GRUNDLEGENDE EINFÜHRUNGSKONZEPTE FÜR IPv6

IPv6, JA GERN – ABER WIE? (UND WIE NICHT)

Carsten Schmoll, 24. November 2014

Fraunhofer FOKUS

GOVERNMENTS ENABLED WITH IPv6 GEN6

European Commission

This project has received funding from the European Union´s

Wir machen Städte schlau

ANNO 2012

SPIEGEL ONLINE NETZWELT

05.06.2012

Start von IPv6

Mittwoch wird das Internet umgestellt

Bild.de

NEUE INTERNET-ADRESSEN

Geht mein Internet bald nicht mehr?

IPV6: DAS MÜSSEN SIE JETZT WISSEN

KLEINE FRAGE VORAB

IPv6

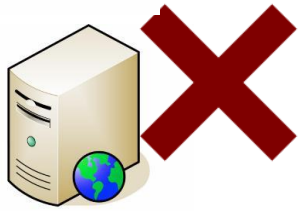
mit / statt / trotz

IPv4 ?

EINFÜHRUNG VON IPv6

- **Von wo kommt IPv6 auf mich zu?**
- **Von innen, von außen, von oben, von unten?**

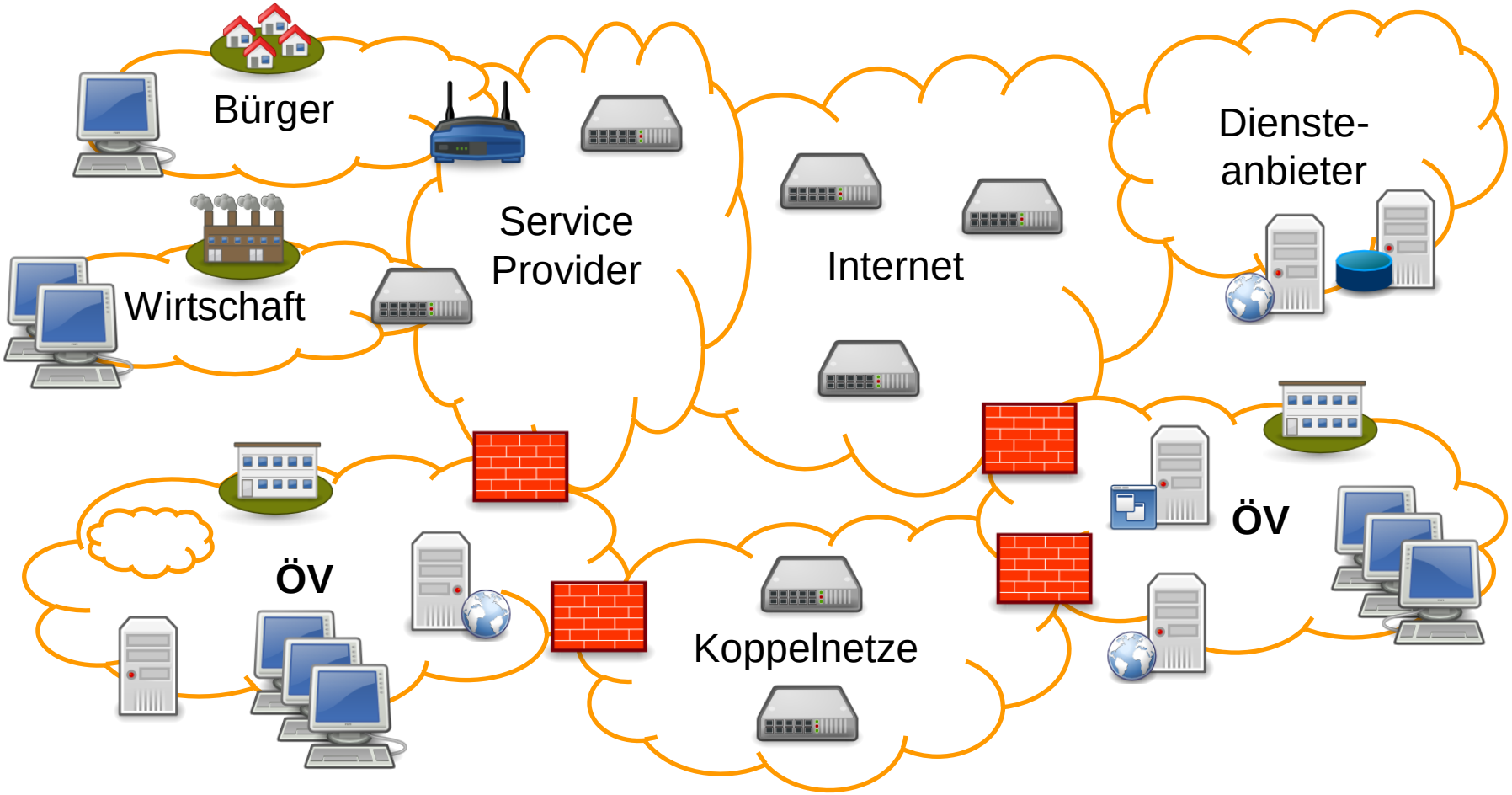
- i.d.R. gilt: „Wenn ich es gar nicht unterstütze, dann kommen auch keine IPv6 Datenpakete auf mich zu.“
  - Ausnahmen bestätigen die Regel, z.B. beim Webhosting



