ads-tec Industrial IT GmbH

Selektiver Routen-Push über Big-LinX VPN

Application Note | IRF1000, IRF3000

Version 1.0

Stand 2026-04-17

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany

Inhaltsverzeichnis

1 Application Note – Selektiver Routen-Push über Big-LinX VPN 3

1.1 Einführung & Anwendungsfall 3
1.2 Systemvoraussetzungen 4
1.2.1 Unterstützte Geräte & Firmware 4
1.2.2 Netzwerkanforderungen 4
1.2.3 Zugang & Berechtigungen 4
1.3 Hintergrund: Wie Routen-Push funktioniert 4
1.4 Konfigurationsschritte 5
1.4.1 Schritt 1 – Betriebsmodus auswählen 5
1.4.2 Schritt 2 – Big-LinX VPN-Verbindung konfigurieren 8
1.4.3 Schritt 3 – Netzwerke für den Push über Big-LinX VPN auswählen 8
1.4.4 Schritt 4 – Einstellungen dauerhaft speichern 9
1.5 Erweiterte Konfiguration 10
1.5.1 Statische Routen über Big-LinX pushen 10
1.5.2 SNAT für VPN-Ziele 10
1.5.3 Paketfilter — Zugriffskontrolle 10
1.6 Fazit 10
1.7 Verwandte Application Notes 10

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany

1 Application Note – Selektiver Routen-Push über Big-LinX VPN

1.1 Einführung & Anwendungsfall

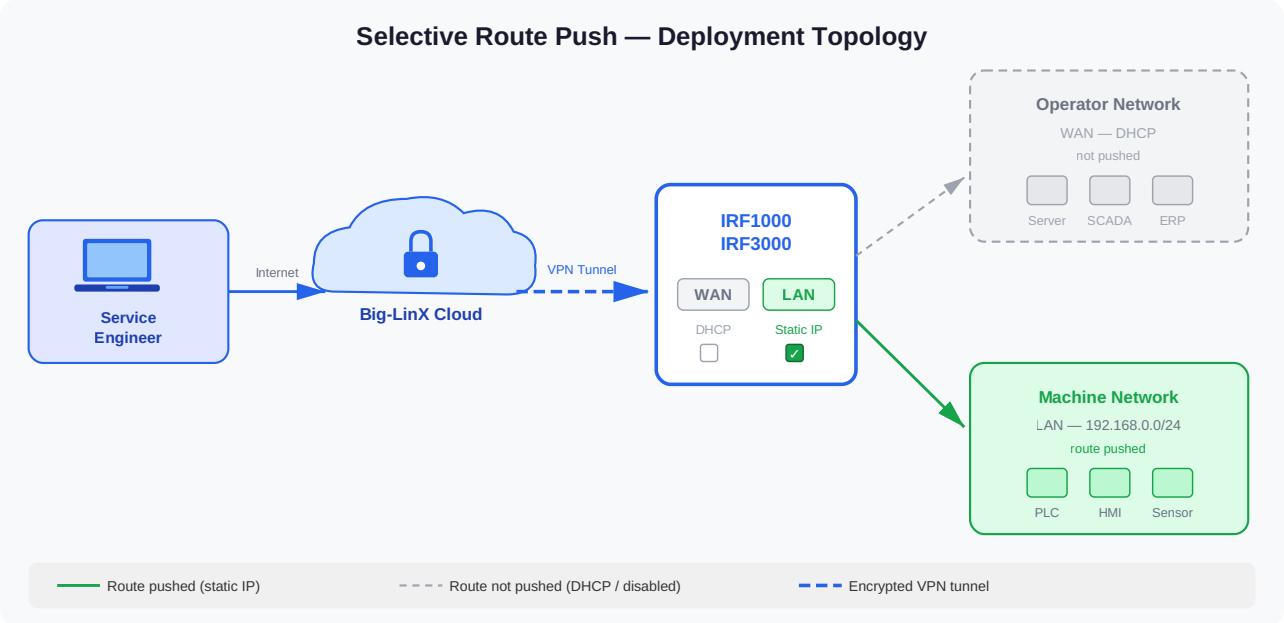
In industriellen Umgebungen wird die IRF-Firewall typischerweise an der Grenze zwischen dem Betreiber-/Fabriknetzwerk (WAN) und dem Maschinennetzwerk (LAN) eingesetzt. Service-Techniker verbinden sich über die Big-LinX Cloud-VPN-Plattform für Wartungsaufgaben aus der Ferne.

