Release Notes Systemsoftware 7.1.4

Version 1.0

Ziel und Zweck

Dieses Dokument beschreibt neue Funktionen, Änderungen und behobene Fehler in **Systemsoftware 7.1.4**.

Haftung

Der Inhalt dieses Dokuments wurde mit größter Sorgfalt erarbeitet. Die Angaben in diesem Dokument gelten jedoch nicht als Zusicherung von Eigenschaften Ihres Produkts. Bintec Access Networks 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.bintec.de.

Als Multiprotokollrouter bauen Bintec-Router in Abhängigkeit von der Systemkonfiguration WAN-Verbindungen auf. Um ungewollte Gebühren zu vermeiden, sollten Sie das Produkt unbedingt überwachen. Bintec Access Networks 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 Bintec Access Networks GmbH.

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

Copyright

Richtlinien und Normen

Bintec-Router 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.bintec.de.

Wie Sie Bintec erreichen

Bintec Access Networks GmbH
Südwestpark 94
D-90449 Nürnberg
Germany

Telephone: +49 180 300 9191 0
Fax: +49 180 300 9193 0
Internet: www.bintec.de

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.bintec.fr

1 Wichtige Informationen

Bitte lesen Sie die folgenden Informationen zu Systemsoftware 7.1.4. Systemsoftware 7.1.4 beruht auf Systemsoftware 7.1.1, daher gelten die gleichen Bedingungen den Funktionsumfang und die Einschränkungen beim Downgrade betreffend.

Hinweis

Beachten Sie unbedingt die Hinweise zum Upgrade auf **Systemsoftware 7.1.4**, die Sie auf unserer Website ebenso wie die Software zum Download bereit gestellt finden.

1.1 BOOTmonitor Update

Ein Update auf **Systemsoftware 7.1.4** erfordert ein BOOTmonitor-Update auf allen Gateways der **X2000**-Familie.

Sie finden die notwendigen Dateien im Download-Bereich Ihres Gateways. Das BOOTmonitor-Update kann genau wie die Systemsoftware mittels des Befehls `update` erfolgen. Eine Beschreibung finden Sie im Handbuch Ihres Gateways im Kapitel "Konfigurationsmanagement".

Achtung!

Das Update des BOOTmonitor muss vor dem Update der Systemsoftware durchgeführt werden. Andernfalls ist ein Update der Systemsoftware nicht möglich.

Für Geräte der X2000-Familie ist ein BOOTmonitor mit einem Stand von mindestens 6.3.8 notwendig.

1.2 DSL-Logik löschen

Auf den Geräten der **X2300**-Familie ist es notwendig, vor dem Update auf **Systemsoftware 7.1.4** die jeweils nicht benötigte DSL-Logik zu löschen.

Gehen Sie dazu folgendermaßen vor:

1. Gehen Sie zur Flash ROM Management Shell: `update -i`.

2. Rufen Sie eine Liste aller im Flash ROM gespeicherten Dateien auf: `ls -l`. Sie erhalten (z. B.) folgende Ausgabe auf der Shell:

```
Flash-Sh > ls -l
  Flags   Version   Length                Date Name ...
Vr-x-bc-B  6.3.04  1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696 2003/01/24 15:48:05 X2E-ADSLp.x2c
Vr---l--f  3.8.129   315904 2003/01/16 13:17:42 X2E-ADSLi.x2c
Flash-Sh >
```

Die Datei "X2E-ADSLp.x2c" wird von **X2300** verwendet (ADSL over POTS), "X2E-ADSLi.x2c" von **X2300i** und **X2300is** (ADSL over ISDN).

3. Löschen Sie die nicht Ihrem Gateway-Typ entsprechende Datei: `rm X2E-ADSLi.x2c` oder `rm X2E-ADSLp.x2c.`
4. Stellen Sie sicher, dass die Datei gelöscht worden ist: `ls -l`.
   Sie erhalten nun folgende Ausgabe auf der Shell (wenn Sie z. B. die Logik für ADSL over ISDN gelöscht haben):

```
Flash-Sh > ls -l
  Flags   Version   Length                Date Name ...
Vr-x-bc-B  6.3.04  1740353 2003/06/05  7:53:06 box155rel.ppc860
Vr---l--f  3.8.129   319696 2003/01/24 15:48:05 X2E-ADSLp.x2c
Flash-Sh >
```

5. Führen Sie ein "reorg" durch, um die Datei endgültig aus dem Flash ROM zu löschen: `reorg`.
   Optional können Sie zur Kontrolle erneut eine Liste der gespeicherten Dateien aufrufen: `ls -l`.
6. Verlassen Sie die Flash ROM Management Shell: `exit`.

Sie haben die nicht benötigte DSL-Logik gelöscht.

1.3 Einschränkungen beim Downgrade

Es ist nicht möglich, direkt von **Systemsoftware 7.1.4** auf eine frühere Version der Systemsoftware zurückzukehren.

Achtung!

Konfigurationen, die unter Systemsoftware 7.1.4 erstellt werden, sind mit älterer Systemsoftware nicht kompatibel.

Sichern Sie die Konfiguration Ihres Gateways auf einem PC, bevor Sie ein Upgrade vornehmen.

Beachten Sie, dass Ihnen nach einem Downgrade bestimmte Funktionen nicht mehr zur Verfügung stehen werden.

Ein stufenweiser Downgrade ist möglich:

1. Sichern Sie die Konfiguration Ihres Gateways auf einem PC, bevor Sie auf **Systemsoftware 7.1.4** upgraden. Informationen zum externen Sichern einer Konfiguration finden Sie im Handbuch Ihres Gateways im Kapitel "Konfigurationsmanagement".
2. Nun können Sie das Upgrade vornehmen und ggf. dennoch zu Ihrer alten Systemsoftware zurückkehren. Nach dem Downgrade müssen Sie die zu dieser Systemsoftware passende Konfigurationen auf das Gateway zurückspielen. Informationen zu den notwendigen Schritten finden Sie im Handbuch Ihres Gateways.

Weitere Informationen zu Beschränkungen beim Up- oder Downgrade sowie die Dokumentation Ihres Gateways finden Sie unter www.bintec.de

1.4 Funktionsumfang

Systemsoftware 7.1.4 ist unterschiedslos sowohl für die neuen Geräte der VPN Access Linie als auch für die Geräte der X-Generation verwendbar. Bitte beachten Sie, dass sich der Funktionsumfang der einzelnen Geräte sowohl einer Linie wie auch unterschiedlicher Linien dennoch voneinander unterscheidet.

Für die folgenden Geräte steht keine Version von **Systemsoftware 7.1.4** zur Verfügung:

- **BinGO! DSL**
- **X1000**
- **X1200**
- **X3200**
- alle Geräte der **BRICK**-Generation.

