HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Mailserver und Spamschutz unter IPv6

Heinlein Professional Linux Support GmbH
Peer Heinlein
<p.heinlein@heinlein-support.de>

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Some Bits and Pieces...

- Wir haben 2^128 IP-Adressen (statt wie bisher 2^32!)
  - Systeme kriegen immer gleich ganze IP-Netze zugewiesen
- DHCP hat umfangreiche Auto-Konfigurationsmechanismen
  - IP-Vergabe (ex DHCP), Routing-Infos, DNS-Infos
  - Ist ein System mit IPv6 im Netz stellt es sich ggf. schnell als Gateway für die anderen dar
- Ein System hat schneller IPv6, also man das selber wollte :-)

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Spammer und IPv6: Der status quo

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Wenig Spam zu sehen...

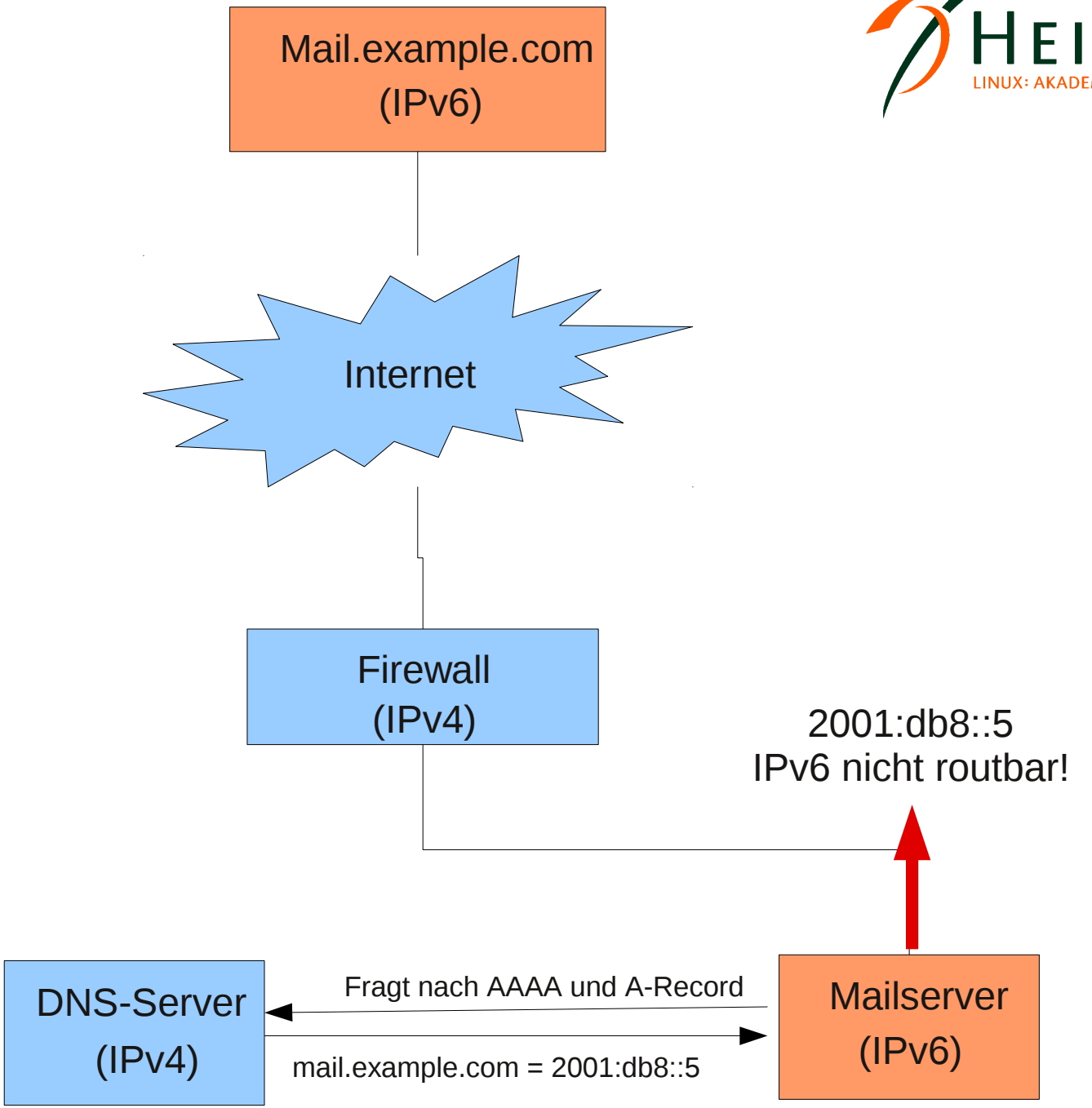
- Mailtraffic, der über IPv6 reinkommt, hat einen sehr geringen Spam-Anteil
- Sind die Spammer zu doof IPv6 zu nutzen?
- Nein!
  - IPv6 bislang fast nur für ISPs verfügbar, nicht für Endkunden.
  - Spam wird aber größtenteils über Botnetze verschickt
  - Breitband-DSL mit IPv6 ist wenig vorhanden => wenig Spam.
  - NOCH. :-)