Wenn ein Big-LinX VPN-Tunnel aufgebaut wird, kündigt das IRF-Gerät seine lokalen Netzwerke als Routen beim VPN-Peer an. Dies teilt dem entfernten Client mit, welche Netzwerke über den Tunnel erreichbar sind. Bis Firmware 2.2.8 wurden alle Schnittstellen mit einer **statischen IP-Adresse** automatisch als Routen gepusht. Da die WAN-Schnittstelle typischerweise DHCP verwendet, wurde sie in der Regel nicht gepusht — aber jede Schnittstelle mit statischer IP war immer enthalten, ohne Möglichkeit dies zu ändern.

Ab **Firmware 2.2.8** steht eine neue Funktion **Selektiver Routen-Push** zur Verfügung. Die Big-LinX VPN-Konfigurationsseite bietet nun pro Schnittstelle Kontrollkästchen, mit denen Administratoren explizit festlegen können, welche lokalen Netzwerke als Routen durch den Big-LinX VPN-Tunnel angekündigt werden. Jede Schnittstelle kann einzeln ein- oder ausgeschlossen werden.

Typischer Anwendungsfall: Ein Maschinenbauer liefert IRF-Geräte an Endkunden (Betreiber). Die IRF ist mit mehreren Netzwerken verbunden, aber nur eines davon soll für den Fernservice erreichbar sein. Mit dem Selektiven Routen-Push konfiguriert der Administrator genau, welche Netzwerke der VPN-Tunnel ankündigt — so bleibt die Routing-Tabelle auf dem entfernten Client sauber und auf das Notwendige beschränkt.

> **Hinweis:** Der Selektive Routen-Push ist eine **Routing-Komfortfunktion**, kein Sicherheitsmechanismus. VPN-Routen können clientseitig jederzeit von einem Benutzer mit Administratorrechten auf seinem Rechner überschrieben werden. Um den Zugriff auf interne Netzwerke zu kontrollieren, verwenden Sie den **Paketfilter** — das ist die eigentliche Sicherheitsfunktion. Siehe die Application Note Big-LinX Filter für Details.



1.2 Systemvoraussetzungen

1.2.1 Unterstützte Geräte & Firmware

Gerätefamilie	Min. Firmware-Version	Unterstützte Modi
IRF1000	2.2.8	Router-Modus
IRF3000 (IRF34XX, IRF38XX)	2.2.8	Router-Modus, Erweiterter Modus

> **Hinweis:** Alle Gerätevarianten sind auch mit integriertem LTE erhältlich (z. B. IRF1421, IRF3421, IRF3821). Die Funktion Selektiver Routen-Push wird unabhängig davon unterstützt, ob LTE vorhanden ist.

1.2.2 Netzwerkanforderungen

- Stabile Internetverbindung an der WAN-/Uplink-Schnittstelle.
- Big-LinX-Zugang auf der Uplink-Schnittstelle konfiguriert.
- Erforderliche WWH- und VPN-IP-Adressen erreichbar (siehe Big-LinX Portal → Support → Download).
- Erforderliche Ports in der Firewall-Umgebung für den Aufbau des VPN-Tunnels über Big-LinX geöffnet.

1.2.3 Zugang & Berechtigungen

- Administratorzugang zur IRF-Weboberfläche.
- Gültiges Big-LinX Portal-Konto mit entsprechenden Berechtigungen.

1.3 Hintergrund: Wie Routen-Push funktioniert

Wenn ein Big-LinX VPN-Tunnel aufgebaut wird, kündigt das IRF-Gerät seine lokalen Netzwerke als Routen beim VPN-Peer an. Der entfernte Client verwendet diese Routen, um zu bestimmen, welcher Datenverkehr durch den Tunnel gesendet wird.