Darüber hinaus besteht die folgende Einschränkungen:

- **BinGO! DSL II** verfügt nicht über die Funktion "Übertragung der IP-Adresse im ISDN", da **BinGO! DSL II** nicht IPSec-fähig ist.

1.5 BRICKware Wizard

Seit Release 7.1.1 unterstützt unsere Systemsoftware den **BRICKware** Configuration Wizard nicht mehr. Mit **Systemsoftware 7.1.4** wird ein neuer, HTML-basierter Configuration Wizard eingeführt.

1.6 Software-Image-Namen

Die Bezeichnungen der Software-Images haben sich dahingehend geändert, dass der eigentlichen Release-Kennung die Bezeichnung des Gerätes vorangestellt wird. Werden Ihre Gateways mittels des Konfigurationswerkzeugs XAdmin konfiguriert, so müssen Sie zunächst noch die alten Image-Namen verwenden. Dazu löschen Sie lediglich die Gerätekennung aus dem Namen: "X1x00II-b7101.x2x" wird so zu "b7101.x2x".

1.7 Voraussetzungen für die Verwendung des AUX-Ports

Systemsoftware 7.1.1 und 7.1.4 unterstützen den Anschluss eines analogen oder GSM-Modems am seriellen Anschluss Ihres Gateways. Für eine erfolgreiche Verbindung müssen bestimmte Voraussetzungen erfüllt sein.

Bitte lesen Sie die Release Notes zur Systemsoftware 7.1.1, um sich über Voraussetzungen und Beschränkungen zu informieren. Insbesondere beachten Sie bitte Folgendes:

- Nur die in den Release Notes 7.1.1 angegebenen Modems sind von Bintec erfolgreich getestet worden und für die Verwendung am AUX-Port freigegeben. Die XON/XOFF-Flusskontrolle muss vollständig unterstützt und funktionstüchtig sein, andernfalls wird eine Verbindung zwischen Gateway und Modem unter Umständen scheitern.
- Stellen Sie sicher, dass das zur Verbindung von Gateway und Modem verwendete Kabel den im Anhang von Release Notes 7.1.1 angegebenen Spezifikationen entspricht. Um sicherzugehen, können Sie ein fertig konfektioniertes Kabel von Bintec erwerben.

1 Wichtige Informationen

2 Neue Funktionen

Systemsoftware 7.1.4 ist ein Major Release und enthält eine Anzahl wichtiger neuer Funktionen.

Die neuen Funktionen sind in den folgenden Kapiteln beschrieben:

- "HTML Wizard" auf Seite 11
- "Übertragung der IP-Adresse über ISDN" auf Seite 13
- "NAT Traversal" auf Seite 18
- "Event Scheduler" auf Seite 20

2.1 HTML Wizard

Systemsoftware 7.1.4 bietet einen HTML-basierten Konfigurations-Wizard, der Ihnen grundlegende Konfigurationsaufgaben erheblich erleichtert und eine funktionsfähige Konfiguration Ihres Routers oder Gateways sicherstellt.

Der HTML Wizard steht auf folgenden Geräten zur Verfügung:

- **VPN Access 5/25/100**
- **BinGO! DSL II**
- **X1000 II**
- **X1200 II**
- allen Geräten der **X2000**-Familie.

Bintec-Router und -Gateways werden mit einer voreingestellten IP-Konfiguration ausgeliefert (IP-Adresse: *192.168.0.254*, Netzmaske: *255.255.255.0*). Durch den Aufruf von 192.168.0.254/wizard können Sie den HTML-Konfigurationsassistenten (**HTML Wizard**) aufrufen. Dieser führt Sie durch eine Grundkonfiguration, die alle wichtigen Einstellungen des Gateways, den Zugang zum Internet über einen Internet Service Provider (ISP) sowie die Verbindung zu einem WAN-Partner (z. B. Firmenzentrale) beinhaltet. Tiefergehende Netzwerk-

kenntnisse sind dabei nicht erforderlich. Ein detailliertes Online-Hilfe-System gibt Ihnen zusätzlich Hilfestellung.

Hinweis

Der HTML Wizard hat aus Sicherheitsgründen einen Default-Timeout von 5 Minuten, d. h. nach 5 Minuten Inaktivität wird die HTML-Session beendet und Sie müssen die Konfiguration vollständig erneut durchführen.

2.1.1 Sprachanpassung

Beim Update eines Gerätes mit **Systemsoftware 7.1.4** wird der HTML Wizard zunächst nur in der englischen Version eingespielt. Es ist jedoch möglich, weitere Sprachen (zunächst Deutsch) nachträglich zu installieren. Geräte, die bereits mit Systemsoftware 7.1.4 ausgeliefert werden, enthalten bereits entsprechende Sprachdateien.

Um eine Sprachdatei nachträglich zu installieren, benötigen Sie einen TFTP-Server, der es dem Gateway ermöglicht, die Datei zu laden. Die **Dime Tools**, die in der **BRICKware for Windows** enthalten sind, beinhalten einen TFTP-Server.

Um die Sprachdatei per TFTP übertragen zu können, muss Ihr Gateway über eine funktionsfähige IP-Konfiguration verfügen.

ToDo Gehen Sie folgendermaßen vor:

1. Laden Sie die entsprechende Sprachdatei von unserem Webserver herunter. Die Datei ist nach der entsprechenden Sprache und dem Typ Ihres Gateways benannt (z. B german.x2c für eine deutsche Sprachdatei der X2x compact).
2. Kopieren bzw. verschieben Sie die Datei in das Root-Verzeichnis des TFTP-Servers und starten Sie den Server.
3. Loggen Sie auf Ihrem Gateway als `admin` ein.
4. Laden Sie die Datei von Ihrem PC herunter (achten Sie darauf, die IP-Adresse Ihres PCs zu verwenden): `update 192.168.0.1 german.x2c`.

Die Sprachdatei steht nun auf Ihrem Gateway zur Verfügung, weitere Schritte sind nicht notwendig.

2.1.2 ASCII-Wizard

Sollte Ihnen der Zugang zu Ihrem Gateway über das LAN nicht möglich sein oder Sie auf den HTML Wizard aus anderen Gründen nicht zugreifen können, können Sie auch eine ASCII-basierte Version des Wizards auf der SNMP Shell starten. Somit können Sie alle Funktionen des Wizards auch über eine serielle Verbindung nutzen.

ToDo Um eine ASCII-Version des Wizards zu starten können Sie auf eine beliebige Art und Weise mit dem Gateway verbunden sein: Es spielt keine Rolle, ob Sie sich über das LAN, über eine serielle Verbindung oder über ISDN-Login mit dem Gateway verbinden. Sie müssen sich als `admin` anmelden und auf die SNMP Shell zugreifen können.