- IPv6 kommt eher als „Anforderung von oben“ auf mich zu
  - Kunden und/oder Projektpartner wollen IPv6 mit Ihnen sprechen
  - Einige E-Mail-Server auf dieser Welt sind schon IPv6-only
  - Bürger bekommen zunehmend IPv6 zu Hause. Bei DS-Lite Technik ist IPv6 nativ verfügbar und IPv4 evtl. eingeschränkt
  - Ich will Internet-of-Things einsetzen und habe keine 10.000 freien IPv4 Adressen mehr verfügbar um jedem Gerät 1 zu geben

© Fraunhofer FOKUS

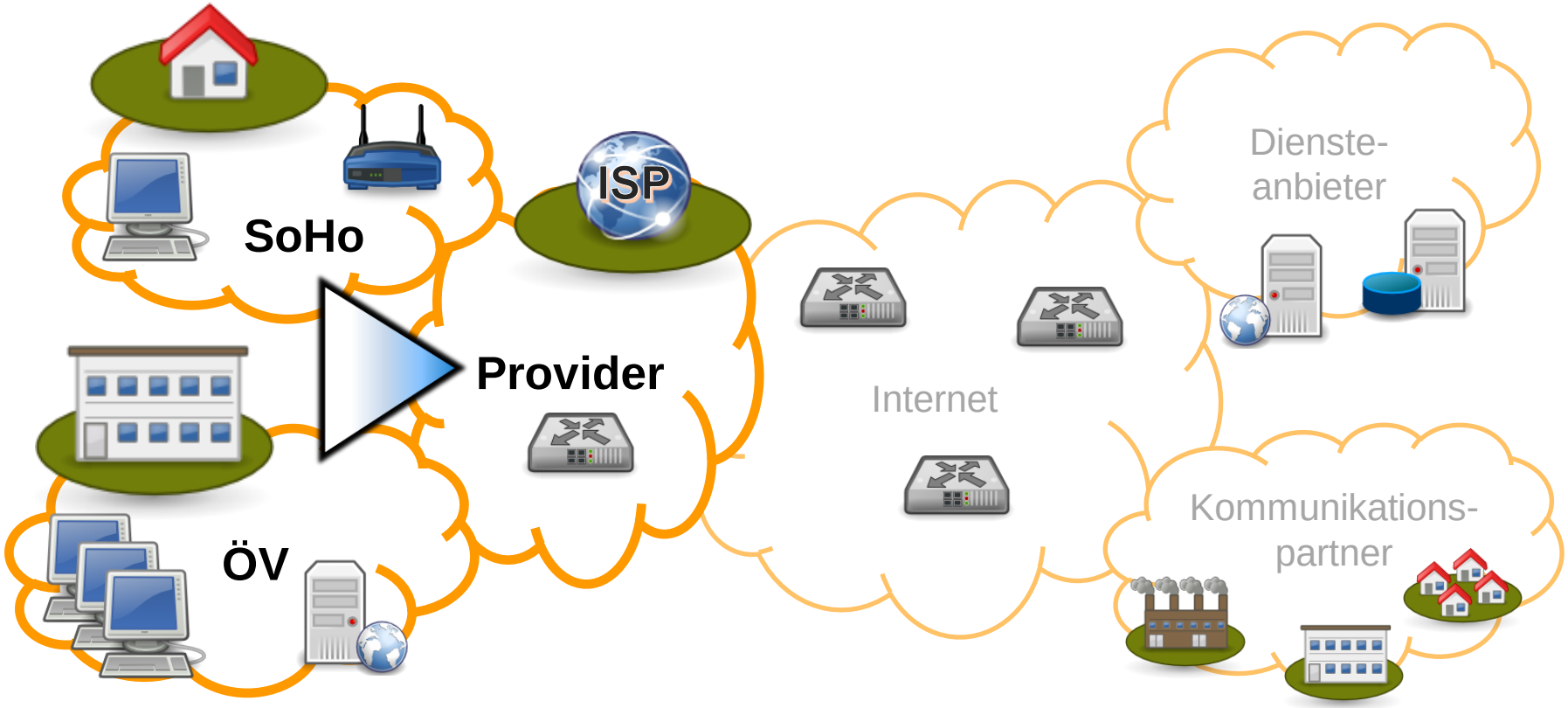
IPv6 KOMMT ÜBERALL…



Fraunhofer FOKUS

© Fraunhofer FOKUS

… AUCH BEI AKTEUREN IM ANSCHLUSSBEREICH



© Fraunhofer FOKUS

KANN ICH DAS NICHT EINFACH EINSCHALTEN?