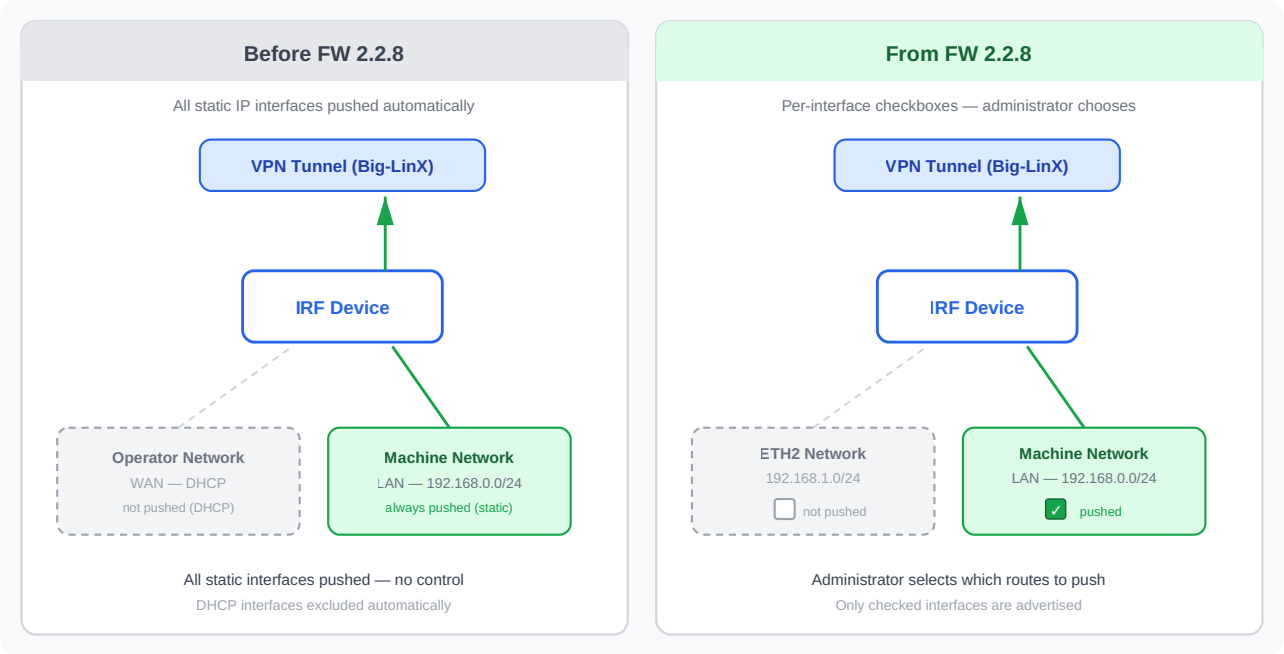
Bisheriges Verhalten (vor 2.2.8): Alle Schnittstellen mit einer statischen IP-Adresse wurden automatisch als Routen gepusht. Schnittstellen mit DHCP (typischerweise WAN) hatten keine feste Netzwerkadresse und wurden nicht gepusht. Es gab keine Möglichkeit, einzelne statische Schnittstellen von der Routen-Ankündigung auszuschließen.

Neues Verhalten (ab 2.2.8): Der Abschnitt **Netzwerk-Routen-Push zu Big-LinX VPN** auf der Big-LinX-Konfigurationsseite zeigt jede Schnittstelle mit einem Kontrollkästchen an. Aktiviert bedeutet, die Route wird gepusht; deaktiviert bedeutet, sie wird nicht gepusht. Dies gibt Administratoren explizite Kontrolle darüber, welche Netzwerke in der Routing-Tabelle des entfernten Clients erscheinen.

Zusätzlich zu Schnittstellennetzwerken können auch einzelne **statische Routen** an Big-LinX VPN-Clients gepusht werden. Jeder statische Routeneintrag auf der Seite **Konfiguration → Netzwerk → IP-Routing** hat ein eigenes Kontrollkästchen **Push zu Big-LinX**. Dies ist nützlich, wenn Geräte hinter der IRF in einem Subnetz liegen, das keiner IRF-Schnittstelle direkt zugewiesen ist (z. B. ein sekundäres Netzwerk hinter einem Managed Switch am LAN-Port).

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany

Hinweis: Schnittstellen, die DHCP verwenden, haben keine feste Netzwerkadresse und ihre Routen werden nie gepusht, unabhängig vom Kontrollkästchen-Status.