Gehen Sie folgendemaßen vor:

1. Melden Sie sich als `admin` an Ihrem Gateway an.
2. Geben Sie im Command Prompt den Befehl `wizard` ein und drücken Sie die **Eingabetaste**.

Die ASCII-Version des Wizards wird gestartet. Es bietet die gleichen Konfigurationsmöglichkeiten wie der HTML Wizard. Auch die Hilfetexte stehen über die Schaltfläche **HELP** zur Verfügung.

2.2 Übertragung der IP-Adresse über ISDN

Mittels der Übertragung der IP-Adresse eines Gateways über ISDN (im D-Kanal und/oder im B-Kanal) eröffnen sich neue Möglichkeiten zur Konfiguration von IPSec-VPNs, da Einschränkungen, die bei der IPSec-Konfiguration mit dynamischen IP-Adressen auftreten, so umgangen werden können.

Bisher unterstützt der IPSec ISDN Callback einen Tunnelaufbau nur dann, wenn die aktuelle IP-Adresse des Initiators auf indirektem Wege (z. B. über DynDNS) ermittelt werden kann. DynDNS hat aber gravierende Nachteile, wie z. B. die Latenzzeit, bis die IP-Adresse in der Datenbank wirklich aktualisiert ist. Dadurch kann es dazu kommen, dass die über DynDNS propagierte IP-Adresse nicht korrekt ist. Dieses Problem wird durch die Übertragung der IP-Adresse

über ISDN umgangen. Darüber hinaus ermöglicht diese Art der Übermittlung dynamischer IP-Adressen, den sichereren ID-Protect-Modus für den Tunnelaufbau zu verwenden.

2.2.1 Funktionsweise

Um die eigene IP-Adresse an den Peer übermitteln zu können, stehen unterschiedliche Modi zur Verfügung: Die Adresse kann im D-Kanal kostenfrei übertragen werden oder im B-Kanal, wobei der Ruf von der Gegenstelle angenommen werden muss und daher Kosten verursacht.

Wenn ein Peer, dessen IP-Adresse dynamisch zugewiesen worden ist, einen anderen Peer zum Aufbau eines IPSec-Tunnels veranlassen will, so kann er seine eigene IP-Adresse gemäß der in “Konfiguration” auf Seite 15 beschriebenen Einstellungen übertragen. Nicht alle Übertragungsmodi werden von allen Telefongesellschaften unterstützt. Sollte diesbezüglich Unsicherheit bestehen, kann mittels der automatischen Auswahl durch das Gateway sichergestellt werden, dass alle zur Verfügung stehenden Möglichkeiten genutzt werden.

Hinweis

Damit das Gateway des gerufenen Peers die Informationen über die IP-Adresse identifizieren kann, sollte die Callback-Konfiguration auf den beteiligten Gateways identisch vorgenommen werden.

Die Übertragung der IP-Adresse und der Beginn der IKE-Phase-1-Aushandlung verlaufen in folgenden Schritten:

1. Peer A (der Initiator des Callbacks) stellt eine Verbindung zum Internet her, um eine dynamische IP-Adresse zugewiesen zu bekommen und um für Peer B über das Internet erreichbar zu sein.
2. Das Gateway erstellt ein begrenzt gültiges Token und speichert es zusammen mit der aktuellen IP-Adresse im zu Peer B gehörenden MIB-Eintrag.
3. Das Gateway setzt den initialen Ruf an Peer B ab. Dabei werden die IP-Adresse von Peer A sowie das Token gemäß der Callback-Konfiguration übermittelt.
4. Peer B extrahiert die IP-Adresse von Peer A sowie das Token aus dem ISDN-Ruf und ordnet sie Peer A aufgrund der konfigurierten Calling Party

Number (der ISDN-Nummer, die Peer A verwendet, um den initialen Ruf an Peer B abzusetzen) zu.

5. Der IPSec-Daemon auf Peer Bs Gateway kann die übermittelte IP-Adresse verwenden, um eine Phase-1-Aushandlung mit Peer A zu initiieren. Dabei wird der Token in einem Teil der Payload innerhalb der IKE-Aushandlung an Peer A zurückgesendet.
6. Peer A ist nun in der Lage, das von Peer B zurückgesendete Token mit den Einträgen in der MIB zu vergleichen und so den Peer zu identifizieren, auch ohne dessen IP-Adresse zu kennen.

Da Peer A und Peer B sich wechselseitig identifizieren können, können auch unter Verwendung von Preshared Keys Aushandlungen im ID-Protect-Modus durchgeführt werden.

2.2.2 Konfiguration

Die Konfiguration erfolgt im Kontext der IPSec-Callback-Konfiguration im Menü ***IPSec ➜ Configure Peers ➜ APPEND/EDIT ➜ IPSec Callback***.

Das Menü sieht folgendermaßen aus (der Screenshot enthält Beispielwerte):

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC] [PEERS] [EDIT] [Callback]                                MyGateway

ISDN Callback:       both

     Incoming ISDN Number:1234
     Outgoing ISDN Number:01234

     Transfer own IP Address over ISDN:  yes

    Mode :              autodetect best possible mode (D or B channel)


