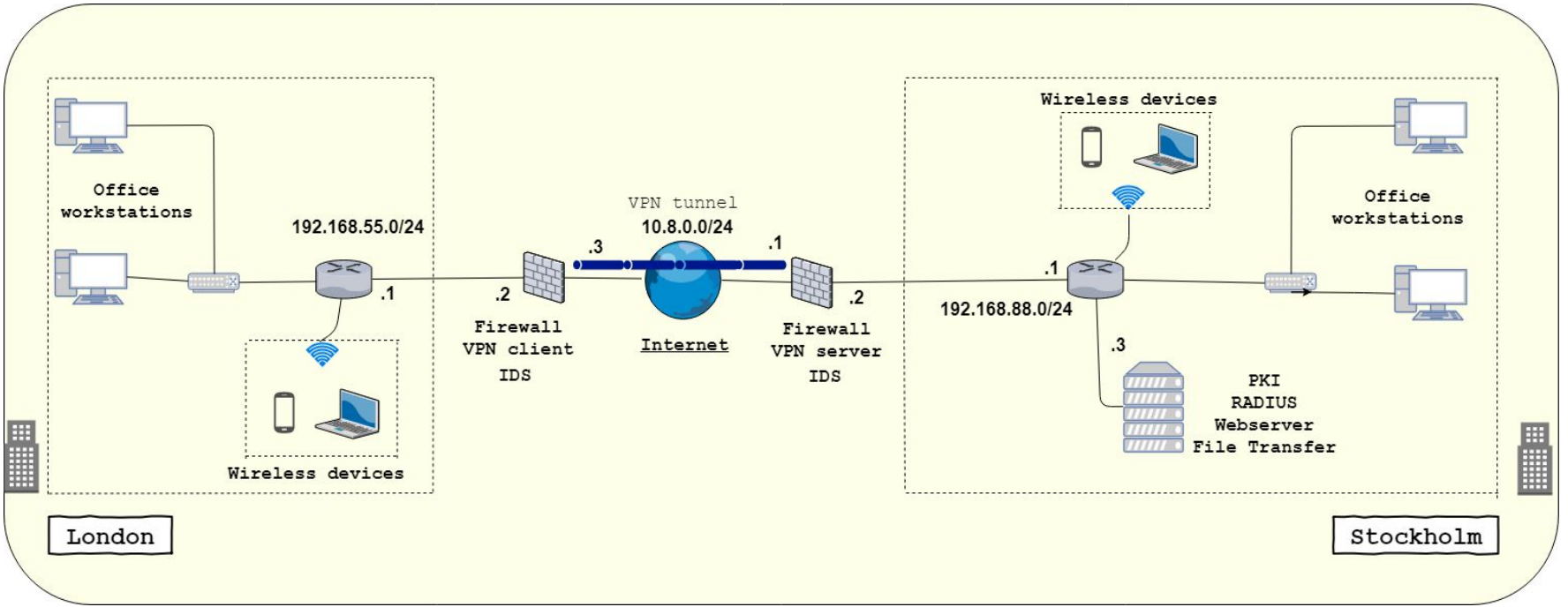
ACME network report

Michal Winiarski
Shubhanker Singh
Waseem Bhat

Network topology



Easypki

- create CAs
- create & sign certs
- revoke
- create crls

- can't create bundles

```
/root/pki
    |
    |-- rootCA
    |
    |-- acmeCA
        |
        |-- certs
        |
        |-- keys
        |
        |-- index.txt
```

