Webhosting on IPv6-only Virtual Machines

Wolfgang Zenker

Dubai, October 25, 2017

punkt.de

Webhosting for small to medium sized websites

Model	Separation	Security	File access	Shell	Webserver	Database	php
old	nameVirtual Host	suexec	ftp (chroot)	no	shared	shared	shared

Webhosting for small to medium sized websites

Model	Separation	Security	File access	Shell	Webserver	Database	php
old	nameVirtual Host	suexec	ftp (chroot)	no	shared	shared	shared
new	jail	jail	ftp, scp	root	own	own	own

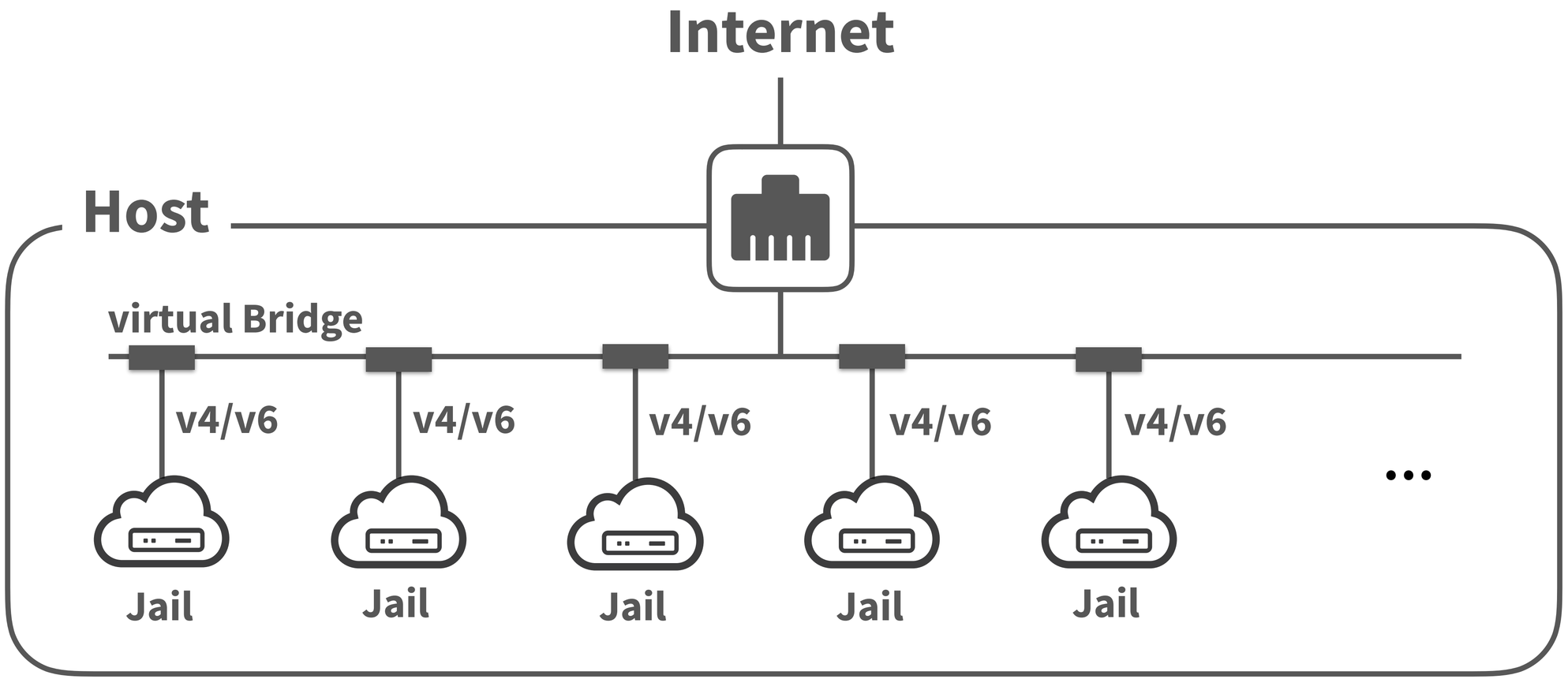
FreeBSD jails

- Jails are lightweight virtual machines
- Extension of chroot model: partition not only file system but also process table, network- and IPC-stack etc.

We use jails combined with ZFS datasets

- System environment on r/o mount from host
- Application environment on r/o mount from blueprint
- Configuration defaults copied from blueprint to r/w dataset
- r/w dataset for application data and software

Jail hosting – version 1



SSL

“dehydrated” script running in each jail to aquire SSL certificates from “Let's Encrypt”

