[de:government]
addressing tomorrow

Bundesministerium
des Innern

de.government -

IPv6 Routingkonzept
für die öffentliche Verwaltung Deutschlands

August 2016

Inhaltsverzeichnis

ABBILDUNGSVERZEICHNIS

Dokumenteninformation

Verfasser	Tahar Schaa (Cassini) im Auftrag des BMI
Version	1.0
Status	30.08.2016
Autoren	Schaa, Bürger, Holz, Krengel, Kocker, Südmeyer
Review	IPv6 AG
Klassifizierung	-

Änderungshistorie

Datum	Version	Änderung	Autoren
12.03.2013	0.1	Initialversion	Tahar Schaa
15.07.2016	0.98	Kapitel 8, OSCI und Routingregelkasten, Korrekturen dritter	Tahar Schaa
30.08.2016	1.0	Finalisierungen	Constanze Bürger, Tahar Schaa

1 MANAGEMENT SUMMARY

Für den Betrieb von IT-Netzwerken und insbesondere des Internets ist das “Internet-Protokoll” (IP) ein zentrales Element, durch das neben dem Transport der Datenpakete auch die Adressierung der am Internet angeschlossenen Komponenten ermöglicht wird. IP-Adressen sind die Grundlage jeder modernen IT-Netzinfrastruktur und gewährleisten die Handlungsfähigkeit im Internet und in Regierungsnetzen

Der ursprüngliche Internet-Adressraum ist zu einer knappen Ressource geworden, die mit dem Wachstum des Internets nicht Schritt halten kann. Konkret bedeutet dies, dass durch das Internetprotokoll Version 4 (IPv4) langfristig nicht mehr ausreichend Internet-Adressen zur Verfügung stehen, um im Internet problemlos zu agieren. Es muss daher auf das neue Internetprotokoll Version 6 (IPv6) umgestellt werden, welches unter anderem einen sehr viel größeren Adressierungsumfang hat.

Das BMI/BVA verwaltet als zentrale Instanz in der Local Internet Registry (LIR) mit dem Namen „de.government“ den IPv6-Adressraum für die gesamte öffentliche Verwaltung Deutschlands. Die organisatorischen Rahmenbedingungen wurden mit dem IPv6-Referenzhandbuch 2011 (2011/04 IT1-190 001-9/0#28) durch den IT-Planungsrat beschlossen.

Neben der Vergabe der Adressen muss auch eine korrekte Wegeführung der Datenkommunikation, das sogenannte „Routing“, sichergestellt werden. Die öffentliche Verwaltung Deutschlands hat dabei besondere Anforderungen, insbesondere vor dem Hintergrund der IT Sicherheit. Eckpunkte wie die Erreichbarkeit, Transparenz, definierte Wegeführung und Nachhaltigkeit, aber auch die Umsetzung von Rechtsgrundlagen, wie z.B. dem IT-NetzG, spielen dabei eine wesentliche Rolle. Das Routing des IPv6-Adressraums der öffentlichen Verwaltung muss dauerhaft, weltweit über das Internet und die Netze der öffentlichen Verwaltungen (u.a. Verbindungsnetz) gewährleistet sein.

Ziel dieses Konzepts ist es, langfristig behördenübergreifend sichere Kommunikation der öffentlichen Verwaltung nachvollziehbar zu gewährleisten.

Das vorliegende Konzept wurde unter der Steuerung des BMI, von Kollegen aus den Ländern, Kommunen, staatlichen Rechenzentren, Polizeivertretern, dem BSI, dem decix, u.a. erarbeitet und von der IPv6 AG durch Unterstützung von Cassini finalisiert.

2 IST SITUATION - HINTERGRUND

Bisher gibt es in der öffentlichen Verwaltung in Deutschland kein behördenübergreifendes Routing. Hauptgrund ist die Verwendung von IPv4. Da die Behörden in ihren IT-Netzwerken identische, sich überschneidende (interne) IPv4 Adressräume nutzen, muss Adressumsetzung (Network Address Translation-NAT) als Technologie eingesetzt werden, um behördenübergreifende Kommunikation - Government to Government (G2G)-Kommunikation - abbilden zu können. Dies kann zwar das grundlegende Sicherheitskonzept der strikten Netztrennung zwischen „innen“ und „außen“ unterstützen, die Verwendung von IPv4 führt jedoch zu folgenden grundlegenden Einschränkungen:

- **Einschränkung von Kommunikation und Diensten** – Es können zwischen den Behörden nur begrenzt viele Dienste miteinander kommunizieren und genutzt werden. Die direkte IP-Telefonie von flächendeckend ausgerollten Voice over IP Telefonen, in zwei Bundesländern, mit Ende-zu-Ende Sicherheit mittels Verschlüsselung ist so beispielsweise nicht möglich.
- **Fehleranfälligkeit und Sicherheitsvorfälle** – Da auf der gesamten Kommunikationsstrecke zwischen einem IT-Dienst in einer Behörde und dem Client heute mehrere Adressumsetzungen stattfinden, ist das Risiko von Fehlkonfigurationen und damit von Sicherheitsvorfällen hoch.
- **Inhomogenes Sicherheitsniveau des Datentransfers** – Jede Behörde regelt ihr Routing bislang eigenständig. Dadurch ist wechsel-

seitig intransparent, wie die Daten außerhalb des jeweiligen Behördennetzwerks weitergeleitet werden.

3 MOTIVATION ZUR NUTZUNG EINES GEMEINSAMEN ROUTINGS

Mit Einführung und Nutzung von IPv6 sind überschneidende IP-Adressräume per Design nicht vorgesehen und aufgrund des wesentlich größeren verfügbaren IP-Adresspools auch nicht mehr erforderlich. In der öffentlichen Verwaltung kann und soll die behördenübergreifende Datenkommunikation mit IPv6 auf einer einheitlichen Basis bedarfsgerecht gesteuert und sichergestellt werden.

Routing, als Funktion in IT-Netzwerken, hat als primäres Ziel, Kommunikation zu ermöglichen und sicherzustellen. Dabei definiert die gesetzliche Aufgabe der jeweiligen Behörde die Anforderungen an die Kommunikation. So sind beispielsweise zu unterscheiden:

- Regierungskommunikation - vertrauliche Kommunikation, Inhalte und die Kommunikationsendpunkte werden vor unbefugtem Zugriff geschützt
- Massenkommunikation - Kommunikation mit dem Ziel, so viele Behörden/Einrichtungen/Menschen wie möglich zu erreichen - z.B. in Naturkatastrophen
- Krisenkommunikation - Kommunikation in besonderen Lagen - schnell auf bestimmte Nutzer beschränkt und prioritär

Um die zuvor genannten Einschränkungen des Routings mit IPv4 in der Behördenkommunikation hinter sich zu lassen, ist es notwendig eine behördenübergreifende IPv6-Routingkonzeption föderal abzustimmen.

Adressaten des hier vorgestellten Konzeptes sind **Bund, Länder, Kommunen** und andere Einrichtungen mit ihren IT-Netzinfrastrukturen, in denen der koordinierte IPv6 Adressraum der deutschen Verwaltung genutzt wird.

4 ROUTINGPRINZIPIEN DER ÖFFENTLICHEN VERWALTUNG

Grundlage für dieses Konzept ist die Definition der Ziele, welche man in der öffentlichen Verwaltung mit dem Mechanismus „IP-Routing“ verfolgt. Diese wurden mit der IPv6 Arbeitsgruppe und dem BSI abgestimmt:

1. **Ermöglichen von Kommunikation** - Die Erreichbarkeit der Teilnehmer mit de.government Adressen ist das oberste Ziel. Die Kommunikation über öffentliche Netze sowie über Verwaltungsnetze muss sichergestellt sein.

2. **Transparenz** - Der IPv6 Adressbereich de.government ist logisch und klar strukturiert. Die LIR de.government stellt Transparenz über die Nutzung der Adressbereiche und die Zuordnung dieser Adressbereiche zu verantwortlichen Stellen her.

3. **Persistente Adresszuordnung** - Jede IP Adresse aus dem Adressblock de.government ist weltweit eindeutig und wird einer Station/einem Gerät dauerhaft zugewiesen. Eine Umadressierung ist zukünftig nicht erforderlich.

4. **Definierte Wegeführung (Routing)** - Es ist klar definiert, über welche Netzwerkinfrastrukturen die Inhaber von IP-Adressen aus de.government kommunizieren. Zu anderen öffentlichen Einrichtungen im Adressbereich de.government werden sie über ein sicheres Verwaltungsnetz geleitet. Soll ein Dienst zudem im Internet verfügbar sein, so ist er gleichzeitig mit der identischen oder einer weiteren IPv6 Adresse für andere Kommunikationspartner aus dem Internet erreichbar.

5. **Nachhaltigkeit und langfristige Tragfähigkeit** - Das Routingkonzept soll nachhaltig sein, auf eine langfristige Gültigkeit und Zukunftssicherheit abzielen.

6. **Sicherheit** – IT-Sicherheit muss in Verbindung mit dem Routing sichergestellt werden.

Erläuterung

Die Diskussion mit zahlreichen Nutzern, Dienstleistern und Experten hat gezeigt, dass die Routingprinzipien bestimmte typische Fragestellungen nach sich ziehen, die hier kurz erläutert werden.

In diesem Konzept werden nur Global Unicast Adressen (GUA) betrachtet, da Unique Local Addresses (ULA) vollständig ungeeignet sind, um ein verwaltungsübergreifendes Adressierungs- und Routingkonzept aufzubauen.

Grundsätzlich ist das Ziel der Routingprinzipien 1 und 3, dass jeder Netzteilnehmer barrierefrei mit jedem anderen kommunizieren kann. Die logischen Verbindungen auf Adressebene (OSI Layer 3) sollten vollvermascht sein können. Die zugrundeliegende physikalische Infrastruktur wird in der Praxis allerdings häufig keine vollvermaschten Netzwerke zulassen. Die konkrete Ausgestaltung von Routingregeln und der Adressierung liegt in der Hoheit der Betreiber von IT-Netzinfrastrukturen.

Das Routingprinzip 4 erfordert ganz besonders ein Konzept zur sicheren Kopplung von Diensten an mehrere verschiedene Netze gleichzeitig. Wesentlich ist, dass Netze mit unterschiedlichen Vertrauensstellungen und Schutzniveaus hier nicht einfach gekoppelt werden. Beispiele für sichere Anbindungskonzepte werden in diesem Dokument gegeben.