Postfix und IPv6

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Postfix und IPv6

- Achtung: Viele Distributionen aktivieren schon lange unbemerkt IPv6!
  - Postfix will ebenfalls IPv6 nutzen!
- Problem: Zwar hat der Host lokal IPv6, Firewall/Upstream können aber nur IPv4
  - Postfix sucht versucht Domains mit IPv6-Relays auch auf IPv6 zu kontaktieren und rennt in Timeouts => Ziele nicht erreichbar


Mail.example.com
(IPv6)
Internet
Firewall
(IPv4)
2001:db8::5
IPv6 nicht routbar!
DNS-Server
(IPv4)
Fragt nach AAAA und A-Record
mail.example.com = 2001:db8::5
Mailserver
(IPv6)

Weniger ist mehr: Wenn man doch nur IPv4 haben will

- Die verschiedenen Protokolle werden über „inet_protocols“ gesteuert.
- Ohne IPv6-Uplink, sollte Postfix auf IPv4 limitiert werden:

```
Postconf -e „inet_protocols=ipv4“
```

- Und wer beides machen kann, der sich öffnen:

```
Postconf -e „inet_protocols=all“
```

Postfix und IPv6: Jetzt aber wirklich

- Postfix kann problemlos mit IPv6 umgehen
  - IPv6-Adressen müssen immer in eckigen Klammern geschrieben werden!
- Durch $mynetworks_style findet man IPv6 auch schnell automatisch in $mynetworks

```
mynetworks = 127.0.0.0/8 91.198.250.0/24 [::1]/128 [fe80::]/64
[fe80::250:56ff:feb5:d]/64
```

- Auch in den access-Maps kann sofort IPv6 genutzt werden

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Postfix und IPv6: Jetzt aber wirklich

- Bei $inet_interfaces=all öffnet Postfix die Ports sowohl unter IPv4 als auch unter IPv6

```
smtp       inet  n   -   y   -   500    smtpd
```

- In der master.cf können Ports auch gezielt an IPv6 gebunden werden

```
[2001:67c:2050::2]:smtp   inet  n   -   y   -   500    smtpd
```

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

RBLs und IPv6

RBLs und IPv6: status quo

- RBLs listen IP-Adressen, von denen aus Spam versandt worden ist
  - Genutzt werden Techniken, mit denen sonst DNS Reverse-Lookups gemacht werden
- Grundsätzlich geht das auch problemlos mit IPv6-Adressen

RBLs und IPv6: Der Haken

- Bei IPv6 erhält jeder Host immer gleich ein ganzes Subnetz zugeteilt, also viele Adressen.
  - Das ist je nach Provider ein /56 oder ein /64er Netz.
  - Also SEHR viele Adressen.
- Problem: Spammer können für jede Spam-Mail eine neue IP-Adresse nehmen.
- Problem: Wie groß ist denn das Subnetze eines Hosts?
  - Es ist unklar, welcher Netzbereich komplett auf RBLs wandern darf!
  - Block zu klein: Spammer hat genug saubere IPs.
  - Block zu groß: Unschuldige werden geblacklisted.