Eindeutig
JEIN!

- auf Endgeräten: **PC** / **Smartphone** / **Tablets**
- i.allg. JA, oder es ist schon aktiv und wird genutzt, sobald es im Netzwerk zur Verfügung steht

- auf **Servern**, **Gateways**, **Routern** und **Firewalls**
- Oft Ja, wenn das Gerät nicht allzu alt ist;
  IPv6 muss auf Gateways/Routern/Firewalls meist erst manuell eingeschaltet werden

- am **Internet-Anschluss** (DSL, Kabel, WAN / „Internet vom Provider“)
- Muss der Internet-Service-Provider anbieten und aktivieren
- Eigene Infrastruktur übernimmt dies i.allg. nicht (zu Hause ggf. doch automatisch)

- auf **Internet-Backbones** und in kommerziellen **Rechenzentren**
- IPv6 längst aktiv auf internationalen Backbones, in Clouds und bei Web- und Server-Hosting (Kunden kaufen sonst nicht mehr)

© Fraunhofer FOKUS

EIN NEUER STANDARD FÜR JEDES SETUP

Dual Stack

Tunnel

- 6in4
- DS-Lite
- 6to4
- Teredo
- 6rd
- ISATAP
- TunnelBroker

Protokollumsetzung

- SIIT
- NAT64
- *XLAT Framework*
- XLAT 464
- Proxy / ALG

weitere Mechanismen

- VLANs
- NAT
- CGN
- Terminalserver-Zugriff

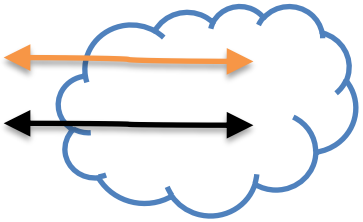
© Fraunhofer FOKUS

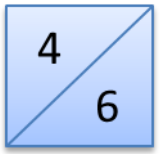
KEINE DIREKTE KOMMUNIKATION ZW. IPv4 UND IPv6

- **IPv4 und IPv6 sind *nicht* zueinander kompatibel**

Mögliche
Lösungstypen

- **Parallel-Betrieb** oder **Tunnel** oder **Zwischen-Systeme** (middleboxes)

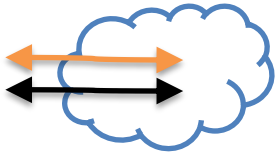




© Fraunhofer FOKUS

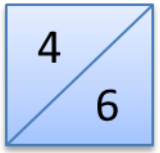
DIE DREI GRUNDLEGENDEN ANSÄTZE

- **Dual Stack** („IPv4 und IPv6 parallel“)
  - Geräte sind über beide Protokolle gleichzeitig erreichbar, automatische / konfigurierbare Auswahl
  - physikalische nicht nötig und nicht empfohlen



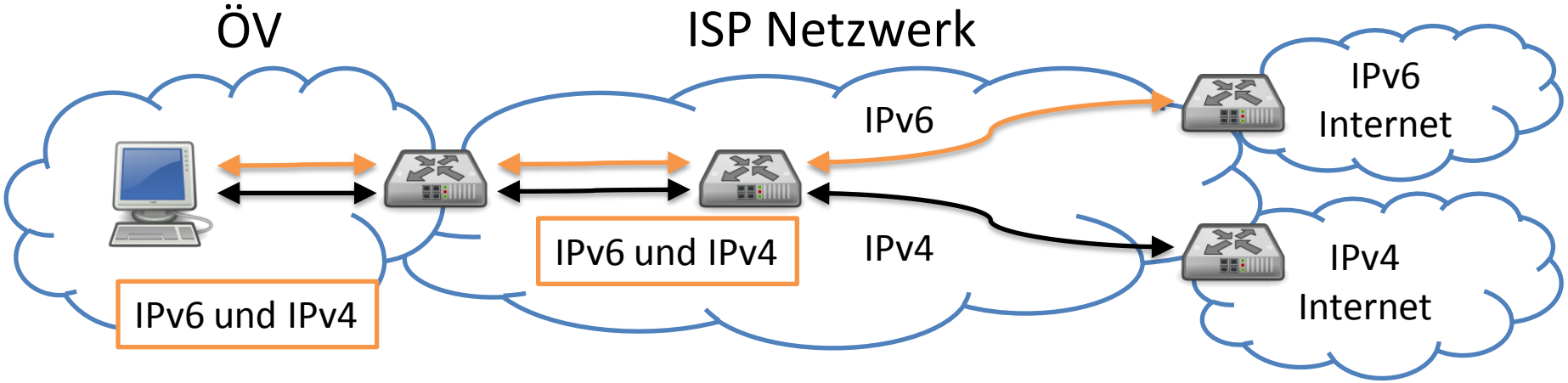
- **Tunnel** („Verbindung von IPv6-Inseln“)
  - Anbindung einzelner IPv4- bzw. IPv6-Inseln
  - Verbindung zwischen mehreren IPv4- bzw. mehreren IPv6-Inseln

