Release Notes
System Software 10.2.12

Inhalt

Hinweise

Release Notes beschreiben Neuigkeiten und Änderungen in einem Release für jeweils alle Geräte, für die das Release zur Verfügung steht. Daher können sie Informationen enthalten, die für Ihr Gerät nicht relevant sind. Informieren Sie sich ggf. im Datenblatt Ihres Geräts, welche Funktionen es unterstützt.

Wenn Sie den Webfilter verwenden wollen, müssen Sie mindestens Release 10.2.8 verwenden, da FlashStart eine Serverumstellung vorgenommen hat. Ohne Update funktionieren Suchmaschinenanfragen (z. B. Google) nicht mehr.

1 Release 10.2.12 Patch 1

1.1 Sicherheitsrelevante Änderungen

-

1.2 Verbesserungen / Fehlerkorrekturen

- **Korrigierte WLAN-Client-Anwesenheitsbenachrichtigung im Ethernet-LAN (ER#6163) –** In der W1001n/Wx003n/Wx003ac-Serie, der RSxx3-Serie und be.IP-Serie mit integriertem WLAN meldete der Access-Point die Anwesenheit von WLAN-Clients zu früh bereits während der Assoziierung im Ethernet-LAN (via LLC-Frames), anstatt erst nach erfolgreicher Authentifizierung. Dies konnte sporadische IP-Netzwerkverbindungsprobleme von WLAN-Clients, insbesondere beim Roaming von einem AP zum nächsten, zur Folge haben.
- **Behebung gelegentlicher dauerhafter WLAN-Ausfälle nach einem Radar-Ereignis (ER#654, ER#3349) –** Unter bestimmten Umständen konnte es bei der W1001n/Wx003n/Wx003ac-Serie, der RSxx3-Serie und be.IP-Serie mit integriertem WLAN passieren, dass im 5GHz-Band im Betrieb auf DFS-Kanälen (alle 5GHz-Kanäle ab Kanal 52) nach der Erkennung eines Radar-Signals oder einer anderen Interferenz das WLAN dauerhaft bis zu einem Neustart des Geräts aufhörte zu senden. Das passierte selbst dann, wenn der Access-Point noch auf einen freien Kanal hätte wechseln können oder die gesetzliche Wartezeit von 30 Minuten abgelaufen war. Dieser Fehler war nicht über den WLAN-Controller feststellbar, sondern nur vor Ort, da der Access-Point auch im Fehlerfall das WLAN-Radio als betriebsbereit meldete.
- **Fehlerbehebung in der IPv6-Adresszuweisung via DHCPv6 (ER#5971) –** Im DHCPv6-Client wurden im Non-Rapid-Commit-Fall die IANA- und IAPD-Sektion (die zuvor mit der DHCPv6-Solicit-Nachricht empfangen wurden) nicht in die darauf folgende ausgehende DHCPv6-Request-Nachricht umkopiert. Dies verursachte IPv6-Verbindungsprobleme bei manchen Providern wie „Deutsche Glasfaser“.
- **Zusätzliche weitere DHCP-Optionen werden nicht mehr bei der IP/MAC-Bindung mitgebunden (ER#6205) –** Im GUI-Menü **Lokale Dienste > DHCP-Server > IP/MAC-Bindung** wurde bei der **statischten IP/MAC-Bindung** (unsichtbar für den Anwender) zusätzlich zur IP/MAC-Bindung weitere DHCP-

Optionen (DNS-Server, Default-Gateway etc.) auf die DHCP-Client-MAC-Adresse gebunden. Dies verursachte bei diesen DHCP-Clients bei späteren Änderungen dieser **DHCP-Optionen im DHCP-Server** Netzwerkprobleme. *Achtung: Bestehende IP/MAC-Bindungen werden nicht automatisch beim Update konvertiert. Nach dem Firmware-Update entfernen sie bitte diese Einträge und setzen sie sie anschließend wieder, um sie zu korrigieren.*

