Welcome to

Simulated DDoS Attacks, breaking the firewall infrastructure

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Goal

Don’t Panic!

How to create DDoS simulations

Some actual experience with doing this

Evaluate how good is this, value

I use Kali 2.0 Linux for this

Kali Linux the new backtrack

BackTrack `http://www.backtrack-linux.org`

Kali `http://www.kali.org/`

hping3 packet generator

```
usage: hping3 host [options]
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood     sent packets as fast as possible. Don't show replies.
...
hping3 is fully scriptable using the TCL language, and packets
can be received and sent via a binary or string representation
describing the packets.
```

Hping3 packet generator is a very flexible tool to produce simulated DDoS traffic with specific charateristics

Home page: `http://www.hping.org/hping3.html`
Source repository `https://github.com/antirez/hping`

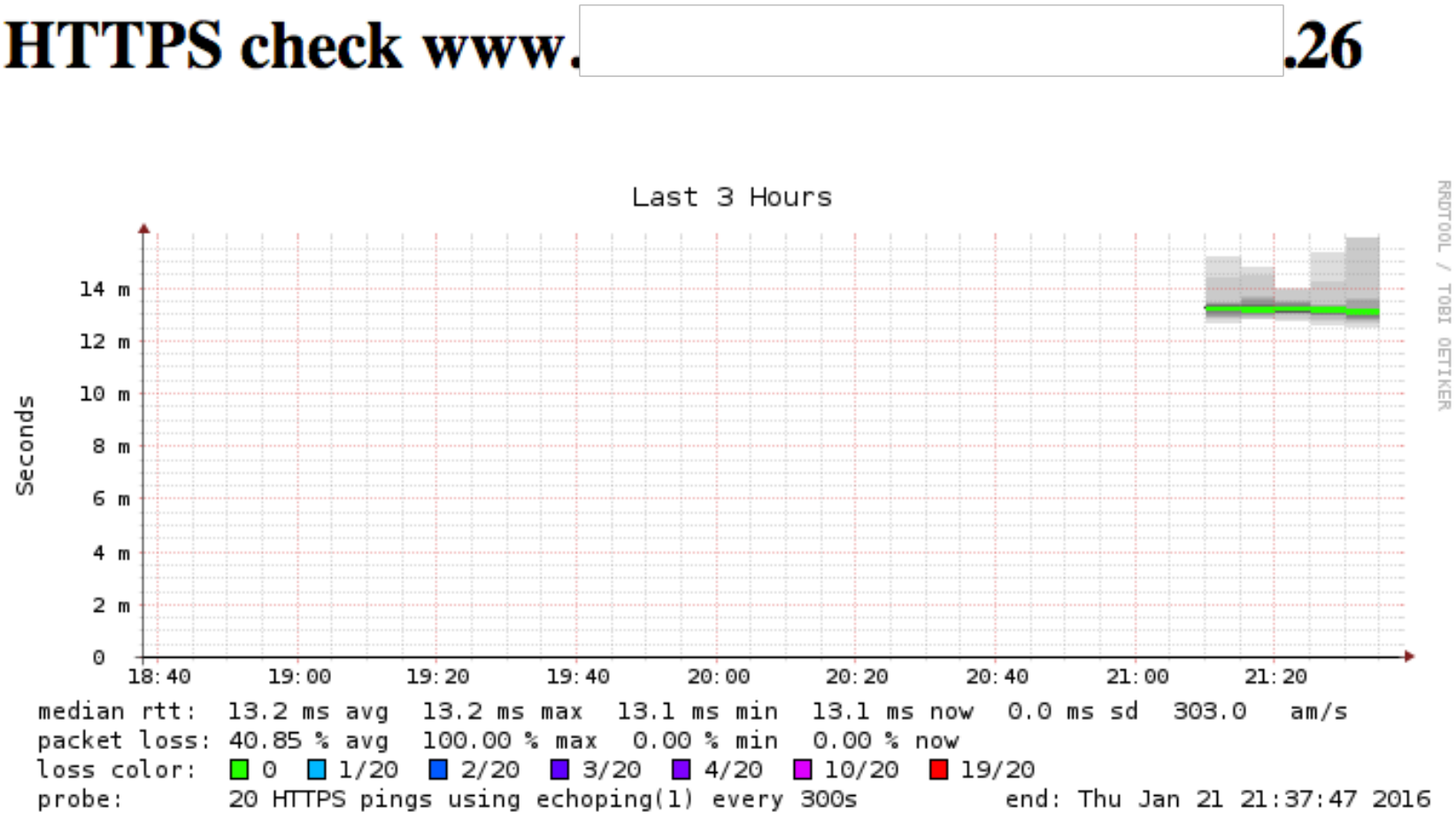
t50 packet generator

```
root@cornerstone03:~# t50 -?
T50 Experimental Mixed Packet Injector Tool 5.4.1
Originally created by Nelson Brito <nbrito@sekure.org>
Maintained by Fernando Mercês <fernando@mentebinaria.com.br>

Usage: T50 <host> [/CIDR] [options]

Common Options:
    --threshold NUM           Threshold of packets to send     (default 1000)
    --flood                   This option supersedes the 'threshold'
...
6. Running T50 with '--protocol T50' option, sends ALL protocols sequentially.
root@cornerstone03:~# t50 -? | wc -l
264
```

T50 packet generator, another high speed packet generator which can easily overload most firewalls by producing a randomized traffic with multiple protocols like IPsec, GRE, MIX