- **Protokollumsetzung**
  - auf Netzwerkebene: zwischen IPv4-only- und IPv6-only
  - auf höheren Ebenen: durch Application Layer Gateways (ALGs) oder Proxies (z.B. http-Proxy)



© Fraunhofer FOKUS

DUAL-STACK

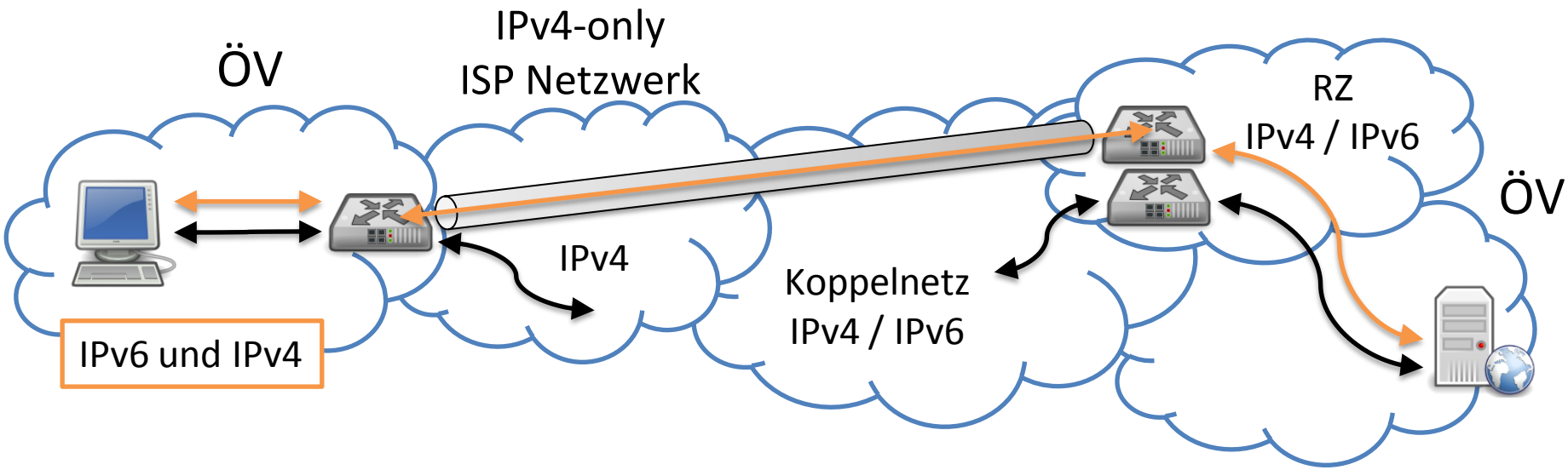


- paralleler Betrieb von IPv4 und IPv6

- universeller Einsatz, im …
- Intranet (bei Anwendungen, Servern, Arbeitsplätzen)
- Internet-Zugang / beim Dienstangebot
- Backbone (heute schon Standard)

© Fraunhofer FOKUS

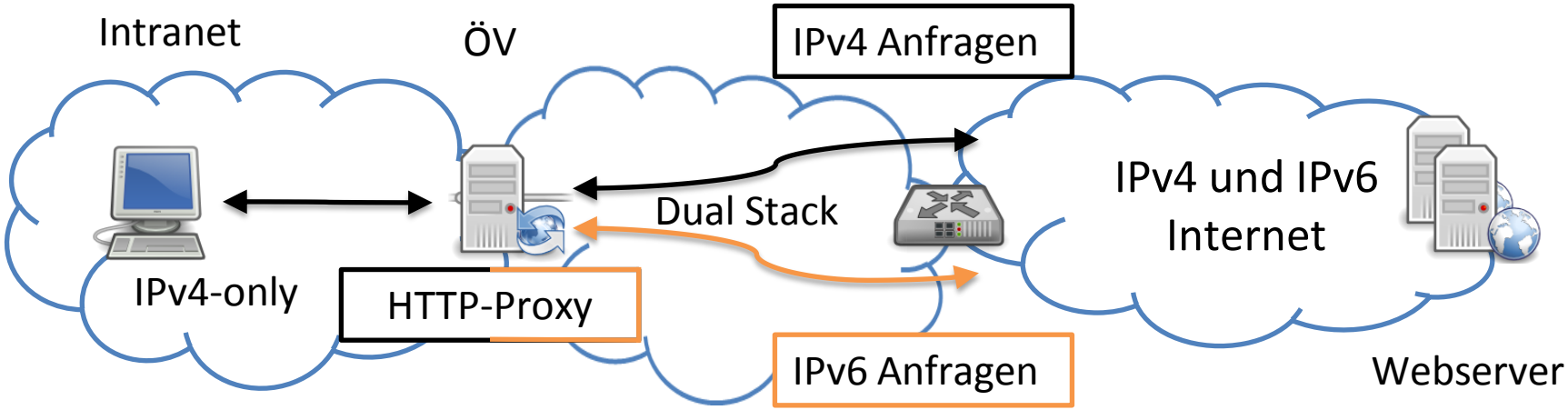
TUNNELBROKER



- Konfiguration statischer Tunnel
- Übertragung von IPv6-Pakten über IPv4-Netze
- extra Tunnelbroker-Server für die Signalisierung unterstützt die Findung des Tunnelendpunktes und den sicheren Verbindungsaufbau