- **Fehlerbehebung bei mehreren DynDNS-Accounts für dieselbe Schnittstelle (ER#5411) –** Unter bestimmten Umständen (insbesondere bei Glasfaseranschlüssen), funktionierte das Update von mehreren **DynDNS-Accounts** für dieselbe Schnittstelle nach einem Neustart des Routers nicht. Im Fehlerfall funktionierte nur der erste DynDNS-Account, das IP-Update der weiteren Accounts schlug fehl.
- **Fehlerkorrektur in der Telefonanlagenkonfiguration beim Hinzufügen eines neuen VoIP-Telefons (ER#3419) –** Unter bestimmten Umständen (insbesondere wenn eine VPN-Verbindung bestand) schlug das Anlegen eines neuen VoIP-Telefons im GUI-Menü **Assistenten > Telefonie > Endgeräte > NEU** mit einer Fehlermeldung fehl.
- **Fehlerbehebung in der Telefonanlage bei Early-Media nach SIP-Forking (ER#6044) –** Nach Erhalt mehrerer Anrufereignisnachrichten vom Provider (SIP-Forking) wurde der externe Early-Media-Rufton nicht immer an einen internen SIP-Teilnehmer weitergeleitet, stattdessen war in diesem Fall nur der lokale Rufton für den Anrufer zu hören.
- **Korrigierte VoIP-Ereignisnachrichtenüberprüfung in der Telefonanlage (ER#6292) –** Unter bestimmten Umständen wurde eine RTCP-Goodbye-Nachricht irrtümlich vom WAN ins LAN weitergeleitet.
- **Sende RTP-Idle-Ton bei Weiterleitung eines externen Anrufs an eine externe Nummer (ER#6148) -** Unter bestimmten Umständen funktionierte bei eingehenden externen Anrufen (insbesondere aus dem T-Mobile-Netz) an der Telefonanlage unter anderem die **Follow-me**-Funktion nicht korrekt, falls diese ebenfalls an einen externen Teilnehmer weiterleiten sollte.
- **Fehlerbehebung bei DNS-Dekodierung in der Telefonanlage (ER#6276) –** Voicemail E-Mails konnten von der Telefonanlage aufgrund eines DNS-Dekodierfehlers nicht an „smtp.office365.com“ (und möglicherweise weitere) zugestellt werden.
- **Behebung eines kleinen Speicherlecks im DNS-Resolver (ER#4418) -** Unter bestimmten Umständen verursachte der DNS-Resolver ein kleines Speicherleck, da er manchmal den Arbeitsspeicher veralteter ipDnsDynamicTable-Einträge nicht wieder freigab.

2 Release 10.2.12

2.1 Sicherheitsrelevante Änderungen

- Es wurden Änderungen zum Schutz vor sogenannten Cross Domain Injections vorgenommen (siehe https://xdi-attack.net).