IP Address requirement

old model: one address shared by all websites on one physical machine

new model: one address per website

IP Address requirement

old model: one address shared by all websites on one physical machine

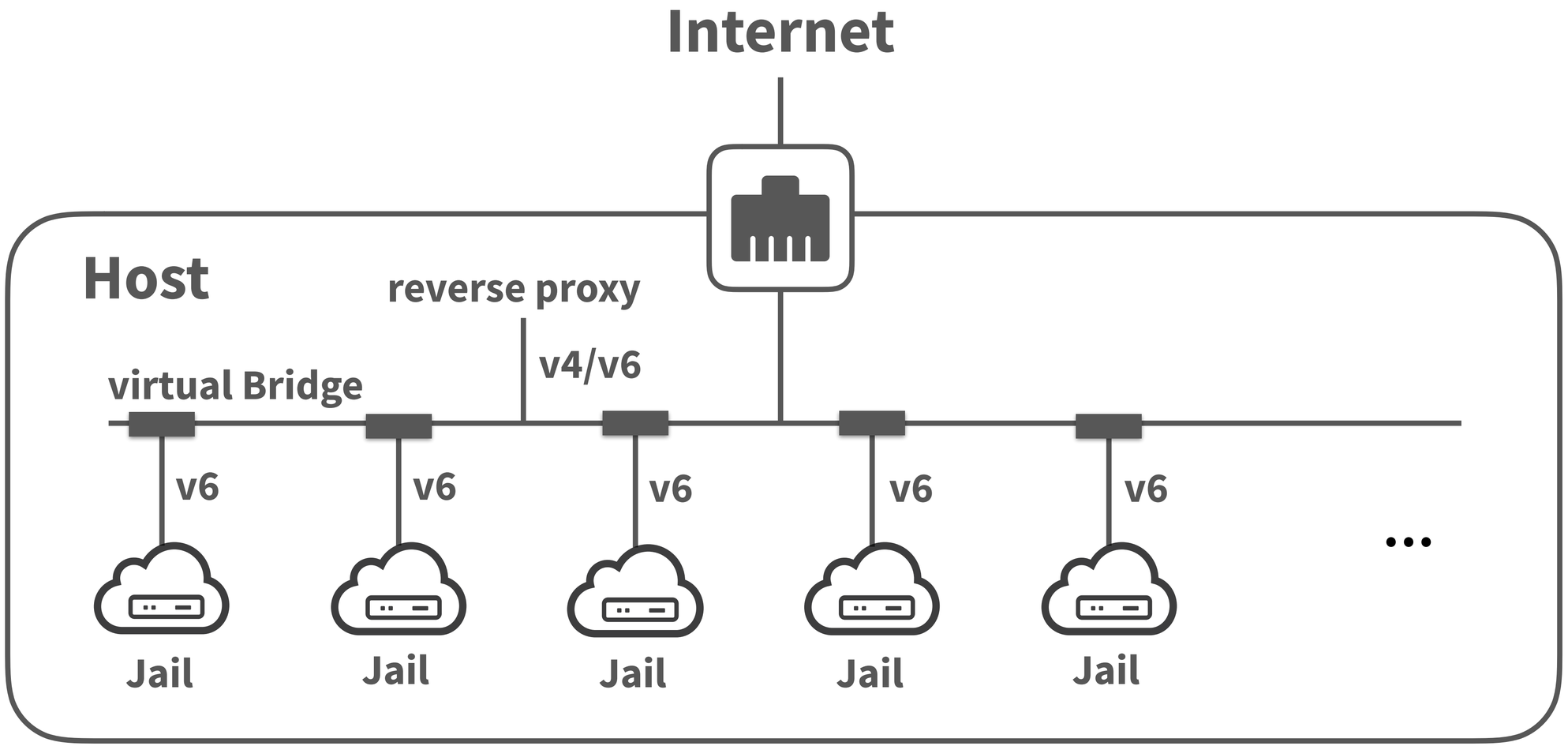
new model: one address per website

AS16188 address space

IPv4: 1 x /20, 1 x (final) /22
-> 5120 addresses

IPv6: 1 x /32
-> 79228162514264337593543950336 addresses

Jail hosting – version 2



First implementation for “nextcloud” hosting

- Application pre-installed
- Customer interacts per https only

SSL

- “dehydrated” script running on host only
- host has r/w access of jail dataset to provision certificate and key
- v4 SSL termination on host, proxy to v6 http on jail

At time of implementation, “Let's encrypt” would send challenges on IPv4 if signing request was by IPv4.

Problem

- Applications sends mail to users
- Some users don't have IPv6 on mailserver

Solution

- Use host system as outgoing mail relay

Problem

- “nextcloud” plugin repository is IPv4 only

Solution (kind of)

- disable plugin installation by customer

Problem

- Let’s encrypt now sends challenge on IPv6

Tried

- run “dehydrated” in jail

-> failed: “dehydrated” does not work on IPv6-only

Solution

- reverse proxy on jail for challenges, going to host IPv6

Problem

- Some webdav clients fail because of SSL termination on host

Solution (probably)

- proxy to https on jail instead of http

Outlook

For "generic" webhosting we expect more challenges:

- customers with IPv4-only need ssh access
- code repositories (e.g. GitHub, RubyGems, ...) are IPv4-only
- ...

Questions?

Thank you

Further questions: hosting@punkt.de

@punktdehosting

https://www.facebook.com/punkt.deGmbH/