© Fraunhofer FOKUS

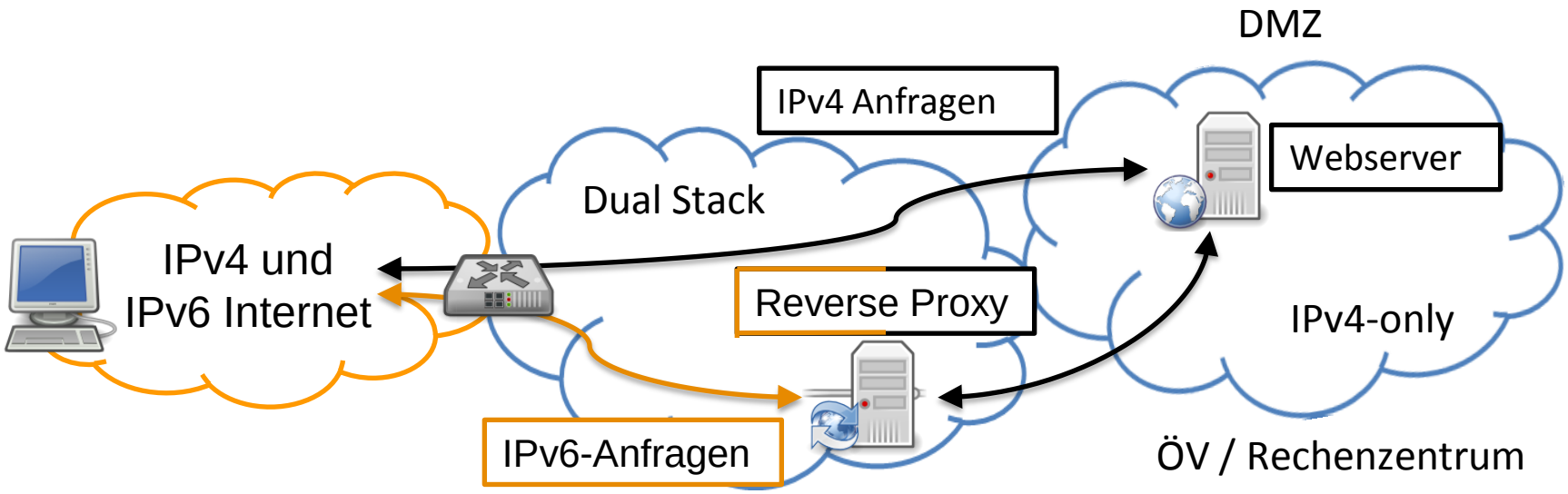
AUSGEHENDER HTTP PROXY



- Mögliche Übergangslösung für Zugriff aus einer IPv4-only-Umgebung ins IPv4- und IPv6-Internet (bzw. aus neuem IPv6-only)
- vorhandener Dienst und dessen Server müssen nicht angepasst werden
- relativ geringer Aufwand; Proxy-Technologie und Lösungen ausgereift
- Brückentechnologie vor Einführung von IPv6 im Intranet