1.4 Konfigurationsschritte

1.4.1 Schritt 1 – Betriebsmodus auswählen

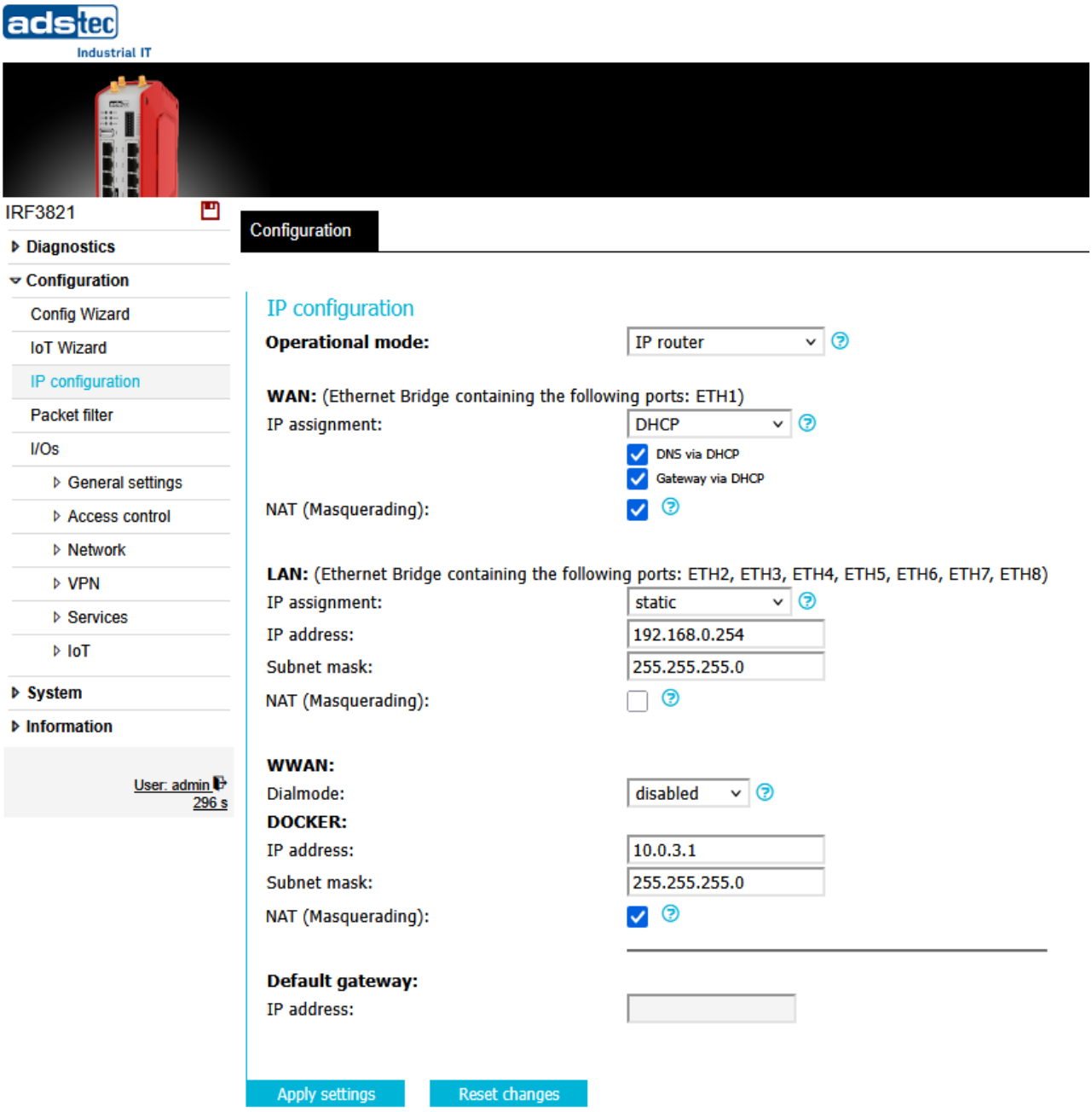
Navigieren Sie zu **Konfiguration** → **IP-Konfiguration** und wählen Sie den gewünschten **Betriebsmodus**.