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

RBLs und IPv6

- RBLs helfen also prima gegen echte Mailrelays, über die Spam verschickt wird, denn die machen kein IP-Hopping
  - Gehackte Webseiten & Co
- RBLs helfen eventuell nur eingeschränkt gegen Botnetz-PC mit Spammer-Software drauf
  - Mal abwarten. ob/wie das genutzt wird.
- RBLs werden zukünftig eher zu WBLs, also Whitelists
  - Spamhaus hat WBL-Projekt bereits gestartet

policyd-weight und IPv6

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

policyd-weight: Nichts ist auch gut

- policyd-weight macht einen Plausibilitätscheck über die Angaben, die das einliefernde System im SMTP-Protokoll gemacht hat.
  - Besonders wird dabei Reverse-Lookup und HELO beachtet
- policyd-weight kann bei IPv6-Adressen nichts sinnvolles berechnen
  - Aber er stört sich aber auch nicht dran, liefert ein leeres Ergebnis ohne Auswirkung zurück an Postfix („DUNNO“).
- Schade, aber so funktioniert alles weiterhin.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Greylisting und IPv6

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Greylisting: Der Retter in der Not

- Greylisting ist – allen Unkenrufen zum Trotz – seit vielen Jahren der beste und nebenwirkungsfreieste Spamschutz, den es gibt.
  - Man muß es nur richtig einsetzen.
  - Ja, Spammer haben mit Greylisting massive Probleme
    - [Details dazu in unserem Vortrag über SPF, DKIM und Greylisting.]
- Spammer, die unter IPv6 nun ständig IP-Adressen wechseln um RBLs auszutricksen werden wegen mit den vielen neuen IPs nicht mehr effektiv genug durch Greylisting durchkommen.
  - Greylisting und RBL sind also wieder einmal ein Dreamteam, das sich gegenseitig absichert. Genial.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SpamAssassin

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

SpamAssassin: Nichts besonderes

- Auch SpamAssassin hat mit IPv6 keine Probleme
  - RegExp-Pattern auf Viagra im Body gehen immernoch
  - Bayes-Filter gehen natürlich auch
  - Die von SpamAssassin geprüften RBLs gehen (prinzipiell) auch.
- Also alles schick.

	Ipv4 22.5. - 2.6.				Ipv6 22.5. - 2.6.		
	Prozent	Gesamt			Prozent	Gesamt	
20,82216299	20,82216299	854360	Erwünschte Nachrichten	66,05807126	66,05807126	8213	Erwünschte Nachrichten
79,17783701	19,68751645	807804	Ungültige Absender-Domain	33,94192874	3,072468431	382	Ungültige Absender-Domain
	0,002315307	95	Greylisting		11,66251106	1450	Greylisting
	4,526522205	185729	Unbekanter Empfänger		18,79675058	2337	Unbekanter Empfänger
	5,753586045	236077	SpamAssassin-Befund		0,402155554	50	SpamAssassin-Befund
	0	0	Virus		0	0	Virus
	0,057712067	2368	RegExp-Filter		0,008043111	1	RegExp-Filter
	38,70522684	1588125	Policyd-Weight		0	0	Policyd-Weight
	10,44495809	428570	RBL Spamhaus/NiXSpam		0	0	RBL Spamhaus/NiXSpam
	100	**4103128**			**100**	12433	

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Praxis:
Die ersten Schritte unter IPv6

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Die Geister, die ich rief...