© Fraunhofer FOKUS

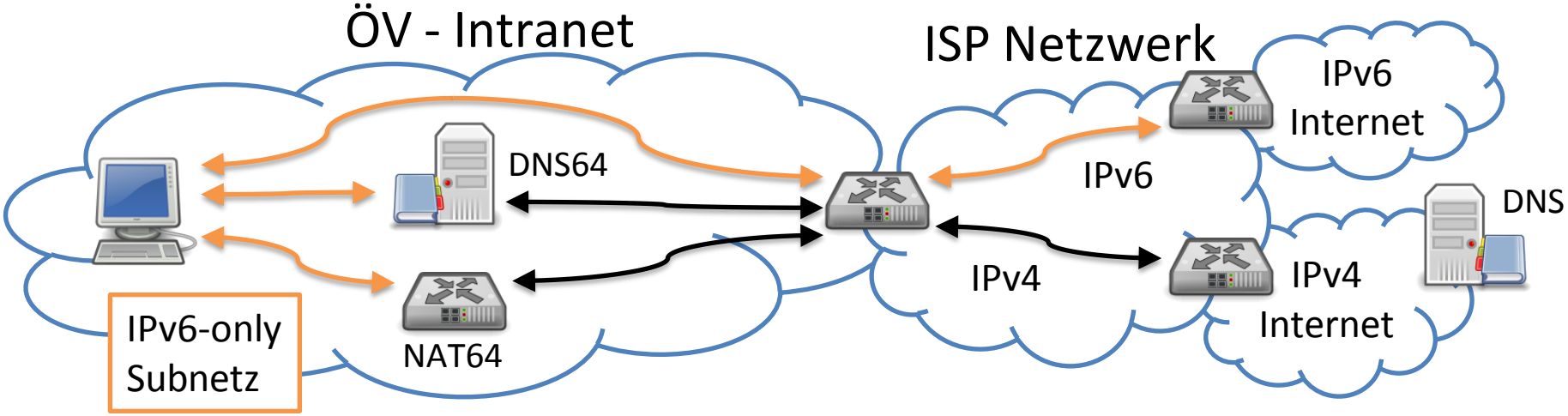
EINGEHENDER HTTP REVERSE PROXY



- zusätzlicher Reverse Proxy, um Inhalte eines IPv4-only Webservers auch im IPv6-Internet abrufbar zu machen
- Konfiguration des bestehenden Webservers kann dabei zumeist komplett unverändert erhalten bleiben.
- Brückentechnologie, bis der Webserver auch Dual-Stack-tauglich ist.

© Fraunhofer FOKUS

NAT64 / DNS64



- Technik, die Endsystemen in (neuen) IPv6-only Umgebungen erlaubt, zusätzlich auch auf IPv4-Systeme im Intranet und Internet zuzugreifen
- funktioniert nur mit Diensten, welche sich über Namen (URI/URL oder Hostname) ansprechen lassen, nicht bei nur numerischer IPv4-Adresse
- benötigt zwingend einen DNS64-Server und NAT64-Gateway im Intranet

© Fraunhofer FOKUS

TECHNIK ALLEIN IST NICHT ALLES

- Technik-Seite
  - ggf. neue Software und Geräte
  - Bedarf an Schulung für „die Netzwerker“/ das NOC

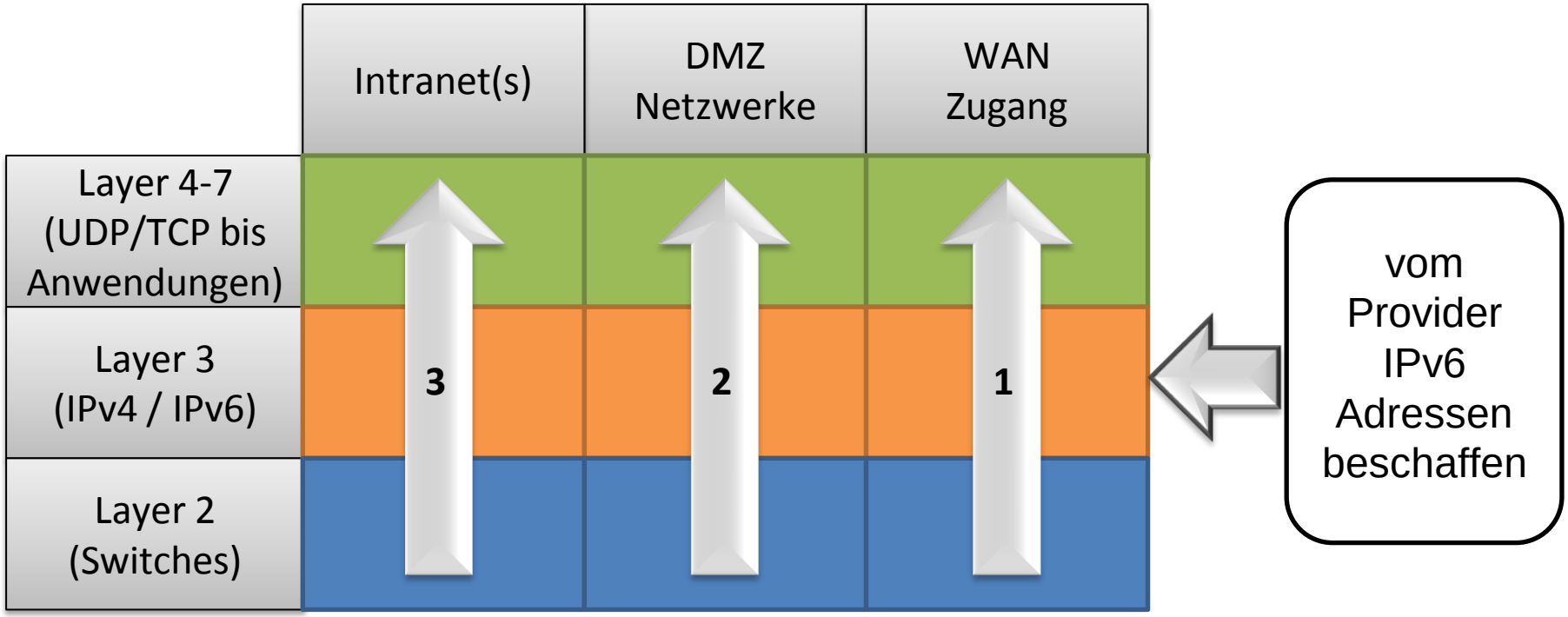
- Kommunikation intern und extern:
  - „wir machen jetzt auch IPv6“