Router-Modus (IRF1000 und IRF3000)

Im Router-Modus fungiert der WAN-Port als Uplink-Schnittstelle, während alle übrigen LAN-Ports ein einzelnes Netzwerksegment bilden. Die folgenden Netzwerke können selektiv über Big-LinX VPN gepusht werden:

- **IRF1000:** WAN und LAN
- **IRF3000:** WAN (ETH1) und LAN (ETH2–ETH4 für IRF34XX, ETH2–ETH8 für IRF38XX)

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany

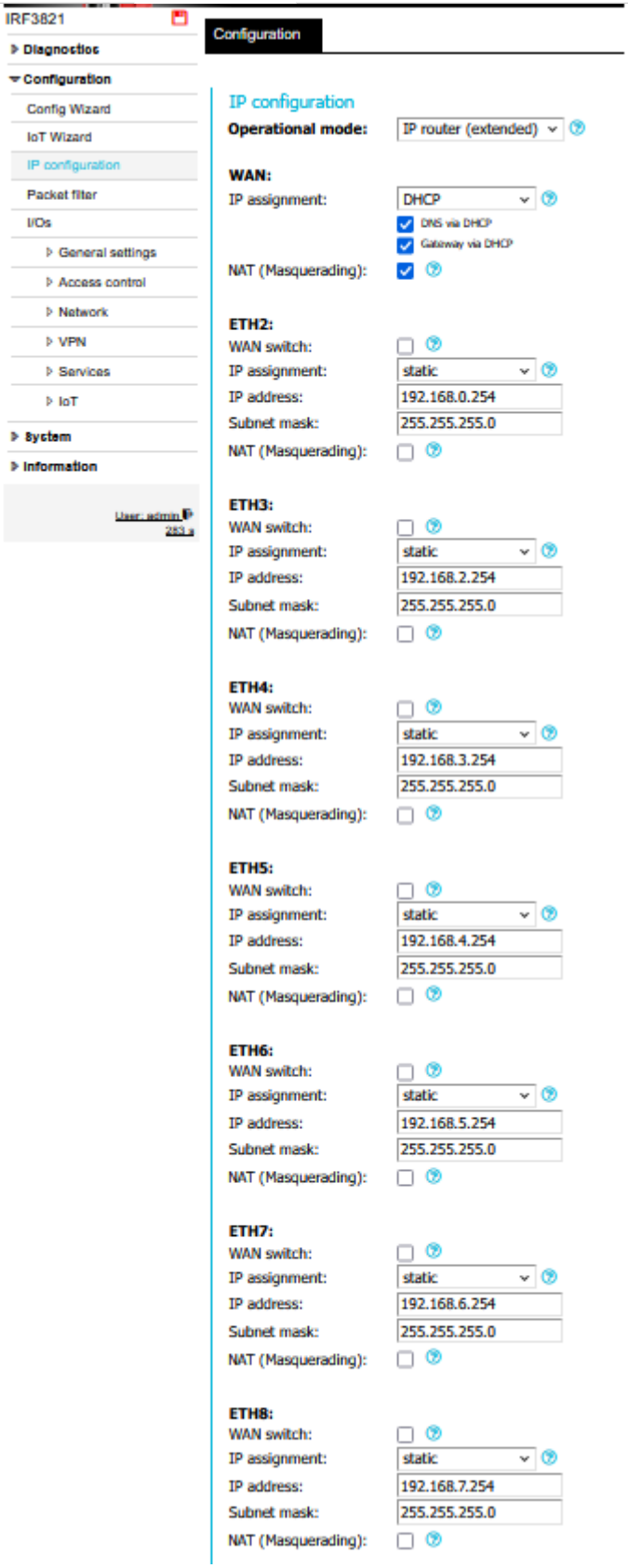


Erweiterter Modus (nur IRF3000)

> **Hinweis:** Der Erweiterte Modus ist ausschließlich auf IRF3000-Geräten (IRF34XX- und IRF38XX-Serien) verfügbar. Er ist nicht auf IRF1000 verfügbar.