5 SZENARIEN

Das Routing in der öffentlichen Verwaltung ist in zwei Szenarien zu betrachten:

1. Routing von Datenverkehr zwischen Behördennetzen – Intra-Government (G2G) Routing

   Ziel ist es, die sichere Datenkommunikation (Kommunikation, Dienste, Transaktionen) zwischen Behördennetzen nach den Erfordernissen des IT-NetzG sicherzustellen.
2. Routing von Datenverkehr zwischen Behörden und Internet – Government-Internet (G2I) Routing

   Ziel ist es die zuverlässige Kommunikation, speziell die Erreichbarkeit, von Behörden auch mit dem Internet dauerhaft, und weltweit sicherzustellen.

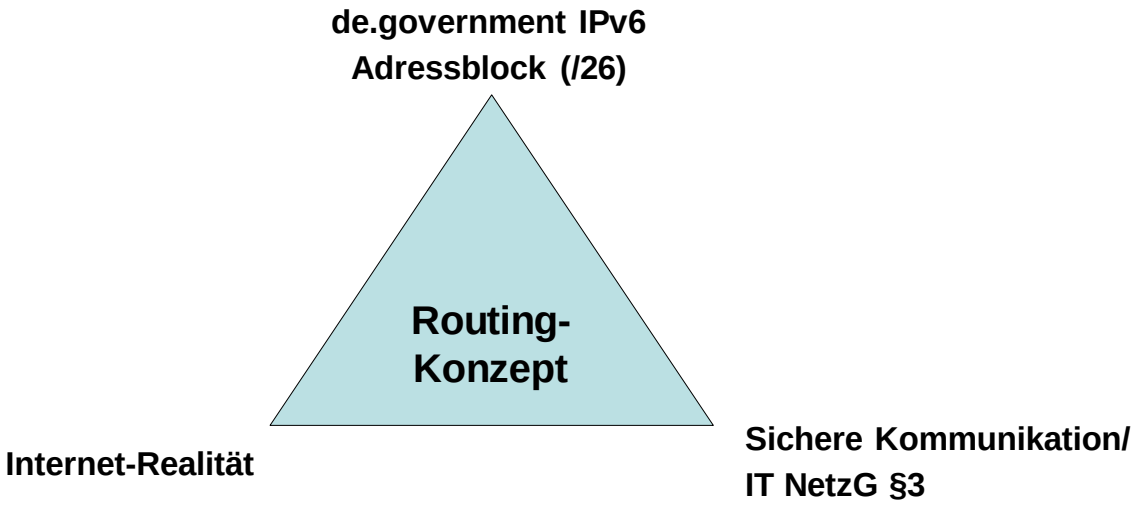


Abbildung 1: Rahmenbedingungen für ein Routingkonzept für die öffentliche Verwaltung

6 G2G ROUTINGKONZEPT

6.1 G2G Routing - Lösungsansatz anhand Verbindungsnetz

Für das Routing von IPv6 Datenverkehr zwischen Behörden wurde das folgende Grundkonzept entwickelt, welches übertragbar auf die meisten Netzinfrastrukturen innerhalb der öffentlichen Verwaltung ist. Typisch für diese Netzinfrastrukturen in der öffentlichen Verwaltung ist die gleichzeitige Kopplung über mehrere Netzwege. Im einfachsten Fall über ein Verwaltungsnetz (z.B. das Verbindungsnetz) und das öffentliche Internet. Dabei sind bestimmte, technisch mögliche Wegeführungen für den Datenverkehr aus Gründen der Informationssicherheit unerwünscht und z.T. durch das IT-NetzG verboten.

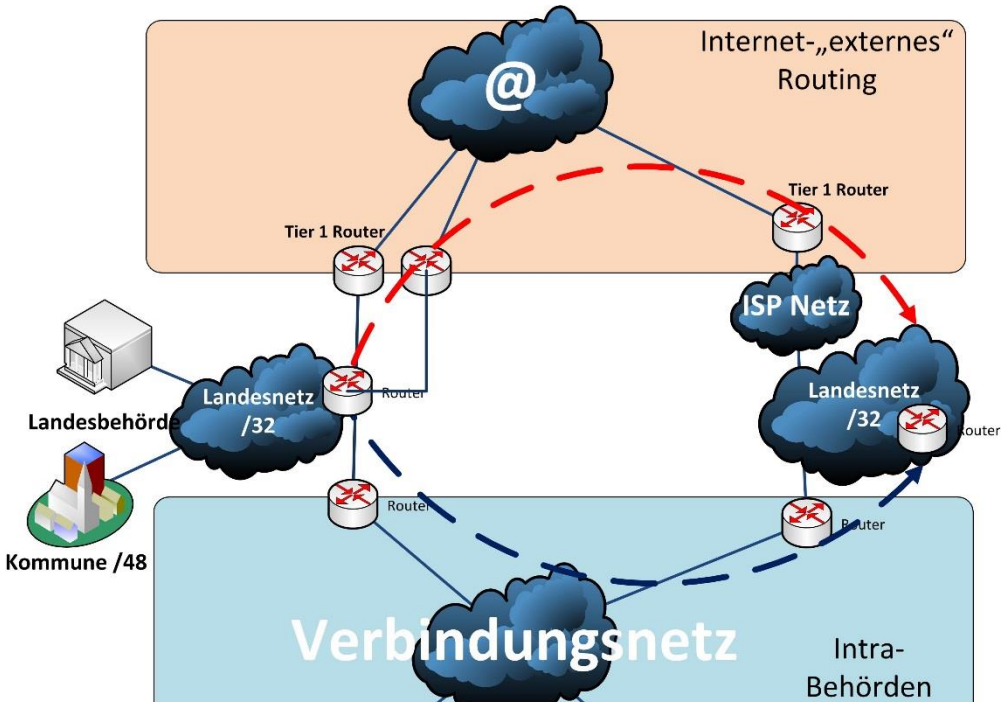


Abbildung 2: Grundstruktur der doppelten Kopplung

Betrachtet man die Netzstruktur zwischen dem Bund und einem Bundesland genauer kommt man zur folgenden schematischen Darstellung.

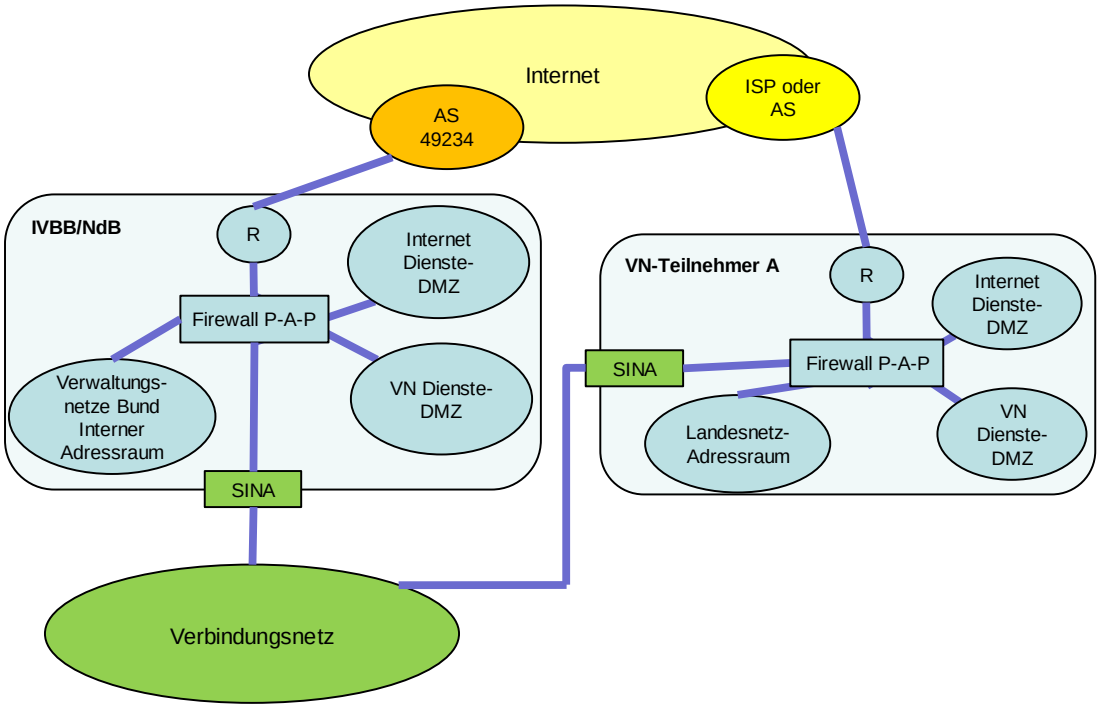


Abbildung 3: Netzstrukturschema IVBB / Land

Ergänzt man ein weiteres Bundesland, erhält man das Gesamtschema für Bund und Länder welche über das Verbindungsnetz gekoppelt sind.