- Man braucht einen Server mit IPv6-Anbindung im Upstream
  - Verschiedene Root-Server mit IPv6
  - Eventuell echter IPv6-Upstream
  - Hilfsweise IPv6 getunnelt von IPv6-Tunnelbrokern wie sixx.net
- Achtung: DHCP & Co unter IPv6 funktionieren ganz anders
  - IPv6 bringt automatisches „Neighbour Discovery“ mit
  - Schnell haben auch andere Rechner im LAN einen funktionierenden IPv6-Uplink
  - Ganz schnell überbrückt sowas die Firewall und alles steht offen im Netz

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Okay, aber was ist mit dem Rest?

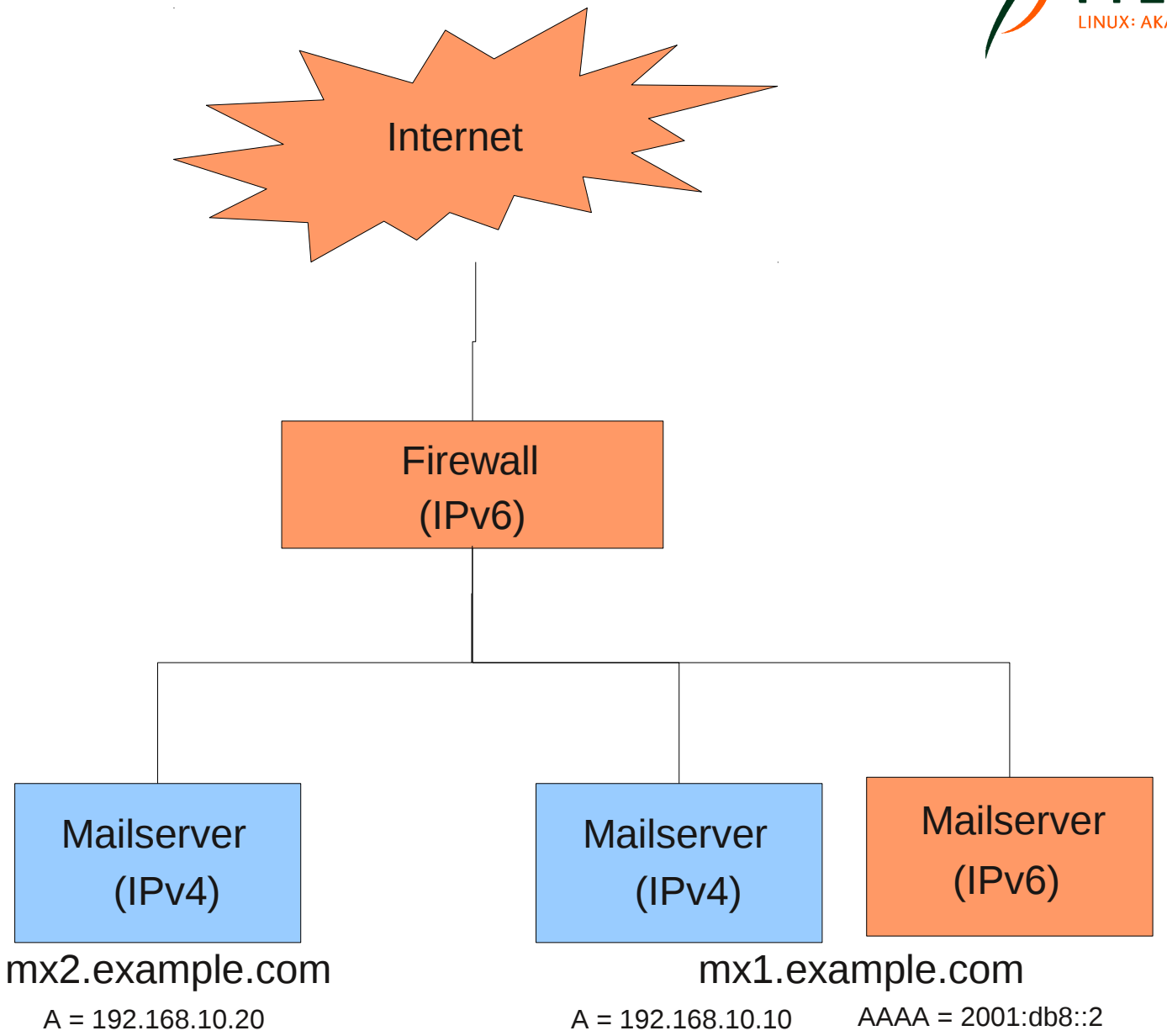
- Bei echtem IPv6-Uplink muß die Firewall IPv6 beherrschen...
  - Viele Firewalls können nur IPv4
  - Manche Firewalls routen IPv6 einfach ungefiltert
- Andere Infrastruktur muß mit IPv6 eigentlich nichts am Hut haben
  - Amavis => Anbindung an Postfix über IPv4 weiterhin möglich
  - DNS-Server => Auch ein überIPv4 angebundener DNS-Resolver kann IPv6-Adressen auflösen!