Im Erweiterten Modus wird jeder physische Port als unabhängiges Netzwerksegment konfiguriert. Dies ermöglicht eine granulare Steuerung, welche einzelnen Port-Netzwerke über Big-LinX VPN gepusht werden:

- **IRF34XX:** WAN, ETH2, ETH3, ETH4
- **IRF38XX:** WAN, ETH2, ETH3, ETH4, ETH5, ETH6, ETH7, ETH8



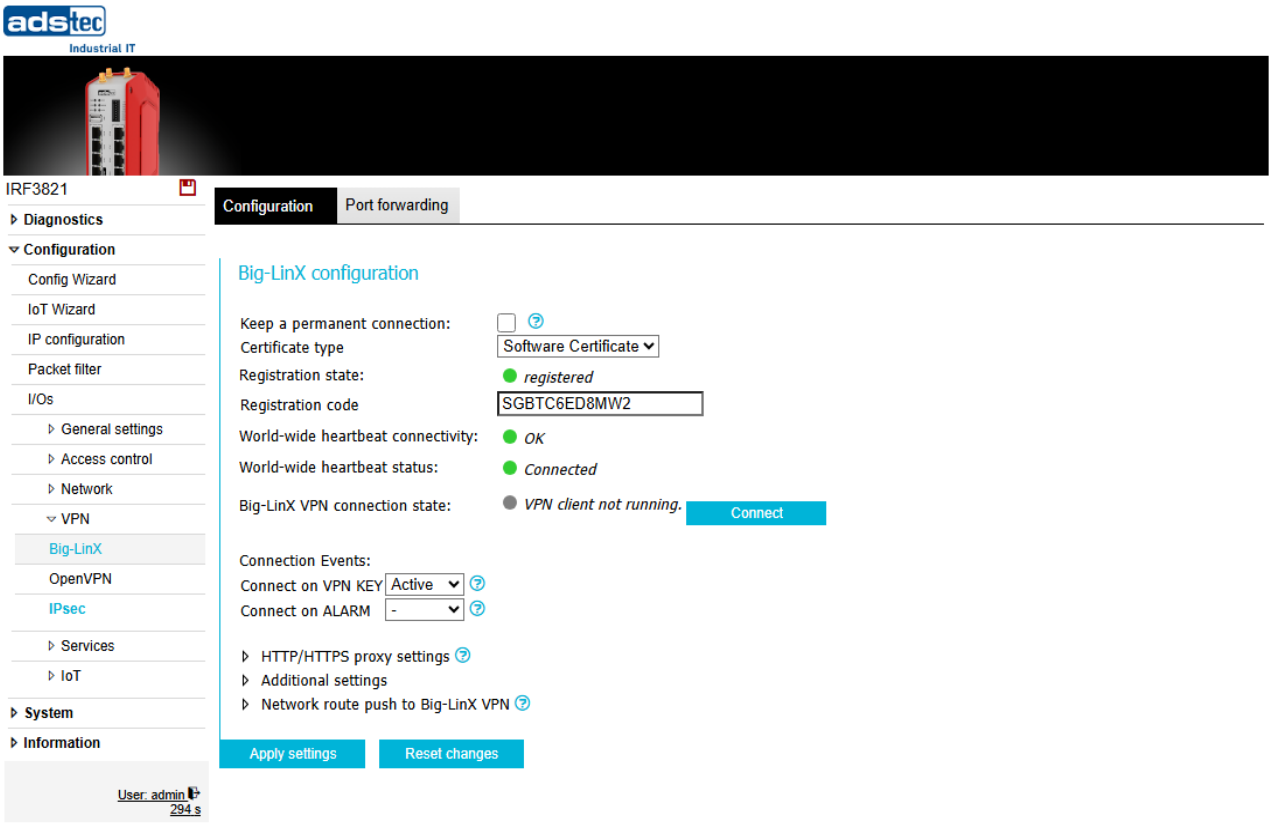
Klicken Sie auf **Einstellungen übernehmen**, um den ausgewählten Betriebsmodus zu aktivieren.

1.4.2 Schritt 2 – Big-LinX VPN-Verbindung konfigurieren

Navigieren Sie zu **Konfiguration** → **VPN** → **Big-LinX**. Wählen Sie Ihren Zertifikatstyp:

- **Software-Zertifikat:** Geben Sie den Registrierungscode manuell ein.
- **Smartcard:** Der Registrierungscode wird automatisch zugewiesen.