               SAVE                              CANCEL
```

Es enthält die folgenden neuen Felder:

Feld	Wert
Transfer own IP Address over ISDN	Hier wählen Sie aus, ob für den IPSec-Callback die IP-Adresse des eigenen Gateways über ISDN übertragen werden soll. Mögliche Werte: ■ *yes* - Die IP-Adresse wird gemäß den Einstellungen in den folgenden Feldern übertragen. ■ *no* - (Defaultwert) Die IP-Adresse wird nicht übertragen.

Feld	Wert
Mode	Nur sichtbar, wenn ***TRANSFER OWN IP ADDRESS OVER ISDN*** = *yes*. Hier wählen Sie aus, in welchem Modus das Gateway versucht, seine IP-Adresse an den Peer zu übertragen. Mögliche Werte: ■ *autodetect best possible mode (D or B channel)* - (Defaultwert) Das Gateway bestimmt automatisch den günstigsten Modus. Dabei werden zunächst alle D-Kanal-Modi versucht, bevor der B-Kanal verwendet wird (die Verwendung des B-Kanals verursacht Kosten). ■ *autodetect best possible mode (D channel only)* - Das Gateway bestimmt automatisch den günstigsten D-Kanal-Modus. Der B-Kanal ist von der Verwendung ausgeschlossen. ■ *use specific D channel mode* - Das Gateway versucht, die IP-Adresse in dem im Feld ***D-CHANNEL MODE*** eingestellten Modus zu übertragen. ■ *try specific D channel mode, fall back on B* - Das Gateway versucht, die IP-Adresse in dem im Feld ***D-CHANNEL MODE*** eingestellten Modus zu übertragen. Gelingt das nicht, wird die IP-Adresse im B-Kanal übetragen (dies verursacht Kosten). ■ *use B channel* - Das Gateway überträgt die IP-Adresse im B-Kanal. Dies verursacht Kosten.

Feld	Wert
D-Channel Mode	Nur sichtbar, wenn ***MODE*** = *use specific D channel mode* oder *try specific D channel mode, fall back on B*. Hier wählen Sie aus, in welchem D-Kanal-Modus das Gateway versucht, die IP-Adresse zu übertragen. Mögliche Werte: ■ *LLC* - (Defaultwert) Die IP-Adresse wird in den LLC Information Elements des D-Kanals übertragen. ■ *SUBADDR* - Die IP-Adresse wird in den Subaddress Information Elements des D-Kanals übertragen. ■ *LLC-and-SUBADDR* - Die IP-Adresse wird sowohl in den LLC- als auch in den Subaddress Information Elements übertragen.

Tabelle 2-1: ***IPSEC ➜ CONFIGURE PEERS ➜ APPEND/EDIT ➜ IPSEC CALLBACK***

2.3 NAT Traversal

NAT Traversal (NAT-T) ermöglicht es, IPSec-Tunnel auch über ein oder mehrere Gateways zu öffnen, auf denen Network Address Translation (NAT) aktiviert ist.

Ohne NAT-T kann es zwischen IPSec und NAT zu Inkompatibilitäten kommen (siehe RFC 3715, Abschnitt 2). Diese behindern vor allem den Aufbau eines IPSec-Tunnels von einem Host innerhalb eines LANs und hinter einem NAT-Gateway zu einem anderen Host bzw. Gateway. NAT-T ermöglicht derartige Tunnel ohne Konflikte mit NAT-Gateways, aktiviertes NAT wird vom IPSec-Daemon automatisch erkannt und NAT-T wird verwendet.

Die Konfiguration von NAT-T beschränkt sich auf die Aktivierung bzw. Deaktivierung der Funktion in den Einstellungen der Phase-1-Profile. Dort ist eine entsprechender Parameter hinzugefügt worden:

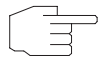
```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[IPSEC][PHASE1][EDIT]                                            MyGateway

Description (Idx 1) :    test
   Proposal              :  1 (Blowfish/MD5)
   Lifetime              :  use default
   Group                 :  2 (1024 bit MODP)
   Authentication Method :  Pre Shared Keys
   Mode                  :  id_protect
   Heartbeats            :  none
   Block Time            :  0
   Local ID              :
   Local Certificate     :  none
   CA Certificates       :
   Nat-Traversal         :  default

   View Proposals >
   Edit Lifetimes >

                         SAVE                              CANCEL
```

Für das Feld ***NAT-TRAVERSAL*** stehen folgende Werte zur Verfügung:

- *default* - Wenn Sie diesen Wert bei der Konfiguration von Peer-spezifischen Parametern (in ***CONFIGURE PEERS*** ➜ ***ADD/EDIT*** ➜ ***PEER SPECIFIC SETTINGS*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT***) auswählen, verwendet das Gateway den für das globale Profil (in ***IPSEC*** ➜ ***IKE (PHASE 1) DEFAULTS: EDIT***) eingestellten Wert. Ein globales Profil kann nicht mit diesem Wert gespeichert werden. Ist beim Update auf **Systemsoftware 7.1.4** bereits ein Phase-1-Profil vorhanden, so wird für dieses der Wert auf *default* gesetzt. Für ein globales Profil bedeutet dies, dass NAT-T deaktiviert bleibt.
- *enabled* - NAT-T wird in diesem Profil aktiviert.
- *disabled* - NAT-T wird in diesem Profil deaktiviert.

Wenn Sie eine IPSec-Verbindung mit dem HTML Wizard oder mit dem IPSec Setup Tool Wizard konfigurieren, wird NAT-T grundsätzlich aktiviert. Bei der

Verwendung des Setup Tool Wizards wird der Wert in einem ggf. existierendes Default-Profil allerdings nicht verändert.



Hinweis

Wenn Sie IPSec sowohl vom Gateway aus als auch von Hosts innerhalb des LANs zulassen wollen, müssen Sie die Einträge in der ***IPNATOUTTABLE***, die sich auf den IKE-Datenverkehr beziehen löschen. Andernfalls werden alle IKE-Sessions auf die gleiche interne IP-Adresse bezogen, und nur die zuletzt initiierte IKE-Session kommt wirklich zustande.

Das Löschen der NAT-Einträge führt allerdings dazu, dass es bei IPSec-Verbindungen vom Gateway zu Peers, die NAT-T nicht unterstützen, unter bestimmten Umständen zu Problemen kommen kann, da der Quellport der IKE-Verbindung vom NAT verändert wird.

2.4 Event Scheduler

Um Ereignisse wie das Deaktivieren eines Internetzugangs beim Überschreiten eines bestimmten Transfervolumens u. ä. zu ermöglichen, bietet Systemsoftware 7.1.4 einen Event Scheduler. Dieser ermöglicht es, beliebige Ereignisse beliebigen Aktionen zuzuordnen.

Abgesehen von voreingestellten und einfach zu konfigurierenden Standardanwendungen wie zeit- oder volumengesteuerte Aktivierung von Interfaces, ermöglicht es der Event Scheduler, beliebig auf MIB-Parameter zuzugreifen. Dadurch können beliebige Ereignisse in der MIB als Auslöser ebenfalls beliebiger Aktionen definiert werden.

Achtung!

Die Konfiguration der nicht voreingestellten Aktionen erfordert umfangreiches Wissen über die Funktionsweise unserer Gateways. Eine Fehlkonfiguration kann zu erheblichen Störungen im Betrieb führen. Sichern Sie ggf. die ursprüngliche Konfiguration auf einem PC.

Die Konfiguration des Event Scheduler erfolgt im Menü ***System ➜ Schedule & Monitor ➜ Event Scheduler (Time & SNMP)***:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED]: Event Schedule                              MyGateway


                    Event Scheduler             disabled

                    Schedule Events >
                    Schedule Commands >

                    SAVE                    CANCEL
```

Im Feld ***Event Scheduler*** aktivieren oder deaktivieren Sie den Scheduler, per Default ist er deaktiviert. Im Menü ***Schedule Events*** konfigurieren Sie die Ereignisse, die eine bestimmte Aktion auf dem Gateway auslösen sollen, im Menü ***Schedule Commands*** die auszuführenden Aktionen. Die Auslöser (Events) können zu Ereignis-Ketten verknüpft werden, so dass auch komplexe Bedingungen für das Auslösen einer Aktion erstellt werden können.

