht beabsichtigt.

Das Problem ist gelöst worden.

4.41 WLAN - WPA-PSK-Konfiguration

(ID 4765)

Das Setup Tool Feld für den Preshared Key bei ***SECURITY MODE*** = *WPA PSK*:

1) war zu klein: nur 46 Zeichen konnten sichtbar eingegeben werden.

2) zeigte falsche Informationen in der Hilfezeile : "...max length = 64 chars". Die tatsächliche maximale Länge ist *63* Zeichen, da die finale *0* eines Schlüssels nicht mit eingegeben wird.

Das Problem ist gelöst worden.

4.42 PPP - Authentifizierungsfehler

(ID 4771)

Wenn eine Authentifizierung in mehreren Schritten durchgeführt wurde, kam es gelegentlich zu Fehlern.

Das Problem ist gelöst worden.

4.43 ATM - Falsche Interface-Geschwindigkeit

(ID n/a)

Wenn ein RPoA- und kein ETHoA-Interface konfiguriert wurde, wurde die ***IFSPEED*** des RPoA-Interfaces nicht richtig gesetzt.

Das Problem ist gelöst worden.

4.44 SNMP - MIB-Suchoperationen fehlgeschlagen

(ID 4767)

Suchoperationen innerhalb der MIB konnten fehlschlagen.

Das Problem ist gelöst worden.

4.45 VJH Compression - Stack Trace mit ISDN PPP

(ID 4798)

Bei aktiviertem VJHC konnte es zu Stack Traces und einem Neustart des Gateways kommen.

Das Problem ist gelöst worden.

4.46 TACACS+ - Instabiles System

(ID 4822)

Beim Einsatz von TACACS+ wurde bei der Verwendung einer beliebigen Anwendung ein Reboot ausgelöst.

Das Problem ist gelöst worden.

4.47 Content Filtering - Behobene Fehler

(ID n/a)

1. Das Serverlisten-Format von Cobion wurde erweitert. Dieses führte zu einem Eintrag mit der IP-Adresse *0.0.0.0* in der ***cofServerTable***. Dieser Eintrag führte gelegentlich zu Panics und manchmal zu längeren Verzögerungen beim Abrufen der Kategorie einer URL bei Cobion.

2. In seltenen Fällen antwortete der Cobion Server mit negativen Antworten auf Lizenzanfragen unserer Produkte. Dieses führte dazu, dass eine ungültige Lizenz angezeigt wurde und keine weiteren Anfragen zum Cobion Server geschickt wurden.

3. Wenn die Internet-Verbindung nach einem Neustart nicht unmittelbar zur Verfügung stand, wie dies zum Beispiel bei ADSL-Verbindungen der Fall sein kann, schlug die Lizenzanfrage an den Content Filter Server fehl und somit war der URL Filter nicht anwendbar.

Das Problem ist gelöst worden.

4.48 IPSec / RADIUS - Peers gelöscht

(ID n/a)

Nach einem fehlgeschlagenen IPSec Preset Reload, wurden die Peers, die bisher nicht aktualisiert wurden, gelöscht. Dieses Ergebnis ist vom Benutzer nicht

beabsichtigt, und es wird empfohlen, die alten Peers zu behalten und nicht zu verwerfen.

Das Problem ist gelöst worden.

4.49 Multi Link PPP - Panic bei fehlgeschlagenem LCP Echo Check

(ID n/a)

Ein fehlgeschlagener LCP Echo Check über eine MLPPP-Verbindung konnte zur einer Panic führen.

Das Problem ist gelöst worden.

4.50 SNMP - MIB Einträge nicht editierbar

(ID n/a)

RIPFILTERTABLE Einträge konnten über SNMP nicht gelöscht werden. Man musste das Setup Tool benutzen.

Das Problem ist gelöst worden.

4.51 PPTP - Neustart

(ID 5130)

Bei der Einwahl auf das Gateway über einen Linux PPTP Client konnte der Verbindungsabbau zu einem Neustart des Gerätes führen (mit oder ohne Stack Trace).

Das Problem ist gelöst worden.

4.52 Activity Monitor - Nicht unterstützte Interfaces

(ID 4149, 4224, 4709)

Der Activity Monitor, Bestandteil unserer **BRICKware**, erkannte nicht alle Interfaces unserer neuen Produkte und die in neueren Software-Versionen auf älteren Geräten und unterstütze diese nicht richtig.

Das Problem ist gelöst worden.

4 Gelöste Probleme