OpenVPN

Server

symmetric key
Server's certificate & key

pushes Stockholm routes
acknowledges London routes

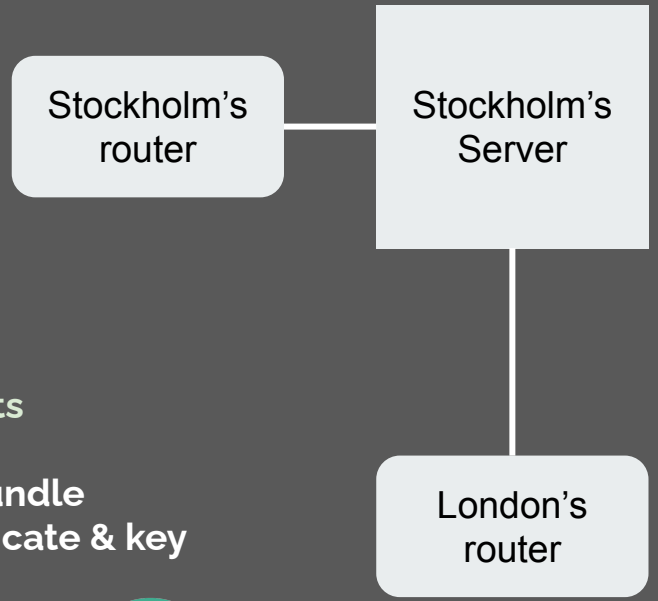
Client

symmetric key
Client's certificate & key

knows Stockholm's public IP

Wireless security

freeRadius
EAP-TLS



Server

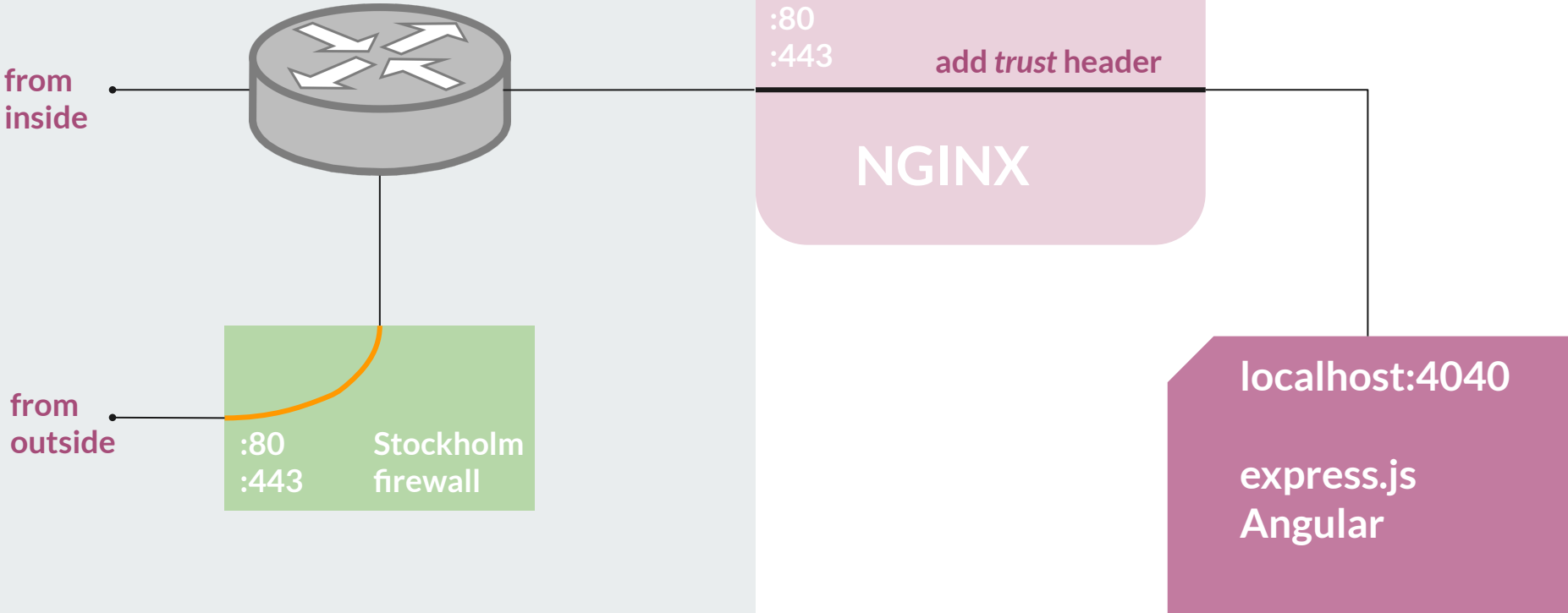
CA bundle
certificate & key

secret password shared with routers
must know routers' IPs

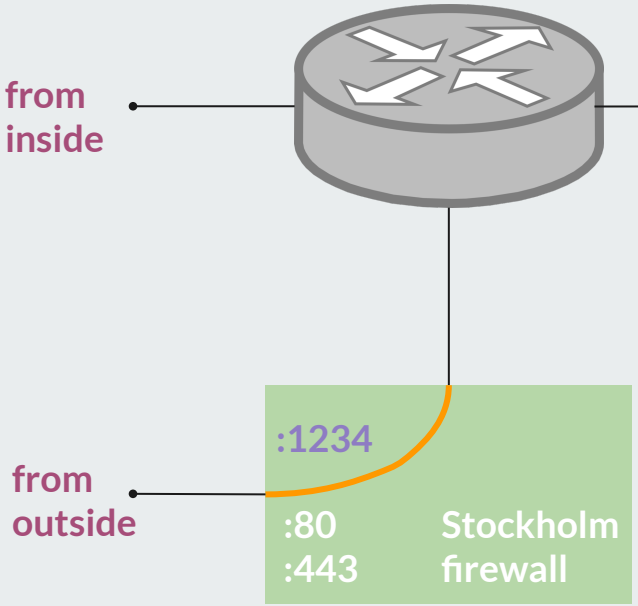
Clients

CA bundle
certificate & key

Web server


from
inside
:80
:443
add *trust* header
NGINX
from
outside
:80
:443
Stockholm
firewall
localhost:4040
express.js
Angular

File transfer server



Firewall-ing. Interesting things

- ➔ allow UDP port 1194 for both firewalls
- ➔ allow tcp :80 :443 (web) :1234 (file transfer) :1812 :1813 (radius) on server machine
- ➔ allow input to localhost on the server (nginx reverse proxy)
- ➔ forward ports :80 :443 and :1234 from Stockholm firewall to the server
- ➔ nat masquerade packets from inside networks to the internet

Intrusion detection system

- snort
- logging incoming ICMP packets

Thank you