2.4.1 Konfiguration der Auslöser (Events)

Die Ereignisse, die eine entsprechende Aktion auslösen, werden im Menü ***System ➜ Schedule & Monitor ➜ Event Scheduler (Time & SNMP) ➜ Schedule Events ➜ ADD/EDIT*** erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü mit der Maske zur Konfiguration eines Ereignisses vom Typ *time*:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events          MyGateway

  Index        1        Description
    NextIndex    none
    Type         time


    Condition             dayly
      Start time (hh:mm)
      End time   (hh:mm)

    Status                notavail

                  SAVE                           CANCEL
```

Wenn Sie ***TYPE*** = *value* auswählen, ändert sich das Menü wie folgt:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_EVT][ADD]: Scheduler Events          MyGateway

   Index        1        Description
     NextIndex    none
     Type         value

     Monitored event       user defined
       Table
       Variable
       Index variable
       Index value

     Condition             range
       Compare value
       End value

     Status                notavail

                   SAVE                           CANCEL
```

Je nach Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für das Ereignis ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.
Next Index	Hier geben Sie an, welcher Eintrag dem aktuellen in einer Ereigniskette folgen soll. Die Einträge einer Ereigniskette bilden eine komplexe Bedingung für eine auszuführende Aktion. Wie die Ereigniskette zu einer Aktion führt, wird im Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** konfiguriert.
Type	Hier wählen Sie, welchen Typ von Ereignis Sie als Auslöser einer Aktion definieren wollen: Zur Verfügung stehen: ■ *time* - Die Aktion wird zu bestimmten Zeiten ausgelöst (Defaultwert). ■ *value* - Die Aktion wird ausgelöst, sobald eine MIB-Variable einen bestimmten Wert annimmt.

Feld	Wert
Monitored event	Nur für ***TYPE*** = *value*. Hier können Sie zwischen unterschiedlichen Ereignissen wählen. Zur Verfügung stehen: ■ *user defined* - Sie können frei wählen, auf welchen Wert welcher MIB-Variablen der Scheduler mit einer Aktion reagieren soll (Defaultwert). ■ *WAN interface total charge* - Eine Aktion wird ausgeführt, wenn auf einem WAN-Interface (die Auswahl des Interfaces erfolgt bei der Konfiguration der Aktion) bestimmte Kosten verursacht worden sind. Dazu ist es notwendig, dass dem Gateway vom Provider Gebührenimpulse übertragen werden. ■ *WAN interface total duration* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface für eine bestimmte Zeitdauer aktiv gewesen ist. ■ *WAN interface total RX traffic* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface eine bestimmte Menge an Daten (in Bytes) empfangen hat. ■ *WAN interface total TX traffic* - Eine Aktion wird ausgeführt, wenn ein WAN-Interface eine bestimmte Menge an Daten (in Bytes) gesendet hat.
Table	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die MIB-Tabelle an, in der sich die MIB-Variable befindet, die für den Auslöser verwendet werden soll, z. B. ***PPPTABLE***.

Feld	Wert
Variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die MIB-Variable ein, die für den Auslöser verwendet werden soll, z. B. ***PPPMAXCONN***.
Index variable	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie die Indexvariable der zuvor ausgewählten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist, z. B. ***PPPTYPE***. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist (z. B. ***BIBOPPPTYPE.1.1(RW): ISDN_DIALUP***). Aus der Kombination der Indexvariablen und ihres Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Index value	Nur für ***MONITORED EVENT*** = *user defined*. Hier geben Sie den Wert ein, den die Indexvariable für den Tabelleneintrag hat, der für den Auslöser verwendet werden soll, z. B. ***ISDN_DIALUP***.

Feld	Wert
Condition	Für ***TYPE*** = *time*: ■ *daily* - Die Aktion wird täglich ausgelöst (Defaultwert). ■ *<Wochentag>* - Die Aktion wird wiederkehrend an einem bestimmten Wochentag ausgelöst. ■ *mon-fri* - Die Aktion wird täglich von Montag bis Freitag ausgelöst. ■ *sat_sun* - Die Aktion wird wiederkehrend nur Samstags und Sonntags ausgelöst. ■ *day <1 .. 31>* - Die Aktion wird wiederkehrend an einem bestimmten Tag des Monats ausgelöst. Für ***TYPE*** = *value*: ■ *range* - Die Aktion wird ausgelöst, wenn der Wert der Variablen zwischen zwei bestimmten Werten liegt (Defaultwert). ■ *greater* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert übersteigt. ■ *equal* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert annimmt. ■ *less* - Die Aktion wird ausgelöst, wenn der Wert der Variablen unter einen bestimmten Wert bleibt. ■ *notequal* - Die Aktion wird ausgelöst, wenn der Wert der Variablen einen bestimmten Wert nicht annimmt.

Feld	Wert
Compare value	Der Wert, zu dem der Wert der Variablen in dem durch ***CONDITION*** bestimmten Verhältnis steht. Wenn ***CONDITION*** = *range*, so ist dies der Startwert des Wertebereichs.
End value	Wenn ***CONDITION*** = *range*, so ist dies der Endwert des Wertebereichs.
Start time (hh:mm)	Nur für ***TYPE*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem die Aktion gestartet werden soll.
End time (hh:mm)	Nur für ***TYPE*** = *time*. Hier geben Sie den Zeitpunkt ein, an dem die Aktion beendet werden soll.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status des Auslösers an. Mögliche Werte sind: ■ *active* - Der Auslöser ist derzeit aktiv. ■ *inactive* - Der Auslöser ist inaktiv. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration des Auslösers ist nicht konsistent.
Last Change	Hier wird der Zeitpunkt der letzten Zustandsänderung angezeigt. Das Feld kann nicht editiert werden.

Tabelle 2-2: ***SYSTEM*** ➜ ***SCHEDULE & MONITOR*** ➜ ***EVENT SCHEDULER (TIME & SNMP)*** ➜ ***SCHEDULE EVENTS*** ➜ ***ADD/EDIT***

2.4.2 Konfiguration der Aktion (Command)

Welche Aktion ausgeführt wird, sobald eines der als Auslöser konfigurierten Ereignisse eintritt, wird im Menü ***System*** ➜ ***Schedule & Monitor*** ➜ ***Event Scheduler (Time & SNMP)*** ➜ ***Schedule Commands*** ➜ ***ADD/EDIT*** erstellt bzw. editiert.