2.2 Verbesserungen / Fehlerkorrekturen

- **Erweitertes WLAN Controller Lizenzlimit** - Für alle BOSS basierten be.IP Geräte wurde die Anzahl der maximal verwaltbaren Access Points auf 48 erhöht. Für BOSS basierte RSxx3-Geräte wurde die Anzahl der maximal verwaltbaren Access Points auf 72 erhöht. Zusätzlich wurde die Anzahl der frei verwaltbaren APs (d. h. ohne die Notwendigkeit, zusätzliche Lizenzen zu erwerben) für alle unterstützten BOSS-basierten Geräte (RXL-Serie, RSxx3-Serie, be.IP-Serie, Rxxx2-Serie, W1001n/Wx003n/Wx003ac-Serie) auf 6 Access Points erhöht.
- **Werkseitige Funkprofile optimiert für Wi-Fi 6 Access Points (#5592)** - In den werkseitigen Standardeinstellungen sind die Funkprofile jetzt für Wi-Fi 6 Access Points (W2044ax und W2022ax) optimiert und haben standardmäßig den Wireless-Modus 802.11ax und 4 Spatial Streams aktiviert.
  Wie immer, wenn ein Bintec Access Point diese Einstellungen nicht unterstützt, wählt er automatisch eine Einstellung, die der übertragenen Konfiguration am nächsten kommt.
  Darüber hinaus wurde der werkseitig voreingestellte Kanalplan im 2,4GHz-Funkprofil von *World Mode* (1, 6, 11) auf *ETSI Mode* (1, 5, 9, 13) geändert, um eine optimale Leistung im überfüllten 2,4GHz-Frequenzband in Europa zu gewährleisten. Im 5GHz-Band wurde der werkseitig voreingestellte Kanalplan für alle Geräte außer der be.IP-Serie vom Plan *Keine Outdoor-Kanäle* auf den breiteren Plan *Keine Wetterradarkanäle* geändert.
  Beachten Sie, dass viele Smart TV WLAN-Clients und einige andere ältere WLAN-Clients mit 5GHz-Unterstützung maximal den Plan Keine Outdoor-Kanäle *unterstützen.*
  Gespeicherte WLAN-Controller-Konfigurationen werden beim Update durch diese Änderungen an den Werkseinstellungen nicht verändert.
- **Verbesserungen im WLAN Controller GUI** - Zahlreiche Verbesserungen wurden in den Bereichen Access Point Management und Monitoring vorgenommen:
  - **Verbesserte WLAN-Netzwerkübersicht und mehr Verschlüsselungsmethoden im WLC-Assistenten auswählbar** - Im GUI-Menü **Assistenten > WLAN (WLC)** zeigt die Übersichtsseite **WLAN-Netzwerke** nun den Gesamtstatus aller verwalteten Access Points, die Anzahl der mit allen verwalteten WLAN-Netzwerken verbundenen WLAN-Clients und die konfigurierte Sicherheit jedes WLAN-Netzwerks an. Auf der Bearbeitungsseite dieses Assistenten können weitere Verschlüsselungsmethoden ausgewählt werden (neben *Inaktiv* und *WPA 2 PSK, OWE Transition*, *OWE*, *WPA 2 und WPA 3 PSK* ist auch *WPA 3 PSK* hinzugekommen).
    Verschlüsselungsmethoden mit OWE und WPA 3 werden nur von OSDx-basierten Access Points unterstützt.
  - **Gelegentlich fehlende Funk- und VSS-Profilzuweisung nach WLAN-Einrichtung über den WLC-Assistenten (#4660)** - Bei der Ersteinrichtung des WLAN-Controllers über das GUI-Menü **Assistenten > WLAN (WLC)** konnte es vorkommen, dass einige

erkannte Access Points nicht korrekt verwaltet wurden. In diesem Fall hatten diese Access Points entweder kein Funkprofil und kein VSS-Profil zugewiesen, oder sie hatten jedes VSS-Profil doppelt auf jedem Funkmodul zugewiesen.