- Einen **PLAN** zur gezielten Einführung
  - IPv6 soll **WO** funktionieren?
  - **WIE** migriere ich dorthin?
  - Mit welchem **BUDGET**? Und bis **WANN**?

Migration
==
Projektarbeit

EINFÜHRUNG „VON UNTEN NACH OBEN“

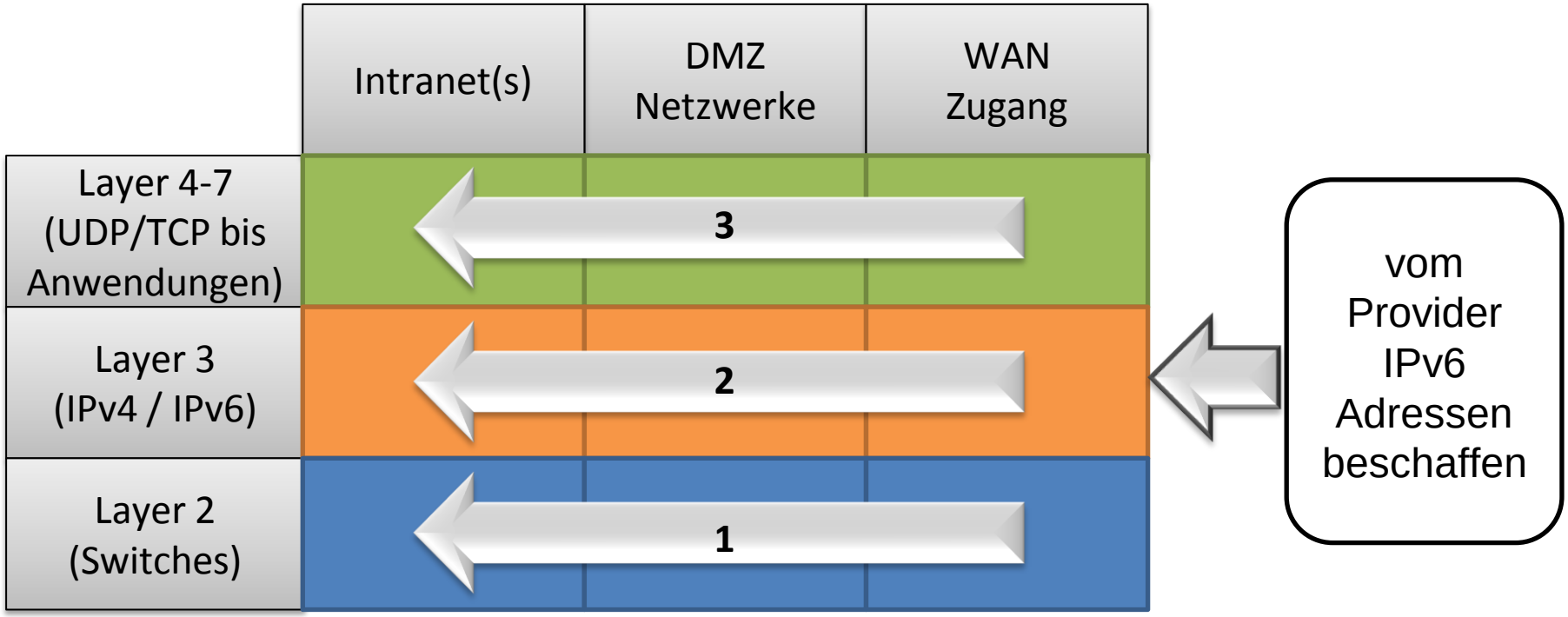
- IPv6-Einführung betrifft verschiedene Layer in Netzwerk-Stack
- IPv6-Einführung kann eines oder mehrere Netze betreffen



© Fraunhofer FOKUS

EINFÜHRUNG „VON AUßEN NACH INNEN“

- Günstiger, wenn sowieso alle Netze umgestellt werden sollen
- Beschaffung von neuen Geräten eher „in einem Rutsch“ möglich



© Fraunhofer FOKUS

NICHT ABWARTEN

- **Jetzt** sich schlau machen!
  - Lesen
  - Sich austauschen
  - IPv6 Testen (am besten im eigenen IPv6 Testbed)

- **Jetzt** vorsorgen
  - automatische Tunnel abschalten / blocken (Sicherheit)
  - Beschaffungen anstoßen (da sehr zeitintensiv)
  - Ziele festlegen („unser Webserver soll IPv6 sprechen“)
  - Adressen besorgen und Adressplan überlegen

IPv6 EINFÜHRUNG – JA, BITTE!