Standardmäßig öffnet sich das Menü mit den Optionen zur Auswahl einer der voreingestellten Aktionen:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

   Index        1        Description
     Mode                 enable
     1. Event Index       none
     Eventlist Condition  all

     Execute command      disable interface
     Interface            en1-0


     Notify               all

     Status    notavail       Last Change    01/01/1970  0:00:00

                  SAVE                            CANCEL
```

Wenn Sie für das Feld ***EXECUTE COMMAND*** den Wert *user defined* auswählen, ändert sich das Menü wie folgt:

```
VPN Access Setup Tool                          Bintec Access Networks GmbH
[SYSTEM][SCHEDULED][SCHED_CMD][ADD]: Scheduler Commands      MyGateway

  Index        1        Description
    Mode                  enable
    1. Event Index        none
    Eventlist Condition   all

    Execute command       user defined
      Table
      Variable
      Index variable
      Index value
      Set value active
          value inactive
    Notify                all

    Status    notavail       Last Change    01/01/1970  0:00:00

                  SAVE                           CANCEL
```

Je nach gewählter Einstellung enthält das Menü folgende Felder:

Feld	Wert
Index	Das Gateway vergibt automatisch eine Index-Nummer für den Eintrag. Der Wert kann aber auch editiert werden. Es stehen alle Werte von *1* bis *65535* zur Verfügung.
Description	Hier geben Sie eine beliebige Bezeichnung für das Ereignis ein. Die maximale Länge des Eintrags beträgt 30 Zeichen.

Feld	Wert
Mode	Hier wählen Sie aus, ob die konfigurierte Aktion aktiv oder inaktiv sein soll. Zur Verfügung stehen: ■ *enable* (Defaulwert) ■ *disable*
1. Event Index	Hier legen Sie das erste Ereignis einer Ereigniskette fest. Die Ereigniskette wird erst von diesem Eintrag an aktiviert, vorhergehende Einträge werden ignoriert. Defaultwert ist *none*.
Eventlist Condition	Hier legen Sie fest, ob alle Einträge einer Ereigniskette zutreffen müssen, damit eine Aktion ausgeführt wird. Zur Verfügung stehen: ■ *all* - Alle Ereignisse einer Ereigniskette müssen auftreten, damit die Aktion ausgeführt wird (Defaultwert). ■ *one* - Mindestens eines der Ereignisse einer Ereigniskette muss auftreten, damit die Aktion ausgeführt wird. ■ *none* - Keines der Ereignisse einer Ereigniskette darf eintreten, damit die Aktions ausgeführt wird. ■ *one_not* - Mindestens eines der Ereignisse einer Ereigniskette darf nicht auftreten, damit die Aktion ausgeführt wird.

Feld	Wert
Execute command	Hier legen Sie die Aktion fest, die aufgrund eines Auslösers ausgeführt wird. Zur Verfügung stehen: ■ *disable interface* - Das im Feld ***INTERFACE*** bestimmte Interface wird deaktiviert (sein ***ADMINSTATUS*** wird auf *down* gesetzt, Defaultwert). ■ *enable interface* - Das im Feld ***INTERFACE*** bestimmte Interface wird aktiviert (sein ***ADMINSTATUS*** wird auf *up* gesetzt). ■ *user defined* - Die Aktion wird in den folgenden Feldern frei konfiguriert.
Interface	Hier wählen Sie aus, welches Interface aktiviert bzw. deaktiviert werden soll, wenn für ***EXECUTE COMMAND*** *disable interface* oder *enable interface* gewählt ist. Defaultwert ist *en1-0*.
Table	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die MIB-Tabelle ein, in der sich die zu setzende Variable befindet.
Variable	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die MIB-Variable ein, die gesetzt werden soll.

Feld	Wert
Index variable	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie die Indexvariable der zuvor ausgewählten MIB-Tabelle ein. Dies ist in einer beliebigen MIB-Tabelle diejenige Variable, die in der Tabellenansicht mit einem Asterisk (*) markiert ist. Die Einträge in einer MIB-Tabelle werden intern indiziert. In der normalen Tabellenansicht wird diese Indizierung nicht angezeigt. Geben Sie auf der Shell `y` ein, um den Tabellenmodus zu deaktivieren. Wenn Sie nun z. B. `pppTable` eingeben, werden die Einträge in einem Format aufgelistet, in dem die Indizierung sichtbar ist (z. B. ***BIBOPPPTYPE.1.1(RW): ISDN_DIALUP***). Aus der Kombination der Indexvariablen und ihres Wertes (inklusive des internen Indexes) ergibt sich die eindeutige Identifikation eines bestimmten Tabelleneintrags.
Index value	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die Indexvariable für den Tabelleneintrag hat, der durch die Aktion geändert werden soll.
Set value active	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die ***VARIABLE*** durch die Aktion zugewiesen bekommen soll. Der Wert wird gesetzt, sobald ein entsprechender Auslöser aktiv wird und bleibt solange erhalten, bis der Auslöser wieder inaktiv wird.
value inactive	Nur für ***EXECUTE COMMAND*** = *user defined*. Hier geben Sie den Wert ein, den die Variable annimmt, sobald der Auslöser inaktiv wird. Dieser Wert wird der Variablen auch nach einem Neustart des Gateways zugewiesen oder wenn die Systemzeit nicht korrekt eingestellt ist.

Feld	Wert
Notify	Hier wählen Sie aus, welche Mechanismen verwendet werden, um über Aktionen zu informieren. Zur Verfügung stehen: ■ *all* - Es werden sowohl SNMP-Traps als auch Syslog-Meldungen erzeugt. ■ *snmptrap* - Es werden nur SNMP-Traps erzeugt. ■ *syslog* - Es werden nur Syslog-Meldungen erzeugt. ■ *none* - Es werden keine Meldungen erzeugt.
Status	Dieses Feld kann nicht editiert werden und zeigt den Status der Aktion an. Mögliche Werte sind: ■ *active* - Die Aktion wird derzeit ausgeführt. ■ *inactive* - Die Aktion wird nicht ausgeführt. ■ *notavail* - Der Status kann nicht festgestellt werden, z. B. wenn der Scheduler nicht aktiviert ist. ■ *error* - Es ist ein Fehler aufgetreten, die Konfiguration der Aktion ist nicht konsistent.
Last Change	Hier wird der Zeitpunkt der letzten Zustandsänderung angezeigt. Das Feld kann nicht editiert werden.

Tabelle 2-3: ***SYSTEM ➜ SCHEDULE & MONITOR ➜ EVENT SCHEDULER (TIME & SNMP) ➜ SCHEDULE COMMANDS ➜ ADD/EDIT***

2 Neue Funktionen

3 Änderungen

Zusätzlich zu neuen Funktionen erweitert eine Reihe von Änderungen den Funktions- und Leistungsumfang unserer Software.

Die Änderungen sind in den folgenden Kapiteln beschrieben:

3.1 Neue Kommandos

Um es zu ermöglichen, sensible Daten wir Preshared Keys einer IPSec-Konfiguration mit der Konfigurationsdatei exportieren und importieren zu können, sind zwei neue Kommandos in die *biboAdmConfigTable* integriert worden: `put_all` **und** `get_all`**.**

Achtung!

Beachten Sie, dass das Abspeichern der Datei auf dem PC unverschlüsselt erfolgt und daher sensible Daten im Klartext gelesen werden können. Sichern Sie Ihren PC entsprechend, damit die gespeicherten Dateien nicht in unbefugte Hände gelangen.

put_all Die Syntax zum Abspeichern der Konfiguration `boot` ist folgende:

```
cmd=put_all host=<IP-Adresse des TFTP-Servers> path=<Name der aus dem Flash zu sendenden Datei> file=<Name der Datei auf dem PC>.
```

Zum Beispiel:

```
x2300ic:biboAdmConfigTable> cmd=put_all host=192.168.0.1 path=boot
file=boot.cf
01: biboAdmConfigCmd.3.7( rw):        put_all
01: biboAdmConfigHost.3.7( rw):       192.168.0.1
01: biboAdmConfigPath.3.7( rw):       "boot"
01: biboAdmConfigFile.3.7( rw):       "boot.cf"
x2300ic:biboAdmConfigTable>
```

get_all Entsprechend ist die Syntax zum Laden einer Datei:

```
cmd=get_all host=<IP-Adresse des TFTP-Servers> path=<Name
der im Flash zu speichernden Datei> file=<Name der Datei
auf dem PC>.
```

Zum Beispiel:

```
x2300ic:> cmd=get_all host=192.168.0.1 path=boot file=boot
00: biboAdmConfigCmd.4.10( rw):        get_all
00: biboAdmConfigHost.4.10( rw):       192.168.0.1
00: biboAdmConfigPath.4.10( rw):       "boot"
00: biboAdmConfigFile.4.10( rw):       "boot.cf"
x2300ic:>
```

3.2 HTML Wizard - LAN-LAN-Verbindung über IPSec

Bisher war es notwendig, für eine IPSec-LAN-LAN-Kopplung zunächst einen Internetzugang über ISDN oder DSL zu konfigurieren. Ein Internetzugang über ein zweites Gateway (also über eine Ethernet-Verbindung) wurde nicht unterstützt.

Systemsoftware 7.1.4 ermöglicht es, eine derartige Konfiguration vorzunehmen. Wenn der anzubindende Standort über eine zweites Gateway an das Internet angeschlossen ist, gehen Sie folgendermaßen vor, um eine IPSec-Verbindung über die Ethernet-Verbindung zu erhalten:

1. Starten Sie den HTML Wizard.
2. Wählen Sie nach der Sprachauswahl für ***KONFIGURATIONSMODUS*** die Option *erweitert*.
3. Wählen Sie alle drei ***KONFIGURATIONSABSCHNITTE*** aus (*Grundeinstellungen*, *Internet-Zugang*, *Verbindung zum Corporate Network*)
4. Folgen Sie der Wizard-Konfiguration bis zur Konfiguration des Internetzugangs. Wählen Sie dort im ersten Konfigurationsfenster für ***INTERNET ZUGANG*** die Option *mit einem anderen Gateway*.
   Das Fenster wird neu aufgebaut und ermöglicht nun die Eingabe weiterer Parameter.
5. Geben Sie die IP-Adresse an, unter der das Gateway, das den Internetzugang realisiert, aus Ihrem LAN erreicht werden kann.

6. Sofern Sie bei der Konfiguration der Grundeinstellungen keinen DNS-Server eingegeben haben, müssen Sie dies hier tun.

Sie haben nun die Voraussetzungen geschaffen, um eine LAN-LAN-Verbindung über IPSec ohne die Konfiguration eines Internetzugangs über ISDN oder DSL vorzunehmen.

7. Folgen Sie der Wizard-Konfiguration zur Konfiguration der LAN-LAN-Verbindung und wählen Sie dort im ersten Konfigurationsfenster für ***VERFUEGBARE VERBINDUNGSTYPEN*** die Option *IPSec*.

3.3 Neuer PMTU- und MSS-Clamping-Mechanismus

Nachdem es bei IPSec-Verbindungen zu Fehlern bei der korrekten Berechnung des PMTU aufgrund fehlender ICMP-Meldungen gekommen ist, sind die entsprechenden Mechanismen grundlegend neu gestaltet worden.

Grundsätzlich ist nun sichergestellt, dass die PMTU Discovery zuverlässig auch für IPSec-Verbindungen funktioniert. Darüber hinaus kann das Verhalten des Gateways für die PMTU Discovery mittels einer neuen MIB-Variablen präzise geregelt werden.

Mittels einer neuen MIB-Variablen (***IKEPRFMTUMAX***) kann für jeden Peer ein Ausgangswert für das MTU definiert werden. Dieser Wert stellt sogleich den Maximalwert für jede MTU-Aushandlung für diesen Peer dar. Die Variable kann alle ganzzahligen Werte von *0* bis *65535* annhemen, wobei alle Werte *<214* automatisch auf den zulässigen Minimalwert von *214* gesetzt werden. Der Defaultwert *0* bezeichnet einen impliziten Wert von 1418 Bytes.

In bereits existierenden Profilen wird beim Update der Software der Defaultwert (*0*) angenommen, ebenso wird dieser Wert bei der Konfiguration mittels des Setup Tool IPSec Wizard und des HTML Wizard verwendet. Eine Konfiguration des Wertes im Setup Tool ist nicht möglich.

Das aktuell ausgehandelte MTU eines Peers wird durch die Variable ***IPSECPEERMTU*** angezeigt.

Entsprechend der Konfiguration des IPSec Peers wird MSS Clamping aktiviert: Wenn Sie einen Peer mit virtuellem Interface konfiguriert haben (***ipsecPeerVirtualInterface*** = *enabled*), wird MSS Clamping sowohl auf eingehenden als auch für ausgehenden Datenverkehr angewendet. Dafür wird der Wert des ***ipsecPeerMtu*** verwendet, sofern keine anderen Einstellungen in ***ipExtIfTxpMssClamping*** vorgenommen worden sind (d. h. der Wert dort *0* ist).

Für Peers mit einer Traffic-List-Konfiguration wird kein MSS Clamping verwendet.

4 Behobene Fehler

Folgende Fehler sind in Systemsoftware 7.1.4 behoben worden:

4.1 Speicherverlust

(ID n/a)

Eine interne Funktion führte zu einem Speicherverlust beim Einsatz der IPSec-Version unserer Systemsoftware.

Dieses Problem ist gelöst worden.

4.2 ATM - Route verweist auf falsches Interface

(ID n/a)