- **Verbesserte und erweiterte Seite Allgemeine Einstellungen** - Im GUI-Menü **Wireless LAN Controller > Controller-Konfiguration > Allgemein** wurden die verfügbaren Einstellungen zur besseren Übersichtlichkeit neu geordnet und um erweiterte Einstellungen ergänzt:
  Die Option **Verwalteter AP-Standort wurde** im Abschnitt **Erweiterte Einstellungen** in **Verwaltete APs-Verbindungszeit-überschreitungen** umbenannt, und die verfügbaren Werte wurden von *Lokal (LAN)* und *Fern (WAN)* in *Streng* und *Locker* umbenannt und um ein *benutzerdefiniertes* Schema erweitert. Für alle Werte gibt es eine detaillierte Beschreibung ihrer jeweiligen Auswirkungen. Darüber hinaus können in den erweiterten Einstellungen die Optionen **WLAN Controller Debug Level**, **Update Intervall für Statistiken von verwalteten APs**, **Alte Berichte zu Nachbar-APs aufbewahren für** und **Initialisierung der AP-Verwaltung** konfiguriert werden. Zuvor waren diese neuen Einstellungen nur über die SNMP-Shell verfügbar.
- **Autoprofile können nun aktiviert und deaktiviert werden** - In der Übersichtsseite des Menüs **Wireless LAN Controller > Controller-Konfiguration > AP-Autoprofil** können nun einzelne Autoprofileinträge über die neue Spalte **Aktion** aktiviert und deaktiviert werden
  Diese Einstellung gilt - wie alles in den Autoprofileinstellungen - nur für neu erkannte Access Points und nicht für bereits verwaltete.
- **Standard-Radius-Server für WPA-Enterprise-Netzwerke konfigurierbar** - Für WPA-Enterprise-VSS-Profile kann der **Standard-Radius-Server** für jeden Eintrag in den Menüs **Wireless LAN Controller > Controller-Konfiguration > AP-Autoprofil > Bearbeiten** und **Wireless LAN Controller > AP-Konfiguration > Access Points > Bearbeiten** ausgewählt werden**.** Er kann also korrigiert werden, wenn die Referenz in einem Eintrag fehlt. Bisher war es nicht möglich, ein funktionierendes WPA-Enterprise-Netzwerk über Autoprofile auszurollen, und auf der Seite **Access Point** wurden diese Einstellungen im Hintergrund von der GUI vorgenommen. Es konnte dann passieren, dass eine fehlerhafte WPA Enterprise-Konfiguration nicht erkannt wurde.
  Falls Sie WPA Enterprise-gesicherte VSS-Profile verwenden, stellen Sie sicher, dass alle konfigurierten Autoprofile und Access Points auf Ihren konfigurierten Standard-Radius-Server verweisen, und fügen Sie den Verweis hinzu, falls er nicht vorhanden ist.
- **Neuer Sicherheitsmodus *WPA 3 Enterprise CNSA* für hochsichere WLAN-Netzwerke** - Der **Sicherheitsmodus** *WPA 3 Enterprise CNSA* wurde dem GUI-Menü **Wireless LAN Controller >**

AP-Konfiguration > Drahtlose Netzwerke (VSS) > Bearbeiten hinzugefügt. *WPA 3 Enterprise CNSA* ist ein erweiterter WPA 3 Enterprise-Modus für hochsichere Umgebungen.
Die Wi-Fi Alliance nennt diesen Sicherheitsmodus *WPA3-Enterprise mit 192-Bit-Modus,* und es handelt sich trotz der ähnlichen Namensgebung um einen völlig anderen Sicherheitsmodus als den üblichen **WPA3-Enterprise**. **WPA 3 Enterprise CNSA** erfordert von WLAN-Clients die Unterstützung von SHA384 für das Key-Hashing, AES-GCMP-256 für die Verschlüsselung, Protected Management Frames (802.11w), Authentifizierung mit EAP-TLS unter Verwendung des Elliptic Curve Diffie-Hellman (ECDH) Austauschs, den Elliptic Curve Digital Signature Algorithm (ECDSA) unter Verwendung einer elliptischen Kurve mit 384 Bit und schließlich einen Radius-Server, der diese Form der Authentifizierung bereitstellt und durchsetzt.
Derzeit unterstützen nur wenige WLAN-Client-Geräte diesen Hochsicherheitsmodus. Im Gegensatz dazu erzwingt der grundlegende WPA3-Enterprise-Modus nur das Minimum von AES-CCMP-128-Verschlüsselung und Protected Management Frames gegenüber dem WPA2-Enterprise-Modus.
WPA 3 Enterprise CNSA wird nur von OSDx-basierten Access Points mit Systemsoftwareversion 2.4.1.1 oder höher unterstützt.