- Bei *Neubeschaffungen* immer darauf achten!
- Bei neuen *Verträgen* immer verlangen! (bei HW / SW / ISP)
- Seien sie **Vorreiter**! (wer ist schon gern Nachzügler?)
- Tauschen Sie sich aus!
  („ach, sie hatten dieses Problem auch?“)
- Migrationsprojekt „zu groß“?
  - Machen Sie kleine Schritte!
  - Die richtige Brückentechnologie ist 100%ig okay.

ZEIT FÜR FRAGEN

Vielen Dank für ihre Aufmerksamkeit!

Fragen?

© Fraunhofer FOKUS

KONTAKT

Fraunhofer FOKUS

Kaiserin-Augusta-Allee 31

10589 Berlin, Germany

www.fokus.fraunhofer.de

Carsten Schmoll

carsten.schmoll@fokus.fraunhofer.de
Tel. +49 (0) 30 3463-7136

© Fraunhofer FOKUS

ENDE

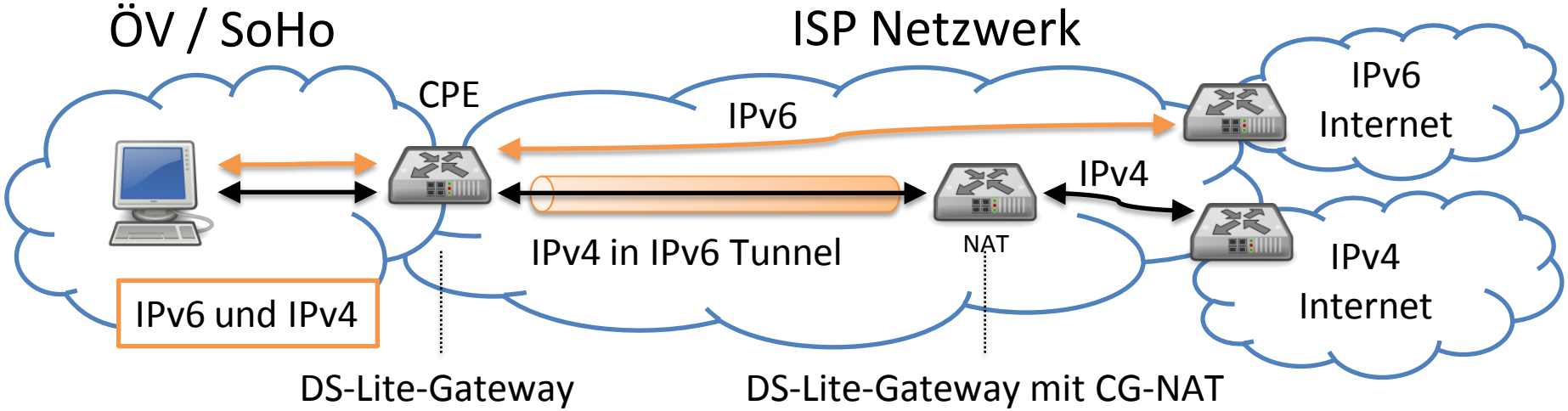
© Fraunhofer FOKUS

STOLPERSTEINE

- Organisatorisch
  - wenig Erfahrung bei der Umsetzung
  - Unwissenheit / fehlendes Verständnis
  - Komplexität bei Dual-Stack

- Technisch
  - unausgereifte Implementierungen
  - teilweise mangelnde Unterstützung
  - automatische Tunnel
  - neue Angriffsmethoden

DS-LITE



- Provider-Technologie: Kunden bekommt IPv6 und eingeschränktes IPv4
- IPv6 wird nativ vom Provider zur Verfügung gestellt, wie bei Dual-Stack
- IPv4 über Carrier Grade NAT bereitgestellt, Einschränkung zu Dual-Stack

© Fraunhofer FOKUS

BEWERTUNGEN

	SoHo	ÖV	ISP
Dual Stack	++	++	++
6in4	(→ Tunnelbroker)	+	
Teredo / 6to4	- (Sicherheit)	-- (Sicherheit)	
ISATAP		-	
DS-Lite / CGN	+ (über ISP)	- (über ISP)	+ (spart IPv4)
6rd	+ (über ISP)	- (über ISP)	+ (ermöglicht IPv6)
ÖV-Tunnelbroker	+	+ (Nutzer/Anbieter)	(ggf. Dienstanbieter)
NAT64 & DNS64	- (Aufwand)	+	
XLAT464	+ (über ISP)	- (über ISP)	+ (für neue ISP)
Proxy / ALG	+	++	- (ggf. Dienstanbieter)
Reverse Proxy		++	(ggf. Dienstanbieter)
L2-VLAN		-	
SIIT		+	+