Moderne Webserver

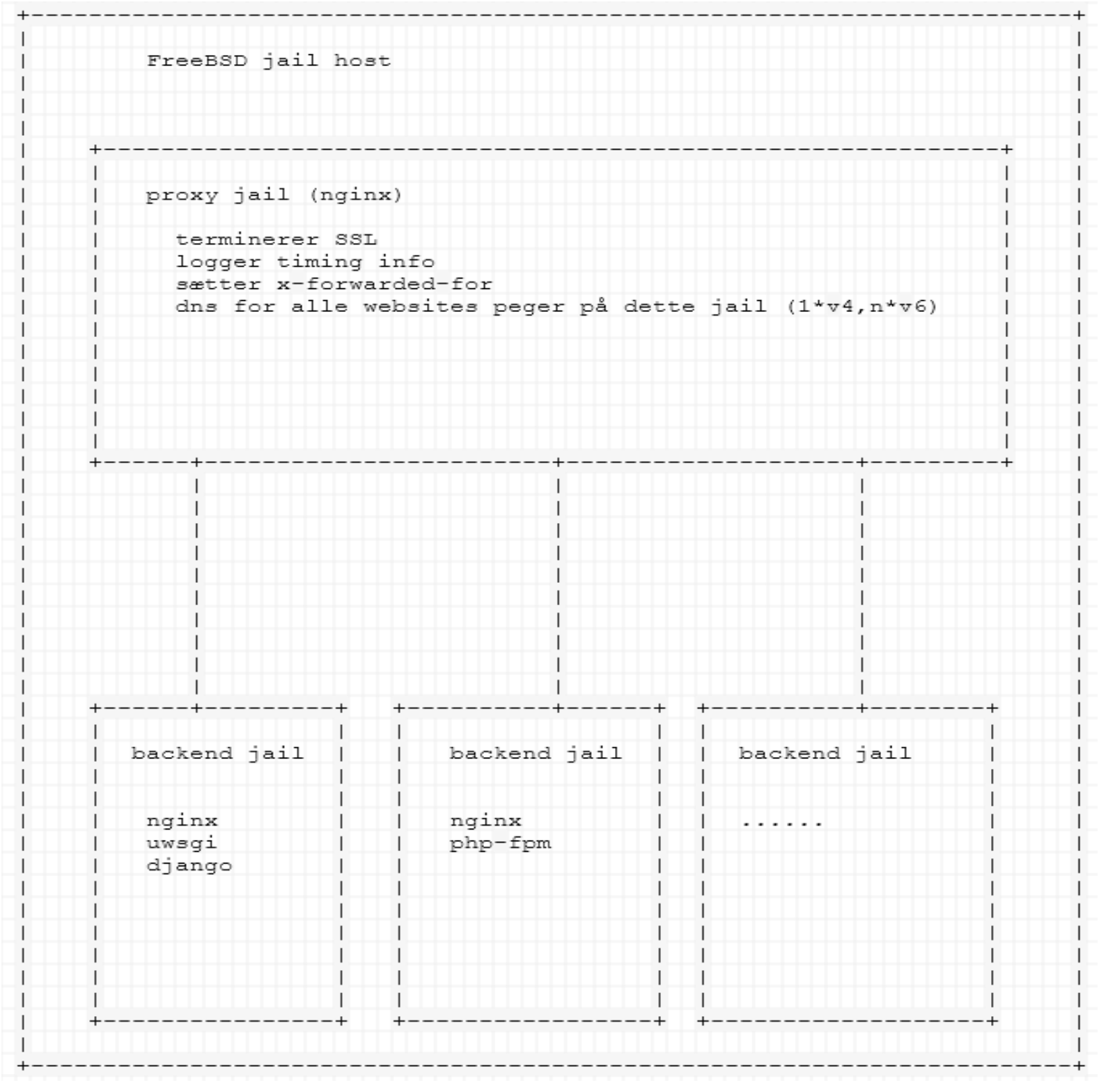
Thomas Steen Rasmussen
The Camp - 21. juli 2014

Moderne Webserver

- Overblik
  - problemet
  - web proxy jailet
  - backend jails
  - logging
- SSL
  - konfiguration
  - ocsp stapling
  - test med ssllabs
  - sslscout

Problemet

- Opdateringer
- Sikkerhed
- Seperation


FreeBSD jail host
proxy jail (nginx)
terminerer SSL
logger timing info
sætter x-forwarded-for
dns for alle websites peger på dette jail (1*v4,n*v6)
backend jail
nginx
uwsgi
django
backend jail
nginx
php-fpm
backend jail
.....

Web Proxy Jailet

- Har en ægte v4 og en masse v6 IPer
- Terminerer SSL og IPv6
- Alle DNS records peger på dette jail
- Logger performance info:

```
githubhook.hushfile.it - 192.30.252.44 - POST /githubhook.php HTTP/1.1 - HTTP 200 - upstream_response_time 3.123 - total_request_time 3.123
```

- Sætter x-forwarded-for header med klient IP

Backend Jails

- Et jail per website
- En skrabet nginx samt en ”content server” til dynamiske ting (uwsgi, php-fpm etc.)
- Næsten alt er mountet readonly
- Logfiler roteres hver nat

Nginx SSL Opsætning

```
ssl on;

ssl_certificate
/usr/local/etc/nginx/certificates/wildcard.hushfile.it.crt;

ssl_certificate_key
/usr/local/etc/nginx/certificates/wildcard.hushfile.it.key;

ssl_dhparam /usr/local/etc/nginx/certificates/hushfile.it-dhparam.pem;

ssl_trusted_certificate
/usr/local/etc/nginx/certificates/alphasl_root_and_intermediate_for_ocsp_
sha1.crt;


ssl_session_timeout 4h;

ssl_protocols TLSv1 TLSv1.1 TLSv1.2;

ssl_ciphers  ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:DH+AES:!3DES:!
RSA:!AES128:!ADH:!AECDH:!MD5:!DSS;

ssl_prefer_server_ciphers on;

ssl_session_cache shared:SSL:50m;

add_header Strict-Transport-Security max-age=31536000;

ssl_stapling on;

ssl_stapling_verify on;
```

OCSP Stapling

- OCSP er en ”mere realtime” måde at få info om certificate revocation status.
- OCSP er lidt langsomt, og meget skidt for privacy.
- OCSP stapling giver fordelene ved OCSP men uden ulemperne.
- Læs masser detaljer på https://blog.tyk.nu/blog/ocsp-stapling-in-nginx/

Test SSL opsætning

- https://www.ssllabs.com/ssltest/
- https://sslcheck.globalsign.com/
- Og flere... bruger samme rating guide: http://surl.dk/duw/

- Mere læsning om SSL best practices:
- http://surl.dk/dux/

sslscout

- Automatisk løbende check af SSL websites
- Work in progress
- Er basalt set en HTML scraper
- ”Følger” best practices

Afsluttende bemærkninger

- Husk altid ”Principle of least privilege”
- Hold øje med logs og grafer
- Hold software opdateret (mailing lister, irc)

Spørgsmål