- **Verbesserte WLAN-Controller-Übersicht** - Das Dashboard im Menü **Wireless LAN Controller > Überwachung > WLAN-Controller** wurde zur besseren Übersichtlichkeit neu angeordnet, und das Feld **Übersicht** wurde um Statistiken über die Betriebszustände von **Funkmodulen**, **Drahtlosnetzwerken** und **aktiven Clients** aller verwalteten Access Points erweitert.
- **Neue Seite zur Überwachung der Funkmodule** - Das Menü **Wireless LAN Controller > Überwachung > Access Points** wurde in die Seiten **Access Points** und **Funkmodule aufgeteilt,** die mehr relevante Informationen anzeigen.
  Die neue Seite **Access Points** enthält keine Funkmodulinformationen mehr, sondern zeigt nun zusätzlich die **CPU-Auslastung**, die **Speichernutzung** und die **ETH-Verbindungsgeschwindigkeit** jedes verwalteten Access Points an, was für die Fehlersuche und das Auffinden von Problemen mit Ethernet-Kabeln und Ethernet-Switch-Ports im Netzwerk nützlich ist.
  Die neue Seite **Funkmodule** zeigt alle Funkmodule der verwalteten Access Points an. Zusätzlich zu allen bisher verfügbaren Informationen zu den Funkmodulen zeigt sie die **Kanalauslastung**, die Anzahl der **Radarerkennungen**, die verbundenen **Clients**, einen Zähler für **DL-** und **UL-Bytes** und den **Status der** Funkmodule. Diese Statistiken helfen, den WLAN-Funkstatus für jeden verwalteten Access Point genauer als bisher zu überwachen und Fehler zu beheben.
  Die Kanalauslastung wird von allen OSDx-basierten Access Points

und von 802.11ac-fähigen BOSS Access Points (z. B. W2003ac) gemeldet, jedoch nicht von BOSS Access Points, die maximal 802.11n unterstützen (z. B. W1001n oder das interne Funkmodul von be.IP Plus).

- **Anzeige des verwendeten Sicherheitsmodus für aktive Clients (#4259)** - Der von den angeschlossenen WLAN-Clients tatsächlich verwendete **Sicherheitsmodus** wird nun im Menü **Wireless LAN Controller > Überwachung > Aktive Clients** angezeigt. Diese Information ist hilfreich in WLAN-Netzwerken, in denen mehrere Sicherheitseinstellungen verfügbar sind, um zu erkennen, welche Sicherheitseinstellung von welchem WLAN-Client verwendet wird. So können Sie z. B. in einem WLAN-Netzwerk mit gemischtem Modus aus *WPA 2 und WPA 3* jetzt sehen, welche verbundenen Clients WPA 3 unterstützen und welche WPA 2 benötigen.
  Dieses neue Feld wird nur von OSDx-basierten Access Points mit der Systemsoftware-Version 3.2.1.1 oder höher angezeigt.
- **Falsche Zahlendimension für Durchsatzgrafik in der Detailseite Aktive Clients (#4139)** - Im Menü **Wireless LAN Controller > Überwachung > Aktive Clients > Details** wird die Zahlendimension der Durchsatzgrafik nun dynamisch entsprechend der aktuellen Durchsatzdatenrate des WLAN-Clients angepasst.
- **Klarere und konsistentere Textbeschriftungen für die Datenrichtung auf den WLAN-Controller-Überwachungsseiten** - Auf allen WLAN-Controller-Überwachungsseiten wurden die Beschriftungen des Byte-Zählers und des Durchsatzdiagramms für beide Richtungen von **Tx (Transmit) Rx (Receive)** in **DL (Downlink)** und **UL (Uplink)** geändert. In einem WLAN-Controller-Kontext sorgten **Tx** und **Rx** für Verwirrung, da sie von der Perspektive abhängen - entweder der eines verwalteten APs oder der des aktiven Clients.
- **Verbesserungen und Fehlerkorrekturen bei der Überwachung von Nachbar-APs (#5515, #5524)** - Die Felder **Radio Fingerprint** und Access Point **Type** wurden in das Menü **Wireless LAN Controller > Neighbor Monitoring > Neighbor APs aufgenommen**.
  Die Anzeige aller Felder kann nun gefiltert werden, und standardmäßig werden die Einträge der benachbarten Access Points nach ihrem **Radio Fingerprint** sortiert, um einen besseren Überblick über die WLAN-Nachbarschaft zu erhalten.
  Alle Einträge mit demselben **Radio Fingerprint** stammen mit hoher Wahrscheinlichkeit von demselben Neighbor Access Point. Dies ermöglicht es, mehrere SSIDs zu identifizieren, die vom selben Nachbarn erstellt wurden und welche Nachbar-SSIDs zusammengehören, und es ermöglicht es, die tatsächliche Anzahl der Nachbar-Access Points zu bestimmen.
  Das Feld **Typ** zeigt an, ob der Nachbar im Access Point-, Mesh- oder Ad-hoc-Modus arbeitet.
  Mesh-Nachbarn werden nur von OSDx-basierten Access Points mit