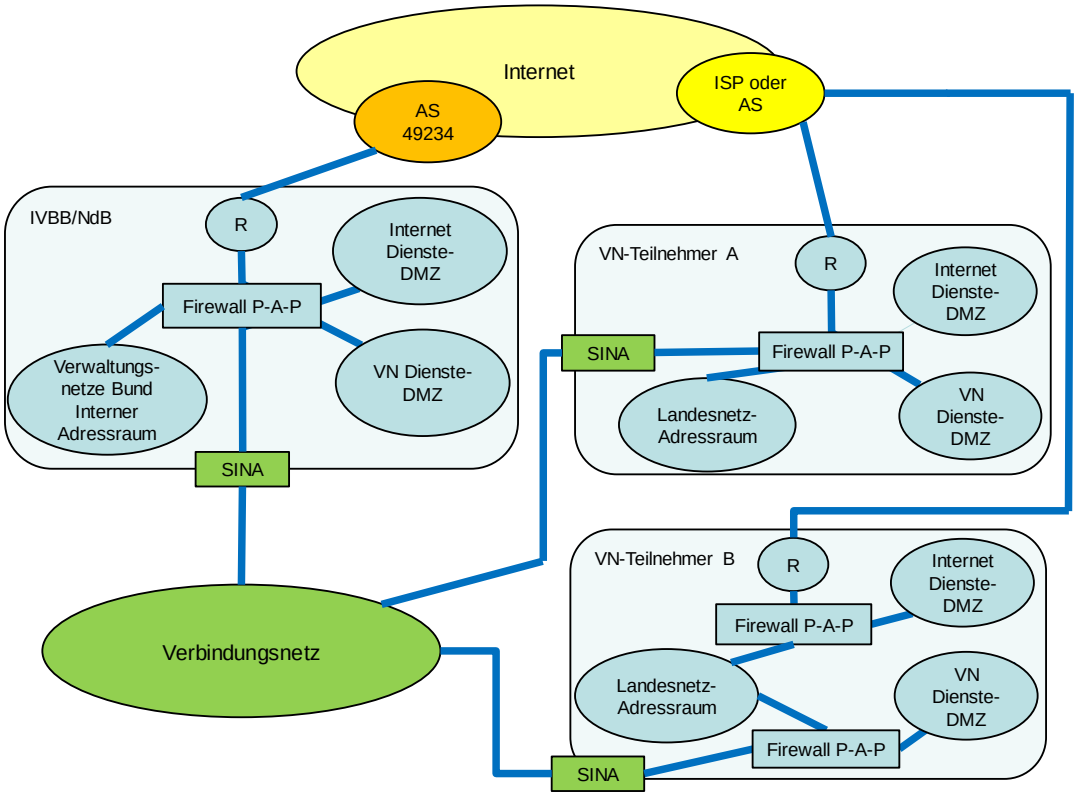


Abbildung 4: Netzstrukturschema Verbindungsnetz

Am Netzübergang der Verbindungsnetz-Teilnehmer wird mittels Routing im Router des Teilnehmers entschieden, ob ein IPv6-Datenpaket über das Verbindungsnetz oder ein anderes Netz geleitet werden muss. Diese Entscheidung sollte nach einem möglichst einfachen Regelwerk basierend auf den jeweiligen IPv6-Zieladressen getroffen werden können.

6.1.1 Adressblöcke de.gov & de.pub.gov

Um alle Anforderungen von Verbindungsnetzteilnehmern abzudecken werden zwei unterschiedliche IPv6 Adressblöcke eingesetzt:

de.gov

- **de.gov**
  - de.government IPv6 Adressblock - aktuell 2a02:1000/26
  - geschlossener Adressblock der öffentlichen Verwaltung in Deutschland
- **de.pub.gov**
  - eigener öffentlicher IPv6 Adressblock,
  - getrennt von de.gov

de.pub.gov

- Größe; mindestens ::/32
- mögliche separate Adressierung von Internet-Diensten

Beide Adressblöcke werden von der LIR de.government verwaltet.

Der de.gov Adressblock 2a02:1000/26 wird zudem unterteilt in einen Bereich, der im Verbindungsnetz erreichbar ist und einen anderen Bereich, der nicht über das Verbindungsnetz ansprechbar ist. Letzterer ist für Behörden gedacht, die nicht mit dem Verbindungsnetz gekoppelt sind.

Im Falle einer Erweiterung des de.gov IPv6 Adressraums wird die Regel angepasst, ohne aber die Komplexität zu erhöhen.

Präfix: 2a02:1000 /26 **Regional Bits:** **6**

Block	Nr.	Dual	Präfix	Block	Nr.	Dual	Präfix
00: Hamburg	0	000000	2a02:1000 /32	08: Niedersachsen	8	001000	2a02:1008 /32
01: Reserve	1	000001	2a02:1001 /32	09: Reserve	9	001001	2a02:1009 /32
02: Schleswig Holstein	2	000010	2a02:1002 /32	10: Reserve	10	001010	2a02:100a /32
03: Reserve	3	000011	2a02:1003 /32	11: Reserve	11	001011	2a02:100b /32
04: Bremen	4	000100	2a02:1004 /32	12: NRW Land	12	001100	2a02:100c /32
05: Reserve	5	000101	2a02:1005 /32	13: Reserve	13	001101	2a02:100d /32
06: Mecklenburg-Vorpommern	6	000110	2a02:1006 /32	14: NRW Kommunen	14	001110	2a02:100e /32
07: Reserve	7	000111	2a02:1007 /32	15: Reserve	15	001111	2a02:100f /32
Block	**Nr.**	**Dual**	**Präfix**	**Block**	**Nr.**	**Dual**	**Präfix**
16:Hessen	16	010000	2a02:1010 /32	24: Saarland	24	011000	2a02:1018 /32
17: Reserve	17	010001	2a02:1011 /32	25: Reserve	25	011001	2a02:1019 /32
18: Reserve	18	010010	2a02:1012 /32	26: DOI+Offentliche	26	011010	2a02:101a /32
19: Reserve	19	010011	2a02:1013 /32	27: Reserve	27	011011	2a02:101b /32
20: Rheinland-Pfalz	20	010100	2a02:1014 /32	28: Sachsen	28	011100	2a02:101c /32
21: Reserve	21	010101	2a02:1015 /32	29: Reserve	29	011101	2a02:101d /32
22: Reserve	22	010110	2a02:1016 /32	30: Reserve	30	011110	2a02:101e /32
23: Reserve	23	010111	2a02:1017 /32	31: Reserve	31	011111	2a02:101f /32
Block	**Nr.**	**Dual**	**Präfix**	**Block**	**Nr.**	**Dual**	**Präfix**
32: Brandenburg	32	100000	2a02:1020 /32	40: Baden Württemberg	40	101000	2a02:1028 /32
33: Reserve	33	100001	2a02:1021 /32	41: Reserve	41	101001	2a02:1029 /32
34: Berlin	34	100010	2a02:1022 /32	42: Reserve	42	101010	2a02:102a /32
35: Reserve	35	100011	2a02:1023 /32	43: Reserve	43	101011	2a02:102b /32
36: Sachsen-Anhalt	36	100100	2a02:1024 /32	44: Bayern	44	101100	2a02:102c /32
37: Reserve	37	100101	2a02:1025 /32	45: Reserve	45	101101	2a02:102d /32
38: Thüringen	38	100110	2a02:1026 /32	46: Reserve	46	101110	2a02:102e /32
39: Reserve	39	100111	2a02:1027 /32	47: Reserve	47	101111	2a02:102f /32
Block	**Nr.**	**Dual**	**Präfix**	**Block**	**Nr.**	**Dual**	**Präfix**
48: Netze des Bundes	48	110000	2a02:1030 /32	56: BMVg res.	56	111000	2a02:1038 /32
49: Netze des Bundes	49	110001	2a02:1031 /32	57: BMVg res.	57	111001	2a02:1039 /32
50: Netze des Bundes	50	110010	2a02:1032 /32	58: BMVg res.	58	111010	2a02:103a /32
51: Netze des Bundes	51	110011	2a02:1033 /32	59: BMVg res.	59	111011	2a02:103b /32
52: Reserve	52	110100	2a02:1034 /32	60: BMVg	60	111100	2a02:103c /32
53: Reserve	53	110101	2a02:1035 /32	61: BMVg	61	111101	2a02:103d /32
54: Vorreserviert	54	110110	2a02:1036 /32	62: BMVg	62	111110	2a02:103e /32
55: Reserve	55	110111	2a02:1037 /32	63: BMVg	63	111111	2a02:103f /32

Abbildung 5: Adressraum de.government (de.gov)

6.1.2 Einsatz und Erreichbarkeit von de.gov & de.pub.gov

Über das Verbindungsnetz werden zur Kommunikation zwischen Behörden grundsätzlich de.gov Adressen verwendet. Um eigene Dienste als Behörde anderen Behörden über das Internet zugänglich zu machen, können alternativ de.pub.gov Adressen eingesetzt werden.

In der Abbildung 6. wird die Erreichbarkeit von Diensten für Bundesländer aus bestimmten Netzbereichen heraus für die beiden Adressblöcke dargestellt. Zum Verbindungsnetz wird nur mittels de.gov Adressen kommuniziert, zum Internet sind beide Varianten (de.gov und de.pub.gov) möglich. Zusam-

menfassend gilt für zulässige und nicht zulässige Kommunikation bzgl. dieses IPv6 Routingkonzepts folgendes:

- Behördenkommunikation von einer de.gov Adressquelle zu einem de.gov Adressziel geht immer über das Verbindungsnetz bzw. daran angeschaltete Netze (hin und zurück)
- Der Zugriff von einer **de.gov** Adresse auf einen Server mit einer **„nicht“ de.gov** Adresse oder **de.pub.gov**. Adresse im Internet ist zulässig. Der Rückweg muss auf dem gleichen Weg erfolgen.
- Der Zugriff von einer **„nicht“ de.gov** Adresse aus dem Internet auf einen Server mit **de.gov** Adresse ist zulässig

Wenn auf einem Server öffentlich zugängliche Inhalte vorgehalten werden, die sowohl von **„nicht“ de.gov** Adressen aus dem Internet als auch von **de.gov** Adressen erreichbar sein soll, UND aus Netzarchitekturerwägungen der Zugriff nicht über das Verbindungsnetz bzw. dessen angeschlossenen Netze (sondern stets über das Internet) erfolgen soll, darf dieser Server **keine de.gov** Adresse tragen.

Hierfür werden Adressen aus dem Bereich **de.pub.gov** angeboten und bereitgestellt.

Dienste die im Internet unter **de.gov** Adressen angeboten werden sind für andere Behörden im Internet nicht erreichbar. Sie sind nur für Netzteilnehmer nutzbar die selbst **keine de.gov** Adressen zum Zugriff nutzen.