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

So gelingt der Start

- Variante 1: Bestehende IPv4-Hosts erhalten auch IPv6-Netz
- Variante 2: Ein eigener IPv6-Testserver soll her

- In beiden Fällen gilt:
  - Ein Hostname hat im DNS eine IPv4-Adresse („A-Record“) und eine IPv6-Adresse (AAAA-Record)
  - Also: Keine neuen Hostnamen, sondern ggf. nur zusätzliche DNS-Records
  - Auch wenn's der gleiche Hostname ist kann beides auf verschiedene physikalische Systeme zeigen („quick and dirty“)
  - Der MX-Record bleibt gleich, über A und AAAA wird der Traffic aufgesplittet


Internet
Firewall
(IPv6)
Mailserver
(IPv4)
Mailserver
(IPv4)
Mailserver
(IPv6)
mx2.example.com
A = 192.168.10.20
mx1.example.com
A = 192.168.10.10
AAAA = 2001:db8::2

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Was ist, wenn's nicht klappt?

- Praxistipp 1:
  Es schadet nicht, einen MX-20-Record zu haben, der nur auf einen IPv4-Host zeigt
  - So werden im Zweifel alle Mails ganz klassisch noch aufgefangen, die bei kaputtem IPv6 sonst irgendwo stranden würden

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Achtung: IPv6-only geht nicht

- Praxistipp 2:
  Auch ein IPv6-Mailserver sollte über IPv4-Adressen und IPv4-Routing verfügen („dual stack“)
  - Es können jederzeit Bounces oder Weiterleitungen an Mailadressen entstehen, die nur über IPv4 zu erreichen sind!

- Mailserver sind ein dankbares System, um IPv6 einzuführen
  - Wenn's mal nicht geht, kommt die Mails halt über IPv4 rein.

- Also: Los geht’s, viel Spaß.

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Soweit, sogut.

Fragen? Fragen!

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Und nun...

- **Vielen Dank für's Zuhören...**
- **Schönen Tag noch...**
- **Und viel Spaß an der Tastatur.**
- **Bis bald.**

HEINLEIN
LINUX · AKADEMIE · SUPPORT · HOSTING

Wir suchen:
Admins, Consultans, Trainer!

Wir bieten:
Spannende Projekte, Kundenlob, eigenständige Arbeit, keine Überstunden, Teamarbeit

...und natürlich: Linux, Linux, Linux...

http://www.heinlein-support.de/jobs

HEINLEIN
LINUX: AKADEMIE · SUPPORT · HOSTING

Heinlein Professional Linux Support GmbH:

- AKADEMIE
  - Von Profis für Profis: Wir vermitteln die oberen 10% Wissen. Geballtes Wissen und umfangreiche Praxiserfahrung aus erster Hand.
- SUPPORT
  - Wir sind das Backup für Ihre Linux-Administration: LPIC-2-Profis lösen im Heinlein CompetenceCall Notfälle, auf Wunsch auch in SLAs mit 24/7-Verfügbarkeiten.
- HOSTING
  - Wenn Hosting kein Massengeschäft sein darf: Individuelles Business-Hosting mit perfekter Maintenance durch unsere Linux-Profis. Sicherheit und Verfügbarkeit werden bei uns groß geschrieben.