Systemsoftware Version 3.2.1.2 oder höher erkannt, BOSS-basierte Access Points erkennen Mesh-Nachbarn weiterhin als Ad-hoc-Typen und sehen die Mesh-ID nicht.
Insbesondere Mesh-Nachbarn können eine hohe Auslastung auf den von ihnen genutzten Kanälen verursachen, da sie die Backbone-Verbindung in dieser Art von WLAN-Netzwerken darstellen.
Die neuen Felder ermöglichen eine einfachere Identifizierung von Engpässen in der WLAN-Durchsatzleistung, die durch WLAN-Nachbarn verursacht werden.
Darüber hinaus wurde das Feld **Channel** so erweitert, dass nun immer der aktuelle Wireless-Modus und die Bandbreite des benachbarten Access Points in einer Kurzschreibweise sowie der Name des Wireless-Modus in einem Tooltip angezeigt werden.
OSDx-basierte Access Points benötigen die Systemsoftware Version 3.2.1.1 oder höher, BOSS-basierte Access Points benötigen die Systemsoftware Version 10.2.10 Patch 1 oder höher, um den Wireless-Modus der Nachbar-Access Points zu melden.
  - **Seite zur Überwachung von Rogue Access Points -** Die fehlende Schaltfläche **ÜBERNEHMEN** für die Annahme bekannter Rogue Access Points wurde im Menü **Wireless LAN Controller > Neighbor Monitoring > Rogue APs** hinzugefügt.
  - **Fehlerkorrekturen auf der Seite Firmware-Wartung -** Die Aktion **Save configuration with state information** wurde im Menü **Wireless LAN Controller > Firmware-Wartung** in **Informationen für den Support umbenannt**, und die Behandlung des URL-Eingabefelds wurde korrigiert, so dass das Protokoll-Präfix nicht zweimal hinzugefügt wird, wenn die URL mit dem Protokoll-Präfix angegeben wurde.
  - **Beim Zugriff auf einige WLC-Menüs schreibt die GUI "NCI Alert"-Meldungen ins Syslog (#4859)** - Dieses Problem wurde behoben.
  - **Neues vordefiniertes E-Mail-Alarm-Ereignis** - Das neue Ereignis *Verwalteter AP-Konfigurationsfehler wurde* dem Menü **Externe Berichterstellung > Benachrichtigungsdienst > Benachrichtigungsempfänger > Bearbeiten/Neu** hinzugefügt.
    Dieser vordefinierte E-Mail-Alarm sendet alle Konfigurationsfehlermeldungen, die vom verwalteten Access Point gemeldet werden. Dieser Alarm vereinfacht die Erkennung und Korrektur von Konfigurationsfehlern des Benutzers, insbesondere wenn unvollständige oder inkompatible WLAN-Einstellungen angewendet werden - ein Fehler, der durch die Benutzeroberfläche nicht verhindert werden kann.
- **DHCP-Server ignorierte einige spezielle DHCP-Anfragen (#6110)** - Der interne DHCP-Server ignorierte fälschlicherweise Client-DHCP-Anfragen an IP-Unicast (an die IP-Adresse des DHCP-Servers) mit der Ethernet-Broadcast-Zieladresse (FF:FF:FF:FF:FF:FF).

