

BGP-lastbalanse...proxy



SUNET-dagarna hösten 2017
Fredrik Thulin

Lastbalanserare eller proxy eller något annat

Vad ska vi med en sådan till?

- Mer än 1 GigE?
- Mer än 1000 samtidiga sessioner?
- Många nior?

99.99% i all ära

En server

Ett rack

En switch

Två routrar (VRRP)

En datorhall

Inget underhåll

= rätt bra chans till upptid över tre år

Två servrar

Två rack

Fyra switchar (LACP)

Fyra routrar

Två hallar

Regelbundet underhåll

= bra upptid, mycket tidsåtgång, skalar inte

Lättrörliga applikationer

Moln

Orkestrering

Containers

Stabila frontends

Par av proxys med failover

Två servrar

Ingen TCP state sync

HAproxy/LVS/annat

Samma L2

CARP/VRRP/heartbeat/annat

Antagligen active-standby

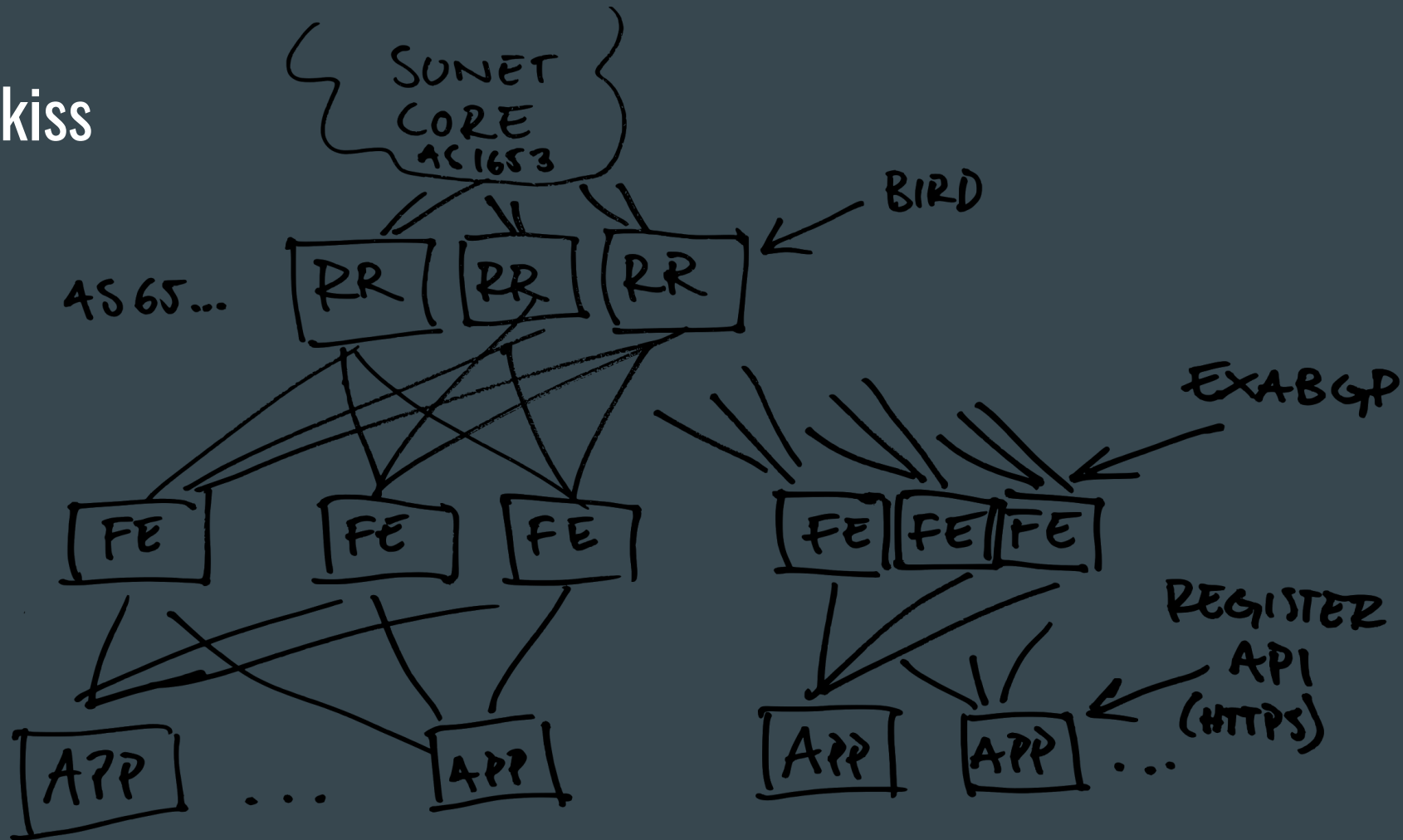
Mer än en hall - anycast

Måste interagera med routrarna

- Lätt!

Verktyg för att motverka DDoS

Skiss



exabgp monitor script

```
# cat /etc/bgp/monitor.d/10_www.dev.eduid.se

#!/bin/sh

STATUS=`/opt/frontend/haproxy/scripts/haproxy-status 'site=www.dev.eduid.se'`

if [ "x`echo $STATUS | grep ^UP\ ` " != "x" ]; then

    exec /etc/bgp/hooks/www.dev.eduid.se_UP.sh

elif [ "x`echo $STATUS | grep ^DOWN\ ` " != "x" ]; then

    exec /etc/bgp/hooks/www.dev.eduid.se_DOWN.sh

fi

echo "UNKNOWN STATUS for www.dev.eduid.se:"

echo "$STATUS"

exit 1
```


exabgp kommandon

```
# /etc/bgp/hooks/www.dev.eduid.se\_UP.sh
```

```
announce route 37.156.192.10/32 next-hop self local-preference 1000
```

```
announce route 37.156.192.11/32 next-hop self local-preference 1100
```

```
announce route 2001:6b0:60:c0::10/128 next-hop self local-preference 1000
```

```
announce route 2001:6b0:60:c0::11/128 next-hop self local-preference 1100
```

```
# /etc/bgp/hooks/www.dev.eduid.se_DOWN.sh
```

```
announce route 37.156.192.10/32 next-hop self local-preference 100
```

```
announce route 37.156.192.11/32 next-hop self local-preference 100
```

```
announce route 2001:6b0:60:c0::10/128 next-hop self local-preference 100
```

```
announce route 2001:6b0:60:c0::11/128 next-hop self local-preference 100
```

Att tänka på

Terminera TLS i frontend eller inte?

Övervakning

- LetsEncrypt

Separat konfigurationshantering för route reflectors och frontends?

Route filter etcetera

Eventuella brandväggar framför frontends kanske också måste peera med route reflectors