In einem der folgenden Menüs wurde ein neuer IP-Eintrag erstellt:

- ***ATM ➜ ETHERNET OVER ATM ➜ ADD/EDIT ➜ IP AND BRIDGING ➜ ADD/EDIT***
- ***ATM ➜ ROUTED PROTOCOLS OVER ATM ➜ ADD/EDIT ➜ IP ➜ ADD/EDIT***.

Eine IP-Route, die sich auf das so definierte Interface bezog, verwies auf ein falsches Interface.

Dieses Problem ist gelöst worden.

4.3 SNMP Shell - Autologout nicht durch "t 0" deaktiviert

(ID 2668)

Unter bestimmten Umständen deaktivierte die Eingabe von `t 0` auf der SNMP Shell den Autologout nicht zuverlässig.

Dieses Problem ist gelöst worden.

4.4 NAT - PMTU Discovery schlägt fehl

(ID 2792)

Die Einstellung des Path Maximum Transfer Units schlug auf Interfaces mit aktiviertem NAT (Network Address Translation) u. U. fehl, so dass es zu Paketverlusten kam.

Dieses Problem ist gelöst worden.

4.5 IPSec Setup Tool Wizard - Falsche Werte angezeigt

(ID 3260)

Während eines IPSec-Wizard-Durchlaufs wurden bei der Konfiguration der Advanced Interface Settings eines Interface Peers andere Werte als die tatsächlich verwendeten angezeigt. Nur wenn die angezeigten Werte mit ***SAVE*** bestätigt wurden, wurden sie in der MIB gespeichert und aktiviert.

Dieses Problem ist gelöst worden.

4.6 Setup Tool - Advanced IP Settings nicht gespeichert

(ID 3266)

Bei der Konfiguration im Menü ***IP*** ➜ ***ADVANCED SETTINGS*** in einem der verfügbaren Kontexte (z. B. bei der WAN-Partner-Konfiguration) wurden die eingestellten Werte nicht in der MIB gespeichert. Eine Konfiguration über die SNMP Shell war möglich.

Dieses Problem ist gelöst worden.

4.7 SSH - Daemon inaktiv

(ID 3301)

Nach einem fehlgeschlagenen Verbindungsversuch konnte es dazu kommen, dass der SSH Daemon beendet wurde, ohne neu gestartet zu werden. Darüber hinaus konnten SSH-Verbindungen über ein Interface, auf dem NAT aktiviert ist, mit dem gleichen Effekt fehlschlagen.

Dieses Problem ist gelöst worden.

4.8 IPSec - Speicherverlust

(ID 3318)

Die Aktivierung von IPSec auf einem Gateway konnte zu einem Speicherverlust mit sporadischen Neustarts führen.

Dieses Problem ist gelöst worden.

4.9 RIP - Routen-Import begrenzt

(ID 3325)

Der Routen-Import via RIP (Routing Information Protocol) war auf 100 Routen begrenzt.

Dieses Problem ist gelöst worden.

4.10 BOOTP Relay - Inform Packets nicht geroutet

(ID 3327)

DHCP Inform Packets wurden von einem Windows-PC generiert und korrekt an den zentralen DHCP-Server übertragen. Die Antwortpakete wurden jedoch nicht an den PC geroutet.

Dieses Problem ist gelöst worden.

4.11 BRRP - Neustart

(ID 3356)

Beim Öffnen des Menüs ***BRRP*** ➜ ***CONFIGURATION*** ➜ ***ADD*** kam es sporadisch zu Neustarts des Gateways mit und ohne Ausgabe eines Stacktraces.

Dieses Problem ist gelöst worden.

4.12 QoS - Falsche Länge eines Eingabefelds

(ID 3366)

Wurde im Menü ***QOS*** ➜ ***IP CLASSIFICATION AND SIGNALLING*** ➜ ***ADD/EDIT*** ➜ ***SIGNALLING (TOS)*** das Feld ***SPECIFY TOS SET RATE LIMITATION*** auf *packets* gesetzt, so wurde für die Felder ***MAXIMUM RATE (PACKETS PER SECOND)*** und ***MAXIMUM BURST SIZE (NUMBER OF PACKETS)*** ein Maximalwert von *256000* (= 6 Stellen) angegeben. Das Eingabefeld ermöglichte aber nur die Eingabe von 5 Stellen.

Dieses Problem ist gelöst worden.

4.13 AUX - Störungen bei PPP-Verbindungen

(ID 3369)

Bei PPP-Verbindungen über das AUX-Interface kam es zu Problemen bei der Datenübertragung, oder das Modem brach die Verbindung zum Gateway ganz ab.

Dieses Problem ist gelöst worden.

4.14 LEDs - HA-LED ohne Funktion

(ID 3377)

Die LED "HA" verhielt sich nicht wie im Handbuch beschrieben: Sie reagierte auf keinen internen Zustand des Gateways und leuchtete daher niemals.

Dieses Problem ist gelöst worden.

4.15 PPP - MTU ignoriert

(ID 3400)

Bei der Authentifizierung (und Identifikation) eingehender PPP-Verbindungen wurde eine MTU-Anpassung durch die Variable ***PPPEXTIFMTU*** nur von dem Gateway beachtet, das die Verbindung aufbaute.

Dieses Problem ist gelöst worden.

4.16 QoS - Problem mit X8E-SYNC

(ID 3412)

Unter hoher Last wurde eine QoS-Konfiguration für Priority Queues mit Bandbreitenbeschränkungen nicht korrekt ausgeführt.

Dieses Problem ist gelöst worden.

4.17 Configuration Management - Konfigurations-Datei nicht importierbar

(ID 3417)

Wenn ein Fehler aus dem Bereich des Email Alert in der MIB gespeichert wurde, konnte das Gateway die Konfiguration nicht wieder in den Flash-Speicher zurückladen, wenn diese auf einem TFTP Server abgelegt worden war.

Dieses Problem ist gelöst worden.

4.18 PPTP - Falsche IP-Einstellungen in PPTP-Partner-Konfiguration

(ID 3438)

Bei der Konfiguration eines PPTP-Partners wurden u. U. falsche IP-Einstellungen in der MIB gespeichert (*static* statt *dynamic client* für ***IPADDRESS*** in der ***BIBOPPPTABLE***).

Dieses Problem ist gelöst worden.

4 Behobene Fehler