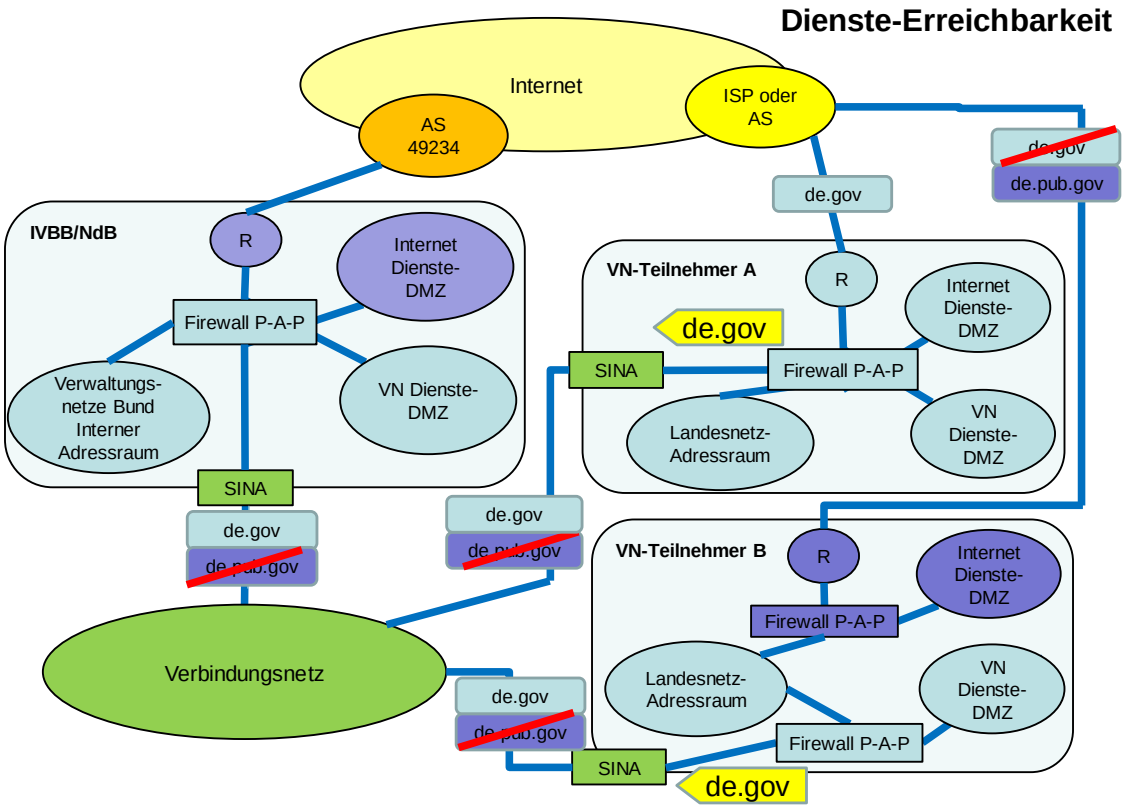


Abbildung 6: De.gov & de.pub.gov Diensteerreichbarkeit

Netzbereiche, die immer über das Verbindungsnetz geroutet werden, sind nach dem aktuellen Adressschema in Abbildung 5 durch **genau zwei Routingregeln beschreibbar**, anhand derer die Router aller Verbindungsnetz-Teilnehmer entscheiden können, ob der Datenverkehr über das Verbindungsnetz geleitet werden soll oder nicht.

Damit dies an dieser Stelle entschieden werden kann, ohne dass die Routingtabellen für die hier durchschnittlich eingesetzten Router zu groß werden, müssen alle Internetdienste unter de.gov Adressen der Verbindungsnetz-Teilnehmer, die auch für Behörden erreichbar sein müssen, unter de.gov Adressen auch im Verbindungsnetz verfügbar sein. Für Ausnahmefälle, bei denen Dienste sowohl für Bürger als auch für Behörden nur über das Internet verfügbar sein sollen, ist der separate offizielle IPv6-Adressblock de.pub.gov

vorgesehen.

Hinweis: Es gibt Fälle, in denen Behörden ihre Dienste anderen Behörden nur im Internet zur Verfügung stellen und so die G2G Kommunikation über das Internet abgewickelt wird. Dies hat meist Kostengründe. Eine weitere Voraussetzung für das Anbieten von Behördendiensten für andere Behörden über das Verbindungsnetz ist die Verfügbarkeit der entsprechenden Bandbreite für Übertragung der gesamten G2G Kommunikation in den sicheren Netzinfrastrukturen der öffentlichen Verwaltung.

Mit dem beschriebenen Routingansatz wird der gesamte IPv6-Datenverkehr, z.B. zwischen zwei Verbindungsnetz-Teilnehmern über das Verbindungsnetz geleitet. Damit wird in der Folge die Forderung vollständig erfüllt, dass immer der sichere Verbindungsnetz-Weg oder ein alternativer sicherer Kommunikationsweg für eine Datenkommunikation zwischen Behörden verwendet wird. Dieser Ansatz kann prinzipiell auf weitere Behördennetze angewandt werden, da er auch mit mehreren gekoppelten Netzen, die nach diesem Konzept ihr Routing betreiben, funktioniert und skaliert. Jedes zusätzliche Netz führt zu mindestens einer weiteren Routingregel in den Routern der verbundenen Netze. Der Ansatz skaliert folglich linear und ist daher auch auf größere Netzebenen wie z.B. TESTA-NG übertragbar.

Der Lösungsansatz geht zunächst von einem statischen Routing mit einer zentral gepflegten Routingtabelle aus. Da alle Verbindungsnetzteilnehmer mit ihren IPv6-Adressbereichen konsequent nur über das Verbindungsnetz routen, hält sich die Komplexität stark in Grenzen.

6.2 Sichere Anbindung von Diensten

Sollen identische Dienste unter de.gov Adressen sowohl für Bürger im Internet, als auch für andere Behörden über Behördennetze nutzbar sein, so

muss bei der Anbindung besonderes Augenmerk auf die Sicherheit gelegt werden, um quasi einen netztechnischen „Kurzschluss“ zwischen Internet und Behördennetz in jedem Fall zu verhindern. Im Folgenden einige Architekturvorschläge zur sicheren Anbindung:

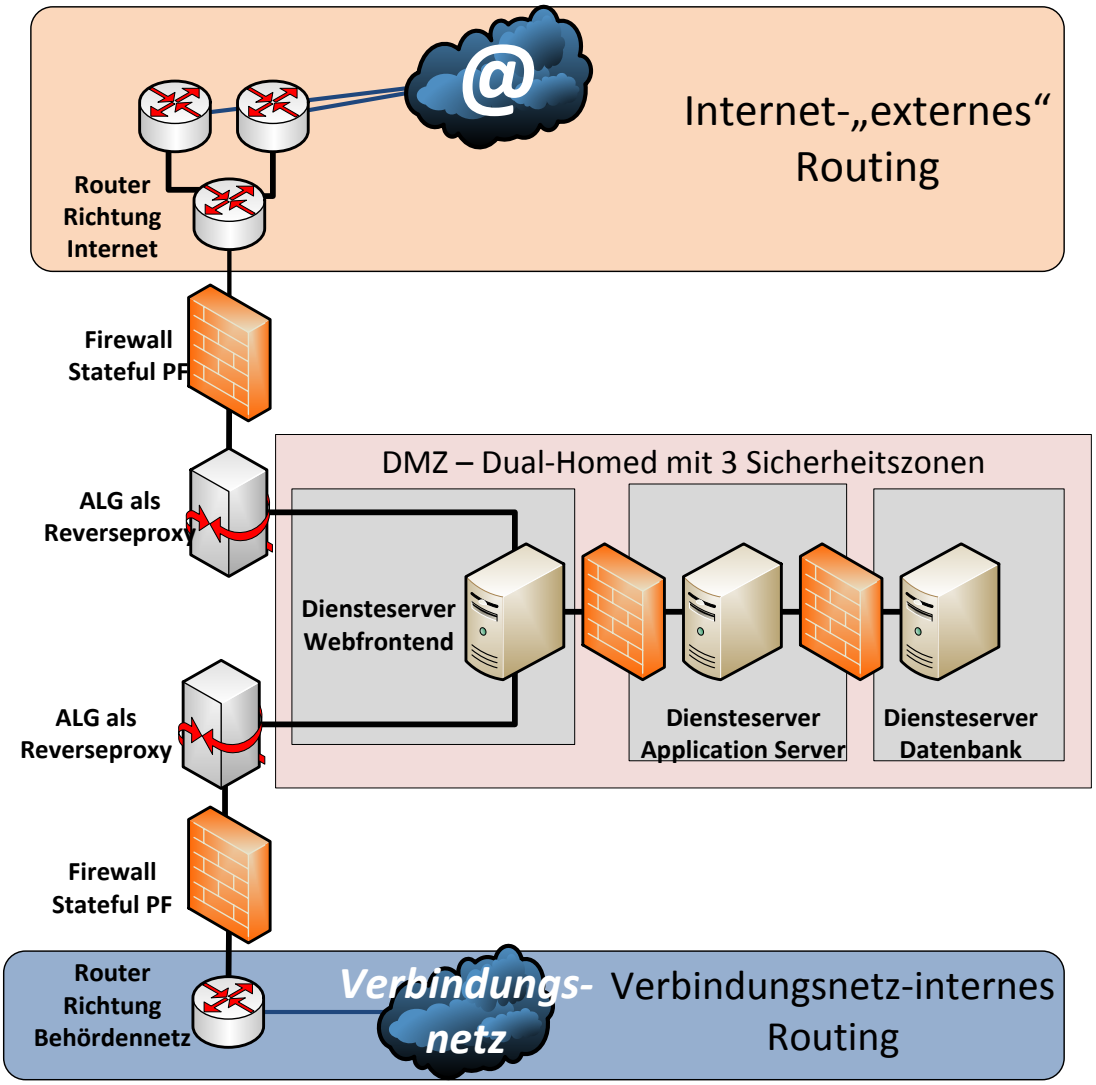


Abbildung 7: 3-Tier Architektur mit Dual-Homed Webfrontend

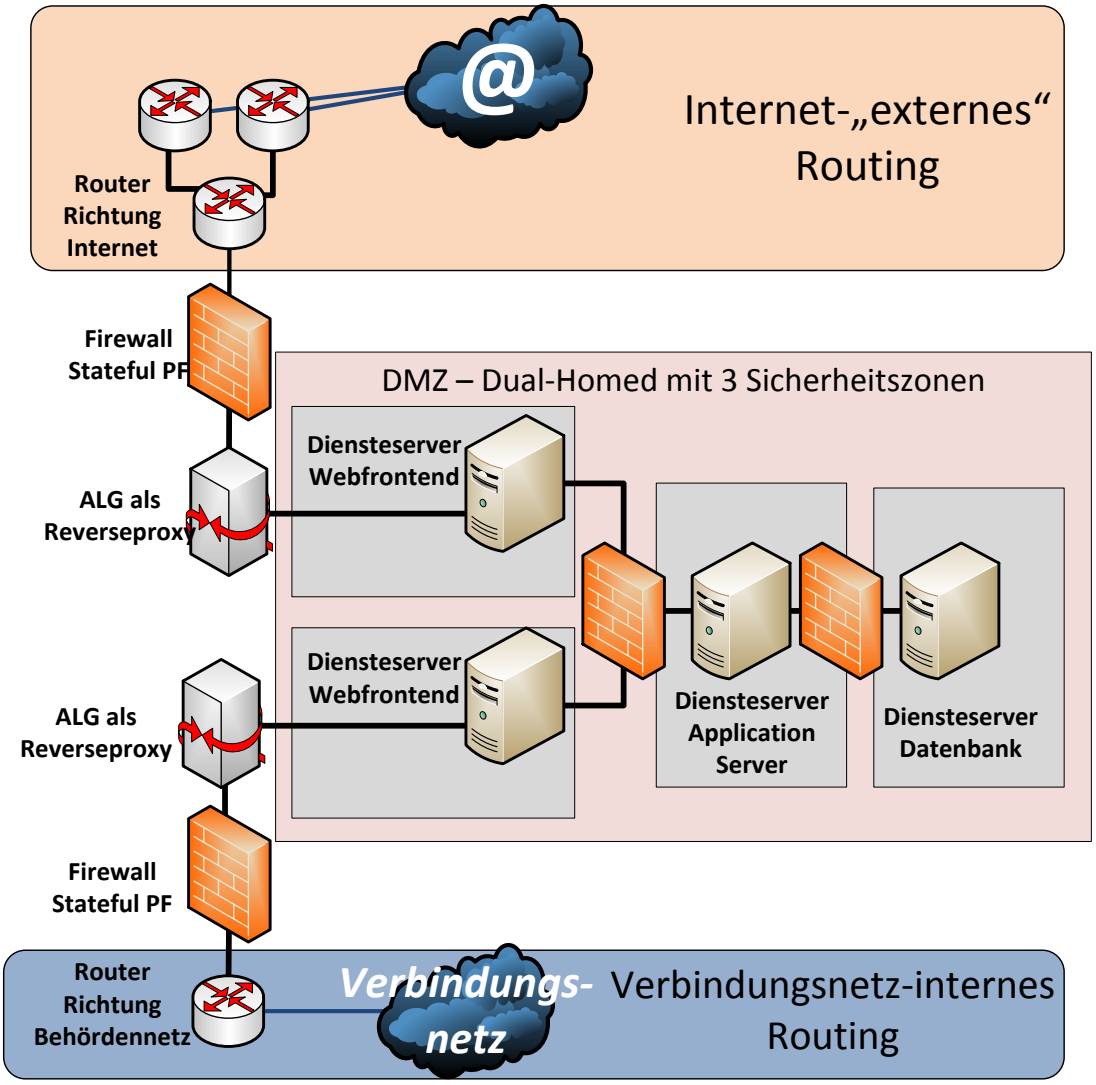


Abbildung 8: 3-Tier Architektur mit doppeltem Dual-Homed Webfrontend

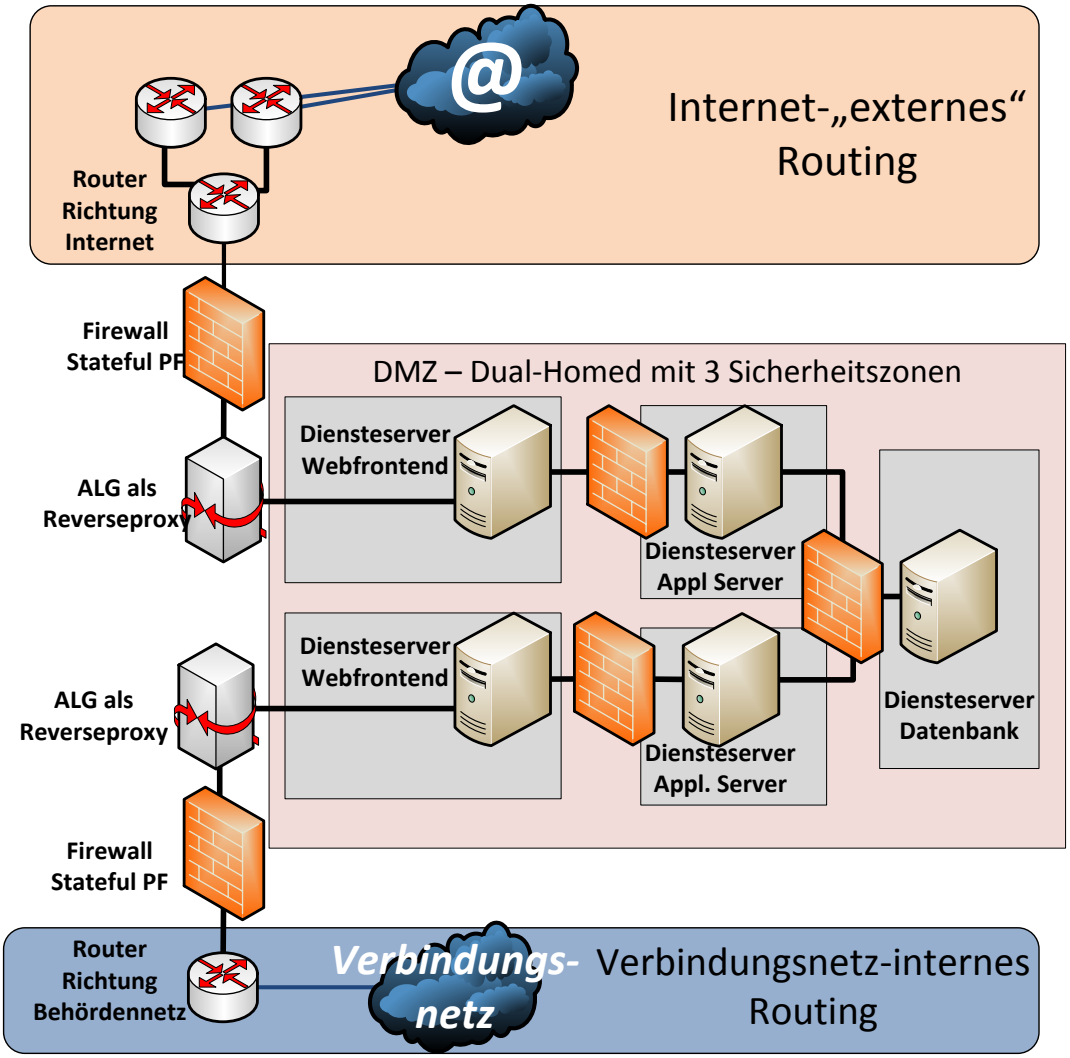


Abbildung 9: 3-Tier Architektur mit doppeltem Dual-Homed Webfrontend und doppeltem Application Server

6.3 G2G Routing - Lösungsansatz übertragen auf weiterere Behördennetze

Der Ansatz ist prinzipiell übertragbar auf weitere Netze wie Testa ng oder CNP-ON. Zu beachten ist, dass die Migration zu IPv6 erfordert, sich übergreifend abzustimmen, unter welchen Adressbereichen Dienste für andere Behörden angeboten werden können und wie das jeweilige Routingkonzept an den Netzkoppelstellen funktioniert. In Deutschland ist dies durch das Adressmanagement der LIR de.government für Behördennetze sichergestellt.

7 G2I ROUTINGKONZEPT

Die öffentliche Verwaltung in Deutschland nutzt einen großen zusammenhängenden **de.gov** (2a02:1000/26) sowie einen kleineren **de.pub.gov** IPv6 Adressraum für bestimmte Dienste. Die Nutzung findet auf die föderalen Strukturen verteilt in eigenständigen Netzinfrastrukturen statt.

Die öffentliche Verwaltung in Deutschland nutzt den Adressbereich 2a02:1000/26 als einheitlichen Adressbereich **de.gov** für die Kommunikation mittels IPv6. Diese Struktur und Nutzung führt zusammen mit den Rahmenbedingungen im Internet dazu, dass das weltweite Routing und damit die Erreichbarkeit nicht mit den üblichen Automatismen sichergestellt werden kann.

7.1 Erreichbarkeit im Internet weltweit

Ein weltweit eindeutig von einer RIR (Regional Internet Registry) zugewiesener IP-Adressraum muss, um diesen auch weltweit erreichen zu können, von den im Internet beteiligten Routern (Vermittlungsknoten des Internets) untereinander bekannt gemacht und jeweils abgespeichert werden.

Die Bekanntmachung geht i.d.R. von dem Router des Inhabers des Adressraums aus und erfolgt mittels des im Internet genutzten Routingprotokolls Border Gateway Protocol (BGP). Eine Route, also ein Weg zu einem bestimmten Adressraum, wird über eine BGP-Annoncierung an die benachbarten Router bekanntgegeben. Diese müssen diese Route dann in ihren Routingtabellen abspeichern, damit in der Folge Datenpakete über diesen Weg geleitet werden können.

Dabei werden alle einzelnen Adressbereiche einer Organisation einer sogenannten Autonomous System Number (ASN) zugeordnet und mehrere Router der Organisation annoncieren, dass sie den Datenverkehr für diese ASN entgegennehmen.

Dieses System führt dazu, dass die Routingtabellen im Internet umso größer werden, je mehr einzelne Adressbereiche annonciert werden. Steigt die Anzahl der in den Routern einzutragenden Routen über einen bestimmten

Wert, so wird mehr Speicher für die Routing Tabelle benötigt. Die Betreiber müssen dann weitere Investitionen tätigen, weshalb diese natürlich daran interessiert sind, möglichst wenige Routingregeln verarbeiten zu müssen.

Abbildung 10: Typisches Router-System, welches mit der vollständigen Routingtabelle des Internets arbeitet.

Ein üblicher Weg zur Reduzierung der Anzahl der Routingeinträge ist es, diese für kleinere Netz nicht mehr zu speichern. Hierzu wird dann ein fester Filter eingerichtet, durch den eintreffende zusätzliche Routingregeln für kleine Netze nicht in die Routingtabelle aufgenommen werden. Die Betreiber, insbesondere der für die weltweite Kommunikation wichtigen Router, welche die vollständige Routingtabelle im Internet halten, sind dabei jeweils völlig unabhängig. Es ist deshalb sehr wahrscheinlich, dass mit steigender weltweiter Nutzung von IPv6 die Routen zu kleineren Adressbereichen von den Betreibern der Router gelöscht werden. In der Folge wären diese Adressbereiche nicht mehr überall im Internet erreichbar. Die Annoncierung kleiner Adressbereiche, wie sie innerhalb von de.government aufgrund der Struktur relativ zwangsläufig vorgenommen werden muss, läuft dem zuwider. Oder anders ausgedrückt, die heute gängigen Routingkonzepte und Best Practices sind für die Anforderungen von Internetserviceprovidern (ISP) und Carriern entwickelt, die den ihnen zugeteilten Adressraum innerhalb ihrer Infrastrukturen weitgehend aggregieren können.