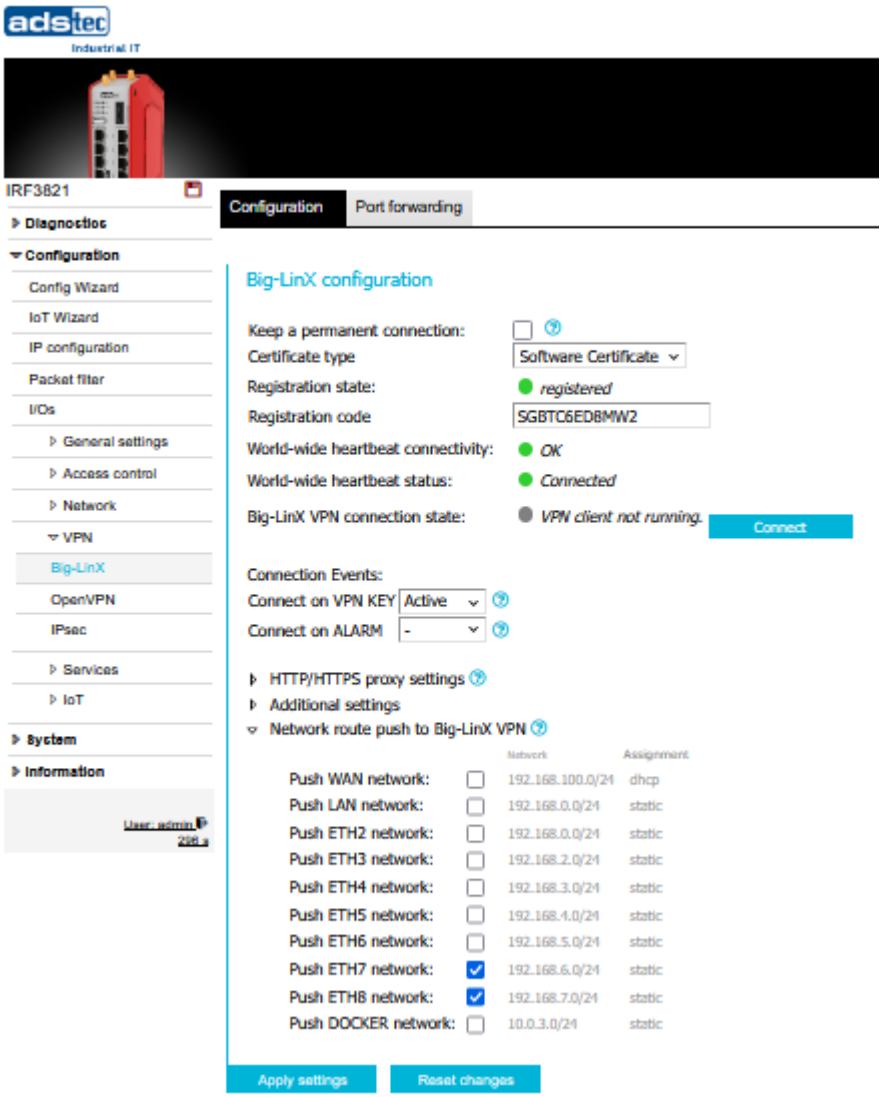
Überprüfen Sie, dass der **Registrierungsstatus** *registriert* und der **World-wide Heartbeat Status** *Verbunden* anzeigt, bevor Sie fortfahren.



1.4.3 Schritt 3 – Netzwerke für den Push über Big-LinX VPN auswählen

Klappen Sie am unteren Ende der Big-LinX-Konfigurationsseite den Abschnitt **„Netzwerk-Routen-Push zu Big-LinX VPN"** durch Anklicken auf.

Es wird eine Liste aller verfügbaren Schnittstellen angezeigt, jeweils mit zugehöriger Netzwerkadresse und Zuweisungstyp (statisch / DHCP). Aktivieren Sie das Kontrollkästchen neben jedem Netzwerk, das als Route durch den Big-LinX VPN-Tunnel angekündigt werden soll. Deaktivieren Sie jedes Netzwerk, das nicht angekündigt werden soll.



Hinweis: Schnittstellen, die DHCP verwenden, haben keine feste Netzwerkadresse. Diese werden in der Liste angezeigt, aber ihre Routen werden **nicht** gepusht, unabhängig vom Kontrollkästchen-Status.