- **Fehler im DHCP Relay (#6036)** - Unicast Replies waren nicht vollständig RFC-konform, was zu Problemen mit Antworten auf DHCP-Anfragen führen konnte.
- **Gesprächsabbruch (#6111)** – Es konnte vorkommen, dass bei bereits laufenden Anrufen an einem Anschluss der Telekom ein Gesprächsabbruch seitens der Plattform ausgelöst wurde.
- **Anrufe fehlgeschlagen (#6060)** - Eingehende Anrufe wurden gelegentlich nach der Signalisierung gleich wieder abgebaut.
- **Kein Rufton (#6048, 6048, 5885, 4538, 3987, 3951, 3117)** - Es konnte vorkommen, dass z. B. im Fall einer Rufweiterleitung kein Rufton zu hören war.

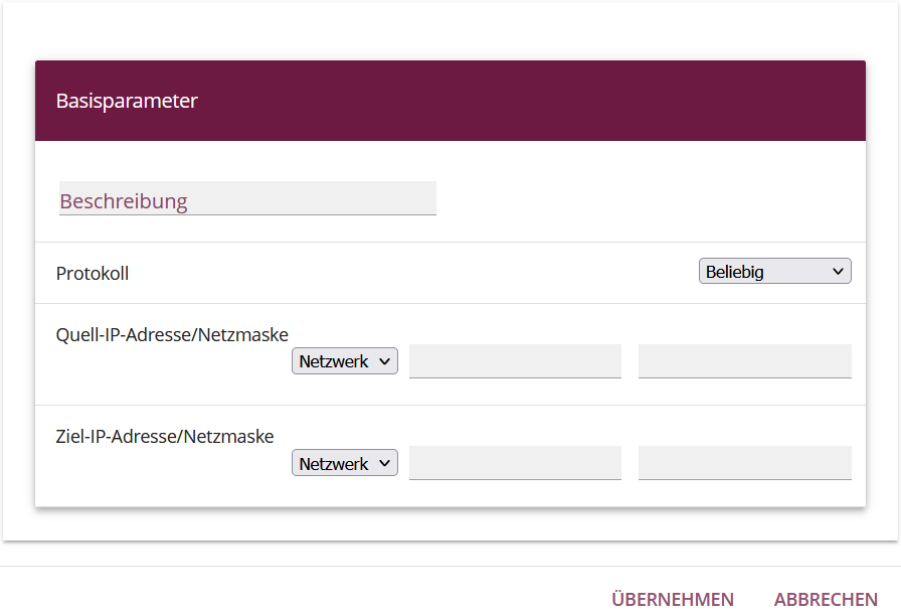
3 Anhang

3.1 Erweiterte Konfiguration von IKEv2-basierten IPSec Peers

Um sicherzustellen, dass bei auf IKEv2 basierenden IPSec-Verbindungen die Aushandlung Verbindungsparameter fehlerfrei funktioniert, empfiehlt es sich die im Folgenden beschriebenen Einstellungen vorzunehmen.

3.1.1 Festlegung des zu tunnelnden Datenverkehrs

Es ist sinnvoll, den Datenverkehr, der tatsächlich über den Tunnel gesendet werden soll, möglichst präzise festzulegen. Dazu können Sie im Menü **VPN > IPSec > IP-Sec-Peers > Bearbeiten > Zusätzlicher Filter des IPv4-Datenverkehrs** eine Eingrenzung des Ziel- und des Quellnetzes vornehmen:



Stellen Sie in diesem Menü sicher, dass die über den Tunnel verbundenen Netze alle IP-Adressen umfassen, die Zugriff auf das entfernte Netzwerk haben sollen, und ebenso alle Adressen, die dort erreicht werden sollen.

Diese Einstellungen sind immer sinnvoll, unabhängig davon, ob im Abschnitt **Erweiterte IPSec-Optionen** der **Startmodus** *Auf Anforderung* oder *Immer aktiv* ausgewählt ist.