Da der de.gov Adressraum nicht auf einer einheitlichen Netzinfrastruktur ei-

nes Betreibers genutzt wird, ergeben sich (ohne weitere Koordination) die folgenden Rahmenbedingungen:

- Der IPv6 Adressbereich (/26) von de.government wird nicht zentral als Route im Internet annonciert
- Teiladressbereiche werden über unterschiedliche ISPs an das Internet gekoppelt
- Teiladressbereiche werden unter verschiedenen ASNs annonciert

Die Nutzung eines einheitlichen IPv6 Adressraums über eine verteilte Netzinfrastruktur unterschiedlicher ISPs ist typisch für Verwaltungen von föderalen und demokratischen Staaten, aber auch für multinationale Konzerne!

Für den Adressraum de.gov können Annoncierungen von ::/48 und sogar ::/56 nicht ausgeschlossen werden, siehe folgende Abbildung.

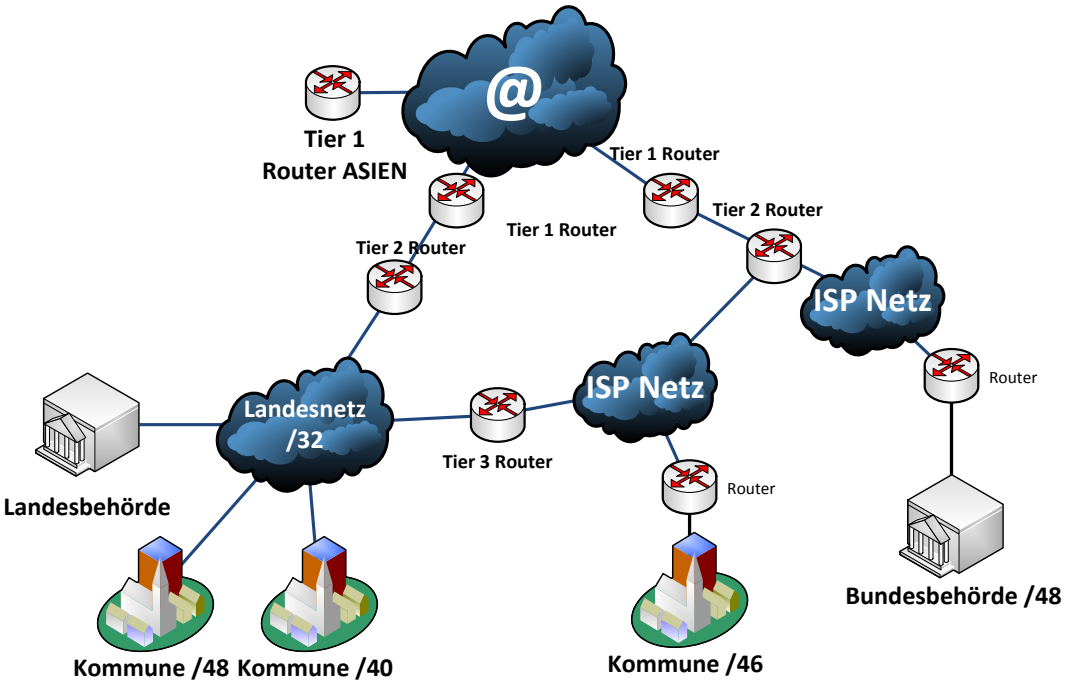


Abbildung 11: Reale Internetanbindung in der öffentlichen Verwaltung

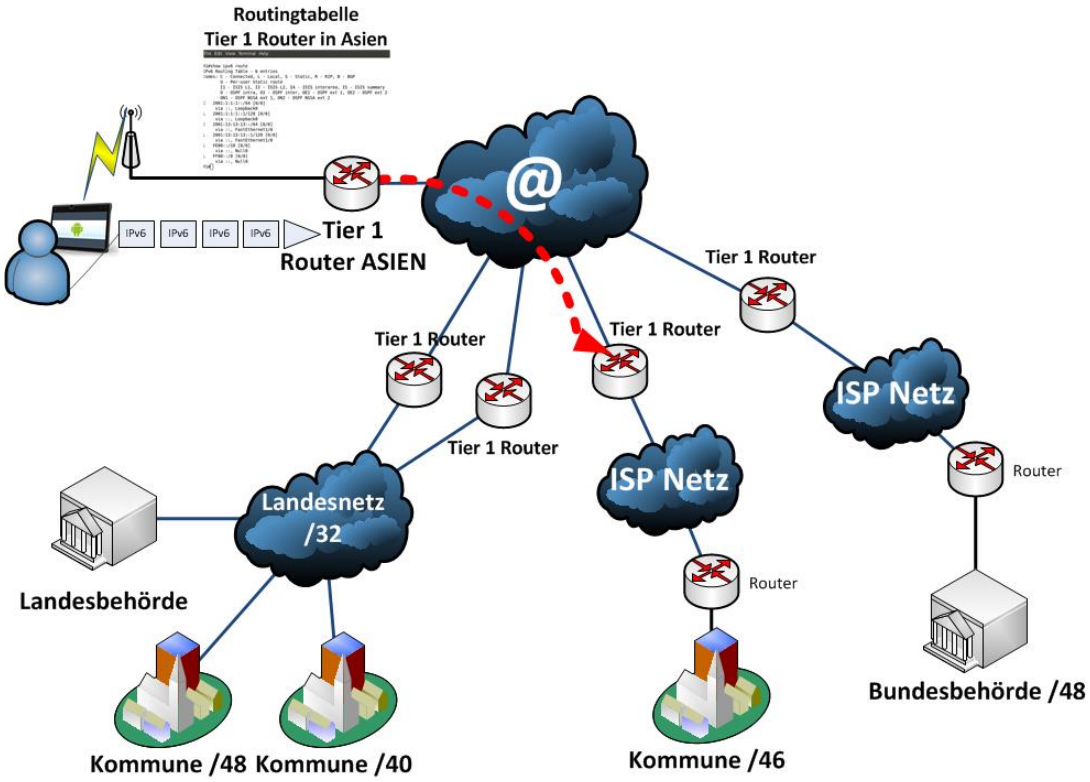


Abbildung 12: Weltweites Routing von de.government Adressbereichen

7.1.1 Risikobetrachtung

Genau lässt sich nicht vorhersagen, wann und wo diese Probleme zum Tragen kommen, da es im Internet keine global verbindliche Routingpolicy gibt. Die einzelnen (Teilnetz)Betreiber sind in den Fragen der Filterung des Routings völlig autonom. Hierzu gibt es auch keine Normungsebene, die diesen Bereich bearbeitet. Zwischen den Providern gibt es allerdings verbreitete Best Practices. Diese unterliegen jedoch ihrerseits einem kontinuierlichen Wandel.

Ein allgemeines „Common Understanding“ der Routerbetreiber im Internet war es, dass ::/32 und größere Adressbereiche langfristig in den Routingtabellen erhalten bleiben werden.

Es gibt Betreiber, die es am liebsten sähen, wenn der Adressbereich einer LIR immer und ausschließlich komplett und „in einem Stück“ als Route im

Internet durch einen oder mehrere Router bekanntgegeben (BGP-annonciert) wird. Zum Teil werden einige Router nach dieser Philosophie konfiguriert, so dass kleinere Bereiche als BGP-Annoncierung von diesen Routern nicht akzeptiert werden.

Da sich diese strikte Haltung „Grundsatz des Strict BGP Filtering für IPv6“ (www.space.net/~gert/RIPE/ipv6-filters.html), um die Routingtabellen im Internet klein zu halten, in der Realität nicht durchhalten lässt, gibt es Vorschläge für Aufweichungsregeln. Ein Vorschlag begrenzt die Anzahl der zusammenhängenden Adressblöcke je ASN auf 20. Ein anderer diskutiert die Änderung des „strict filtering“ in der Weise, das bezogen auf eine LIR allocation bis zu einer bestimmten Anzahl von Bits der Adressraum in kleineren Teilen annonciert werden darf. Dabei würden, z.B. 8 Bit für den Adressraum de.gov bedeuten, dass ::/26 + 8 Bit = ::/34 Adressblöcke noch von den anderen Routern im Internet akzeptiert würden.

Zusammengefasst erfüllt die öffentliche Verwaltung aufgrund ihrer Struktur keine dieser Regelvorschläge zur Begrenzung der Größe der Routingtabellen im Internet.

Unter diesen Umständen ist das weltweite Routing der annoncierten Teilnetze von de.government (de.gov und de.pub.gov) ohne weiteres nicht sichergestellt.

Aufgrund des von vielen Betreibern angewandte Grundsatz des Strict BGP Filtering für IPv6 (www.space.net/~gert/RIPE/ipv6-filters.html) wurden in Einzelfällen bereits relativ gering deaggregierte IPv6 Adressbereiche schon auf der Anbindung zum Internet blockiert.

Da de.government einen /26 Adressbereich zur Nutzung erhalten hat, was für jeden im Internet ersichtlich ist, ist es sogar denkbar, dass Betreiber zukünftig gerade Routingeinträge für diesen Adressbereich von Beginn an nur in Form einer BGP-Annonce mit der Größe /26 akzeptieren könnten.

Konkrete Fälle, bei denen dies eingetreten ist, sind bereits öffentlich dokumentiert. Eine große deutsche Verlagsgruppe hat ein verteiltes Rechenzentrum zur Bereitstellung digitaler Inhalte an drei Standorten installiert. Hierfür haben sie einen /32 IPv6 Adressraum von der RIPE NCC als LIR erhalten. Der Adressraum wurde in 4 /34 Teile aufgeteilt und auf die 3 Rechenzentren verteilt. Mehrere Tage lang waren die Rechenzentren offline, da die Annoncierung nicht akzeptiert wurde (https://ripe69.ripe.net/presentations/137-RIPE69_Langner_Rey_Schaetzle_Slash48_Considered_Harmful.pdf).