Klicken Sie auf **Einstellungen übernehmen**, um die Konfiguration zu übernehmen.

1.4.4 Schritt 4 – Einstellungen dauerhaft speichern

Wichtig: Ein Klick auf **Einstellungen übernehmen** wendet die Änderungen sofort an, speichert sie jedoch **nicht** dauerhaft. Wird das Gerät ohne Speichern neu gestartet, gehen alle Änderungen verloren.

Um die Konfiguration dauerhaft zu speichern, verwenden Sie eine der folgenden Methoden:

- Klicken Sie auf die Schaltfläche **„und speichern"** (neben Einstellungen übernehmen), **oder**
- Klicken Sie auf das **Diskettensymbol** in der Menüleiste oben rechts und wählen Sie **Einstellungen speichern**.

1.5 Erweiterte Konfiguration

1.5.1 Statische Routen über Big-LinX pushen

Zusätzlich zu Schnittstellennetzwerken können Sie einzelne statische Routen an Big-LinX VPN-Clients pushen. Navigieren Sie zu **Konfiguration** → **Netzwerk** → **IP-Routing**. Jeder statische Routeneintrag hat ein Kontrollkästchen **Push zu Big-LinX**.

Anwendungsfall: Geräte hinter der IRF befinden sich in einem Subnetz, das keiner IRF-Schnittstelle direkt zugewiesen ist — beispielsweise ein sekundäres Netzwerk hinter einem Managed Switch am LAN-Port. Erstellen Sie eine statische Route für dieses Subnetz und aktivieren Sie **Push zu Big-LinX**, damit VPN-Clients es erreichen können.

1.5.2 SNAT für VPN-Ziele

Die Big-LinX-Konfigurationsseite enthält unter den erweiterten Einstellungen ein Feld **SNAT für Ziel**. Wenn aktiviert, wird Source-NAT (Masquerading) auf Datenverkehr angewendet, der für einen bestimmten Server oder ein Subnetz im Big-LinX-Netzwerk bestimmt ist. Dies verhindert, dass der entfernte Endpunkt interne Netzwerkadressen erlernt.

Geben Sie das Ziel in CIDR-Notation an (z. B. `172.16.1.100/32` für einen einzelnen Server, `172.16.1.0/24` für ein Subnetz).

1.5.3 Paketfilter — Zugriffskontrolle

Der Selektive Routen-Push steuert, welche Netzwerke dem VPN-Client *angekündigt* werden, aber die Routen-Ankündigung allein verhindert keinen Zugriff. Ein Benutzer mit Administratorrechten auf seinem Rechner kann Routen jederzeit manuell hinzufügen oder ändern. Um tatsächlich einzuschränken, welche Geräte und Dienste über den VPN-Tunnel erreichbar sind, konfigurieren Sie **Paketfilterregeln** auf der Big-LinX-Schnittstelle.

Detaillierte Schritte finden Sie in der Application Note Big-LinX Filter.

1.6 Fazit

Die Funktion Selektiver Routen-Push gibt Administratoren explizite Kontrolle darüber, welche lokalen Netzwerke als Routen durch den Big-LinX VPN-Tunnel angekündigt werden. Bisher wurden alle Schnittstellen mit statischer IP automatisch gepusht. Jetzt kann jede Schnittstelle einzeln ein- oder ausgeschlossen werden, wodurch die Routing-Tabelle des entfernten Clients sauber und auf das Notwendige beschränkt bleibt.

Die Funktion ist ab **Firmware 2.2.8** auf allen IRF1000- und IRF3000-Geräten, einschließlich LTE-Varianten, verfügbar und wird direkt auf der Big-LinX VPN-Konfigurationsseite über Kontrollkästchen pro Schnittstelle konfiguriert.

1.7 Verwandte Application Notes

Application Note	Relevanz
Big-LinX Filter	Paketfilterregeln zur Zugriffskontrolle über den Big-LinX VPN-Tunnel konfigurieren

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany

Application Note	Relevanz
Eingeschränkter Fernzugriff	Eingeschränkte Benutzerkonten für Fernwartungspersonal erstellen

© ads-tec Industrial IT GmbH • Heinrich-Hertz-Str.1 • 72622 Nürtingen • Germany