3.1.2 Startmodus

Bei IPSec-Verbindungen, die dauerhaft aktiv sein müssen und bei denen der bintec-elmeg-Router die Verbindung initiiert, empfiehlt es sich, den **Startmodus** des Peers im Menü **VPN > IPSec > IPSec-Peers > Bearbeiten > Erweiterte Einstellungen** auf den Wert *Immer aktiv* zu setzen, um einen eindeutigen Zustand der IPSec-Schnittstelle zu gewährleisten:

3.1.3 Eindeutige Rollenverteilung zwischen Client und Server

Bei der Konfiguration einer IPSec-Verbindung sollten Sie stets auf eine klare Rollenverteilung der beiden IPSec-Verbindungspartner (Initiator- oder Responder-

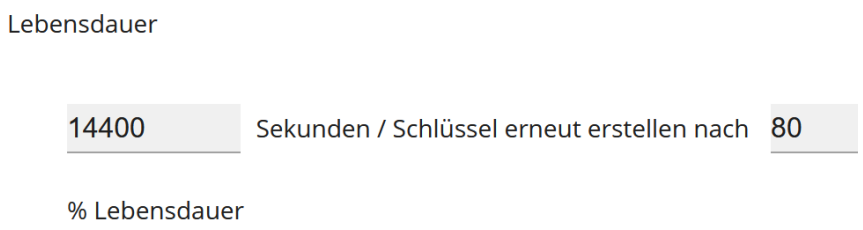
Rolle) achten. Dies ist sowohl für den anfänglichen Verbindungsaufbau als auch für die periodische Neuaushandlung der IPSec-Verbindung wichtig.

Achten Sie daher bei der Konfiguration der **Lebensdauer** im Phase-1- und im Phase-2-Profil darauf, dass der eingestellte Wert auf Initiator-Seite kürzer ist als auf Responder-Seite. So können Sie z. B. für die Phase-1-Lebensdauer des Initiators zwei Drittel der Phase-1-Lebensdauer des Responders einstellen. Verfahren Sie ebenso für die Phase-2-Lebensdauer.

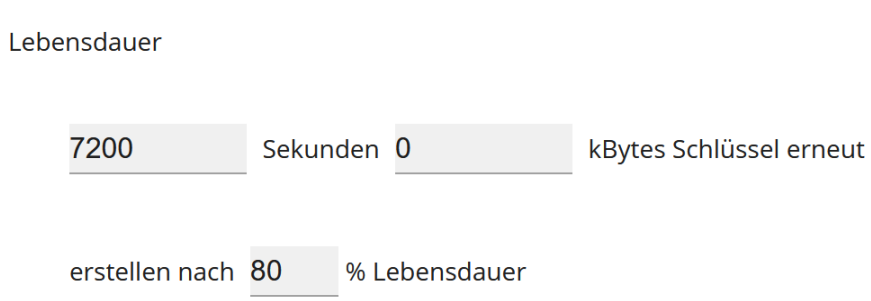
Aufgrund der asymmetrischen Konfiguration der Lebensdauer und der damit verbundenen klaren Rollenverteilung können Sie Kollisionen bei der sich periodisch wiederholenden Neuaushandlung der IPSec-Verbindung vermeiden.

Sie finden die Einstellungen in folgenden Menüs:

- **Internet & Netzwerk > VPN > IPSec > Phase-1-Profile > Bearbeiten**

  Stellen Sie die Werte so ein, dass die Gültigkeit der Phase-1-Parameter auf dem sich einwählenden Client kürzer ist als auf dem Server.
  Achten Sie darauf, dass Sie hier das Profil auswählen, das der betreffende Peer auch tatsächlich verwendet!
- **Internet & Netzwerk > VPN > IPSec > Phase-2-Profile > Bearbeiten**

  Stellen Sie die Werte so ein, dass die Gültigkeit der Phase-2-Parameter auf dem sich einwählenden Client kürzer ist als auf dem Server.
  Achten Sie darauf, dass Sie hier das Profil auswählen, das der betreffende Peer auch tatsächlich verwendet!

Die Gültigkeit der Phase 1 sollte die der Phase 2 deutlich übersteigen!