7.1.2 Ausnahme von der Unsicherheit – IPv6 PI

Es gibt, im Gegensatz zu den oben beschriebenen Unwägbarkeiten, einen besonderen IPv6 Adressbereich der RIPE, für den die weltweite Erreichbarkeit auch für relativ kleine annoncierte Prefixe weltweit sichergestellt ist. Für besondere technische Sachverhalte können Organisationen IPv6 Adressen erhalten, ohne selbst RIPE Mitglied mit einer eigenen LIR zu werden. Solche Adressen werden Provider Independent – Adressen genannt, da sie unabhängig von einer LIR bezogen werden.

Diese Adressen werden oft auch in kleinen Blöcken zwischen ::/32 und ::/48 von der RIPE zugewiesen, also Prefix-Größen, für die die weltweite Erreichbarkeit eigentlich nicht sichergestellt ist. Diese Blöcke werden aus einem von der RIPE fest definierten Bereich 2001:678::/29 vergeben. Da die RIPE aber in ihrer Policy definiert, dass sie aus diesem Bereich kleine Blöcke bis zur Größe ::/48 vergibt, werden diese in diesem speziellen Fall von allen Internet Routerbetreibern akzeptiert.

Dieses Beispiel könnte Grundlage für eine Lösung zur Sicherstellung des IPv6 Routings für die öffentliche Verwaltung in Deutschland sein.

7.1.3 Fazit mit Anforderung

Eine wesentliche Anforderung an ein Routingkonzept für die Datenkommunikation der öffentlichen Verwaltung in Deutschland ist die dauerhafte Sicherstellung des weltweiten Routings der de.government Adressen, trotz eines aufgeteilten Adressbereichs und einer verteilten Netzinfrastruktur. Aufgrund dieser Rahmenbedingungen ist es für die Sicherstellung des Routings des Adressbereichs von de.government, de.gov und de.pub.gov, im Internet notwendig, Maßnahmen zu ergreifen. Diese sollen sicherstellen, dass möglichst unabhängig von Änderungen der Internet Routing Best Practices die Erreichbarkeit der Adressräume de.gov und de.pub.gov weltweit langfristig sichergestellt ist. Hierzu ist es zum einen notwendig, dass der IPv6-Adressraum der LIR de.government in geeigneter Weise und in geeigneter Aufteilung im Internet via BGP annonciert wird und zum Anderen müssen die Datenpakete für diesen Adressbereich von allen relevanten Routern zuverlässig weitergeleitet werden.

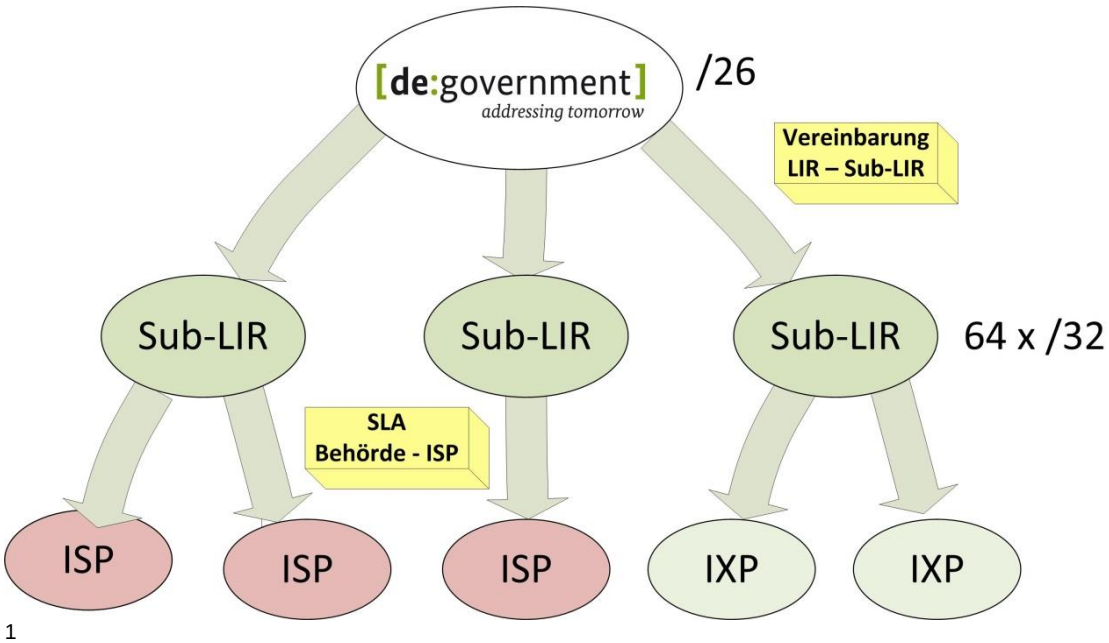
7.1.4 Lösungsdiskussion

Natürlich wäre es theoretisch möglich, dass die öffentliche Verwaltung in Deutschland ihren IPv6 Adressraum vollständig aggregiert, also quasi an einem Stück im Internet via BGP annonciert. Dies würde allerdings voraussetzen, dass es einen einheitlichen Internetübergang auf einer gemeinsamen Infrastruktur gäbe.

Eine solche zentralisierte Infrastruktur ist sowohl politisch als auch technisch kaum umsetzbar.

Somit muss ein Lösungsansatz darauf basieren, dass die Annoncierung des Adressraums dezentral erfolgt, aber dennoch durchgängig sichergestellt ist.

Es stellt sich die Frage nach einer Routingverantwortung, welche Verwaltungsebene sich für die Sicherstellung des Routings auf welcher „specific“ Ebene verantwortlich zeichnet.



[1]

Abbildung 13: IPv6 Routing Verantwortung im Internet

Die Konzeption für das Routing des de.government Adressbereichs für Datenkommunikation mit dem Internet teilt sich in mehrere Funktionsbereiche auf:

- Jede Behörde annonciert zunächst ihren Teil des IPv6 Adressraums de.gov den sie über die LIR de.government erhalten hat vollständig! Häufig wird dies nicht durch die Behörde selbst, sondern durch einen ISP oder einen anderen IT-Dienstleister der Behörde erfolgen müssen.

  Hieraus folgt die oben beschriebene Problematik von vielen Routen-Annoncierungen kleiner Prefixe. Deshalb muss zunächst in einem ersten Lösungsschritt das Routing dieser kleinen Prefixe der öffentlichen Verwaltung innerhalb der Deutschen Teilnetze des Internets sicherge-

[1] Legende zur Abbildung: ISP – Internet Service Provider; IXP - Internet Exchange Point; Sub-LIR – Sub-Local Internet Registry

stellt werden.

In einem zweiten Lösungsschritt muss das Routing zu diesen Deutschen Teilnetzen des Internets über aggregierte Routen-Annoncierungen aus dem weltweiten Internet sichergestellt werden.

- Die Sub-LIRs annoncieren ihre gesamte Sub-Allocation, welche sie von der LIR de.government erhalten haben, ebenfalls vollständig in Richtung Internet. Ggf. erfolgt dies wiederum über den ISP oder den IT-Dienstleister der Organisation, welche die Verantwortung für die jeweilige Sub-LIR trägt.
- Zur vollständigen Sicherstellung des weltweiten Routings des de.government IPv6-Adressraums wird zudem der gesamte Adressraum, aktuell ::/26, zentral durch oder im Auftrag des BMI in Richtung Internet annonciert.

7.1.4.1 Grüne Wolke - Lösungsschritt 1

Für die korrekte Weiterleitung der Datenpakete auch an die kleinen annoncierten Prefixe ist immer die kooperative Mitwirkung aller Internet Provider, die Behörden in Deutschland anbinden, notwendig.

Diese notwendige kooperative Mitwirkung wird kurz am Beispiel eines Bundeslands mit einer Sub-LIR und seinen Kommunen skizziert:

Das Bundesland nimmt seine Routingverantwortung für den IPv6 Adressraum seiner Sub-LIR war und beauftragt seinen Netzdienstleister A, seinen gesamten IPv6 Adressraum (::/30) mittels BGP zu annoncieren.

In diesem Adressraum liegen auch die kleineren Adressbereiche der Kommunen dieses Bundeslands. Eine Kommune beauftragt ebenso ihren Netzdienstleister B, den von der Sub-LIR des Landes an die Kommune zugewiesene Adressraum (::/40) zu annoncieren.

Fremde Router im Internet, welche die Route (::/40) zur Kommune nicht in ihren Routingtabellen speichern, senden in diesem Fall sämtlichen Datenverkehr für die Kommune an den oder die Router von Netzdienstleister A

des Landes.

Damit der Datenverkehr trotzdem die Kommune erreicht, muss Netzdienstleister A die empfangenen Datenpakete an seine Konkurrenz den Netzdienstleister B weiterleiten.

In diesem Fall würde der Netzdienstleister A der Sub-LIR, z.B. eines Bundeslandes Verkehr transportieren, der eigentlich von einem Konkurrenzunternehmen, Netzdienstleister B, transportiert werden müsste. Dies wird als sogenannter „Transit“ bezeichnet und ist heutzutage im Innenverhältnis der ISPs kostenpflichtig. Kostenfrei ist diese Art der Durchleitung von Fremdverkehr nur, wenn zwei ISPs bilateral ein sogenanntes Peering-Abkommen abgeschlossen haben.

Die Unterbindung von gewünschter Datenkommunikation mit dem Internet aufgrund fehlender Peering-Abkommen zwischen ISPs würde den Zielen des gemeinsamen Adressraums zuwiderlaufen und muss unbedingt verhindert werden. Deshalb wurde in der IPv6 Arbeitsgruppe das Konzept des sogenannten „**Grüne Wolke Zertifikat**“ entwickelt.

ISPs von Behörden sollen sich darin verpflichten,

- kostenneutral Fremdverkehr mit dem Ziel de.government Adressraum anderer ISPs weiterzuleiten und
- alle notwendigen Routingeinträge für die korrekte Weiterleitung in den Routingtabellen ihrer Router zu halten (BGP More Specifics)

um sicherzustellen, dass gewünschte IPv6-Datenkommunikation zwischen Behörden und Internetteilnehmern immer sicher möglich ist. Dieses Vorgehen ist in jedem Fall notwendig, da die Organisationen der öffentlichen Verwaltung in Deutschland wahlfrei über alle Anbieter Internetkopplungen betreiben.

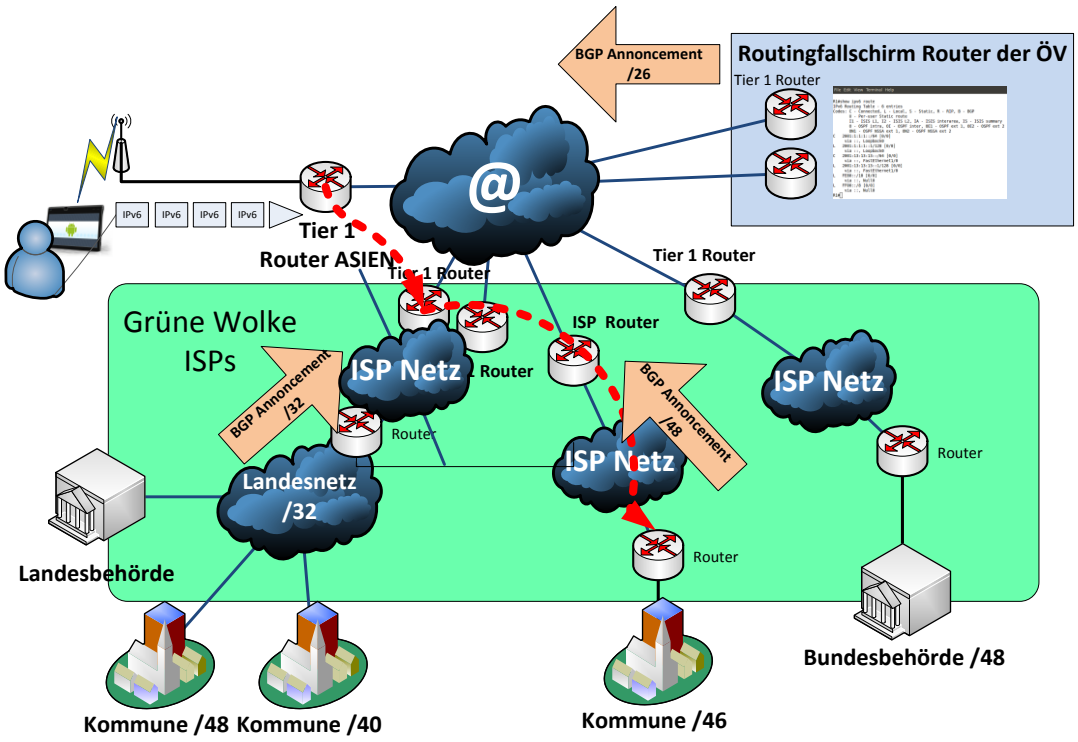


Abbildung 14: Prinzip der Grünen Wolke

Um diese übergreifende Policy deutschlandweit bei den relevanten ISPs durchzusetzen, muss der Bund stellvertretend für die gesamte öffentliche Verwaltung mit einer entsprechenden Rahmenvereinbarung auf die Provider zugehen. Für die zusätzlich notwendigen bilateralen Vereinbarungen zwischen einzelner Behörde und Provider ist eine Mustervorlage erforderlich.

7.1.4.2 Routingfallschirm - Lösungsschritt 2

Mit Lösungsschritt 1, der Grünen Wolke, ist sichergestellt, dass wenn ein Datenpaket für eine Behörde in Deutschland einen Router eines deutschen Behörden ISPs oder IT-Dienstleisters passiert, es immer die richtige Behörde erreicht. Nun muss noch sichergestellt werden, dass alle Datenpakete einen solchen Router im Internet auch erreichen. Der optimale Fall der Wegeführung ist dabei, dass das jeweilige Datenpaket sein Ziel durch die Annoncierung der direkten Route zu einem, ggf. auch kleineren Prefix erreicht. Dies wird voraussichtlich auch häufig der Fall sein aber, wie oben beschrie-

ben eben nicht immer sichergestellt sein. Deshalb müssen darüber hinaus Adressbereiche zur Sicherstellung des weltweiten Routings auf drei Ebenen annonciert werden:

1. ::/40 und kleiner durch die ISPs der Nutzer der einzelnen Prefixe
2. N x ::/32 durch die Sub-LIRs oder beauftragte ISPs
3. ::/26 (ggf. später ::/25) durch zentrale Router-Instanz im Auftrag des BMI

Die Annoncierung auf verschiedenen Ebenen führt zu einer Teilentlastung der Router, welche den gesamten Adressbereich annoncieren. Im BGP-Routing des Internet gilt das Prinzip, dass immer die genaueste Regel in der Routingtabelle eines Routers „gewinnt“ und angewandt wird. Hierdurch bedingt wird im Internet zielnah generierte Kommunikation oftmals ohne den Umweg über die zentralen Aggregations-Router direkt dem Zielstandort zugeführt.

Das BMI hat die Zielsetzung das weltweite IPv6 Routing des de.government Adressraums in jedem Fall sicher zu stellen und plant daher die Implementierung einer Router-Instanz, die den gesamten /26 Adressraum im Internet annonciert. Damit übernimmt das BMI die oberste Routingverantwortung in Richtung Internet.

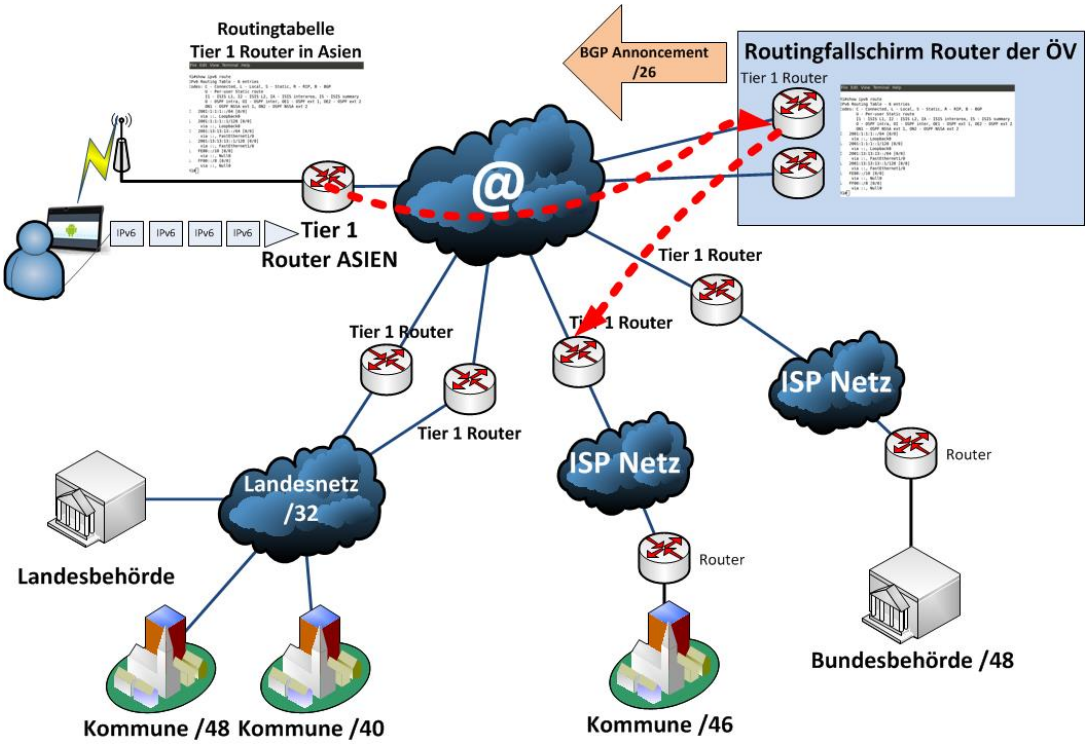


Abbildung 15: Prinzipdarstellung Routingfallschirm

Wichtig:

Das Grundkonzept sieht vor, dass die behördenrelevanten Internetrouter Adressbereiche nur in Richtung Internet annoncieren um gewünschten Verkehr zwischen Internet und Behörden zuverlässig zu ermöglichen.

Die Blockierung unerwünschter Datenverbindungen geschieht dann über Accesslisten auf diesen Routern oder dahinter geschalteten Firewallsystemen. Ankommender oder abgehender Verkehr zu anderen Behörden im IPv6-Adressraum de.pub.gov der LIR de.government wird hier blockiert!

Diese Konzeption bildet die Anforderungen des IT-NetzG auf der Ebene des IPv6 Routings ab.

7.2 Ausgangssituation Sicherheit (Darknet Traffic und Highjacking)

Die Routingfunktion ist insbesondere im Internet einigen Sicherheitsrisiken ausgesetzt, zu denen in diesem Konzept Maßnahmen beschrieben werden.

Hierzu gehören die missbräuchliche Entführung von Adressräumen (Hijacking) sowie das Abfangen von Datenverkehr zu Adressenräumen, die zwar Teil des Adressraums sind, aber keiner Infrastruktur zugeordnet sind. Dieser sogenannte Darknet Traffic resultiert aus Angriffsversuchen und fehlkonfigurierten Systemen Dritter. Aus der Abschöpfung dieses Verkehrs lassen sich oft sensitive Daten extrahieren.

7.2.1 Darknet Traffic - Maßnahmen

Aus Sicherheitsgründen, um zu verhindern das Darknet Traffic der öffentlichen Verwaltung von Dritten abgeschöpft werden kann, sollte der gesamte Adressbereich als ::/26 auf einem vertrauenswürdigen Router via BGP annonciert werden. Darüber hinaus müssen auf kleinerer Aggregationsebene die ungenutzten Bereiche der Größe ::/32 und kleiner ebenfalls einzeln annonciert werden.

Es bietet sich an, dort diesen Verkehr durch ein CERT überwachen und analysieren zu lassen, um Informationen über Angriffe und Angriffsversuche zu erhalten. Ggf. müssten hierzu datenschutzrechtliche Fragen zwischen Bund und Ländern (Kommunen) geklärt werden.

7.2.2 Adressraum Highjacking

Um zu verhindern, dass andere Organisationen im Internet technisch vorgeben können, der Adressraum von de.government (oder Teile davon) gehöre ihnen und so die legitimen Systeme und Netze im Internet nicht mehr erreichbar wären, müssen neben der durchgehenden Annoncierung (siehe vorheriges Kapitel) alle Annoncierungen mit dem sogenannten RPKI-Verfahren digital signiert werden. Dies gibt auch das BSI für Behörden vor.

Diese Aufgabe sollte zentral durch die LIR de.government sichergestellt werden.

8 UMSETZUNG UND MASSNAHMEN

Die konkrete Umsetzung und detaillierte Definition der erforderlichen Maßnahmen erarbeitet die IPv6 AG.