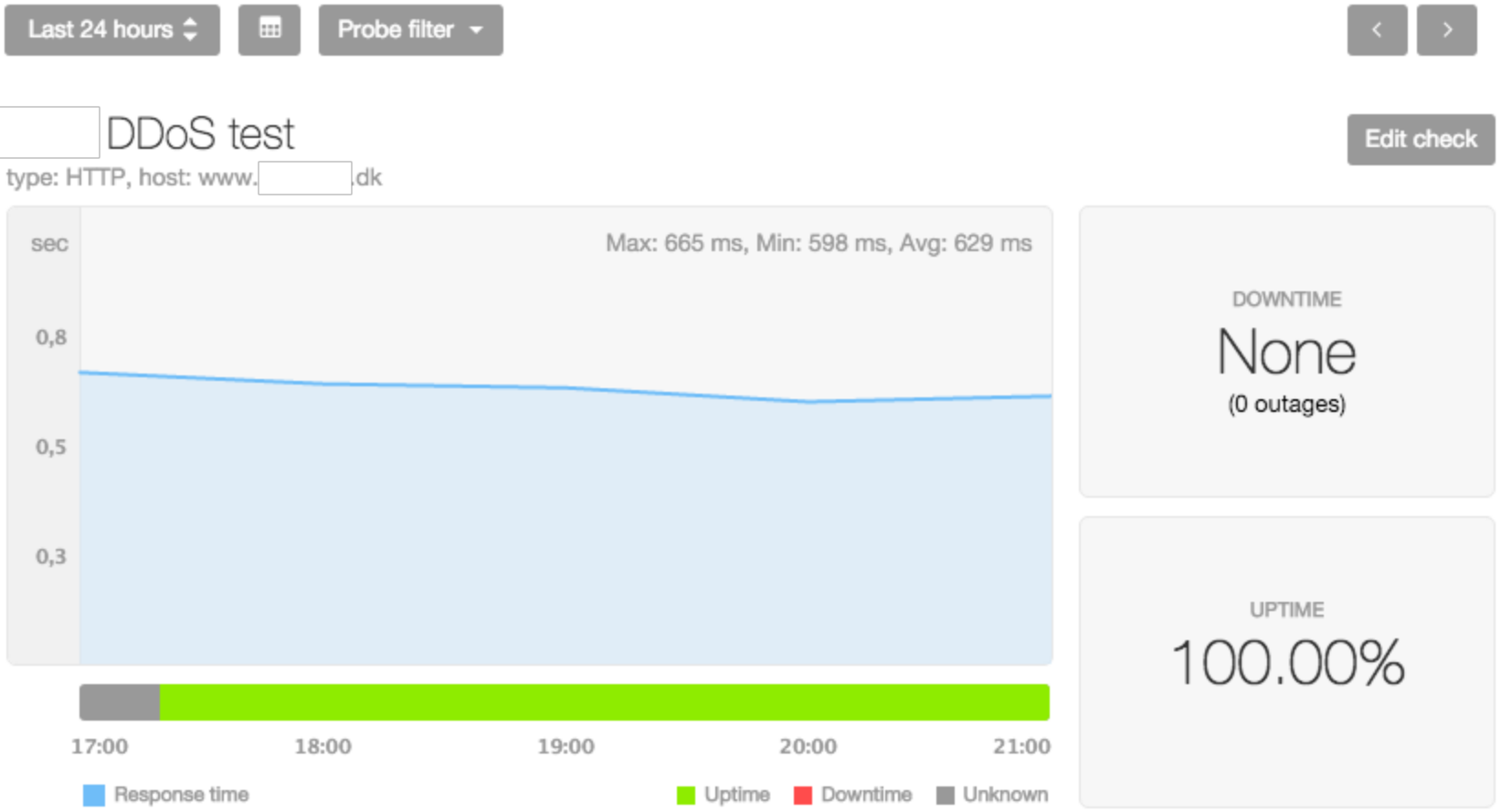
home page: `http://t50.sourceforge.net/resources.html`

Before testing: Smokeping



Before DDoS testing use Smokeping software

Before testing: Pingdom



Another external monitoring from Pingdom.com

Running the tools

A minimal test would be:

- TCP SYN flooding
- TCP other flags, PUSH-ACK, RST, ACK, FIN
- ICMP flooding
- UDP flooding
- Spoofed packets src=dst=target ☺
- Small fragments
- Bad fragment offset
- Bad checksum
- Be creative
- Mixed packets - like `t50 --protocol T50`
- Perhaps esoteric or unused protocols, GRE, IPSec

Process

- Start small, run with delays between packets
- Turn up until it breaks,
- Monitor speed of attack on your router interface pps/bandwidth
- Give it all shes got
  `hping3 --flood -1` and `hping3 --flood -2`

Comparable to real DDoS?

Tools are simple and widely available but are they actually producing same result as high-powered and advanced criminal botnets. We can confirm that the attack delivered in this test is, in fact, producing the traffic patterns very close to criminal attacks in real-life scenarios.

Running hping3

```
# export CUST_IP=192.0.2.1
# date;time hping3 -q -c 1000000  -i u60 -S -p 80  $CUST_IP


#  date;time hping3 -q -c 1000000  -i u60 -S -p 80  $CUST_IP
Thu Jan 21 22:37:06 CET 2016
HPING 192.0.2.1 (eth0 192.0.2.1): S set, 40 headers + 0 data bytes

--- 192.0.2.1 hping statistic ---
1000000 packets transmitted, 999996 packets received, 1% packet loss
round-trip min/avg/max = 0.9/7.0/1005.5 ms

real 1m7.438s
user 0m1.200s
sys 0m5.444s
```

Dont forget to do a killall hping3 when done ☺

Experiences from testing

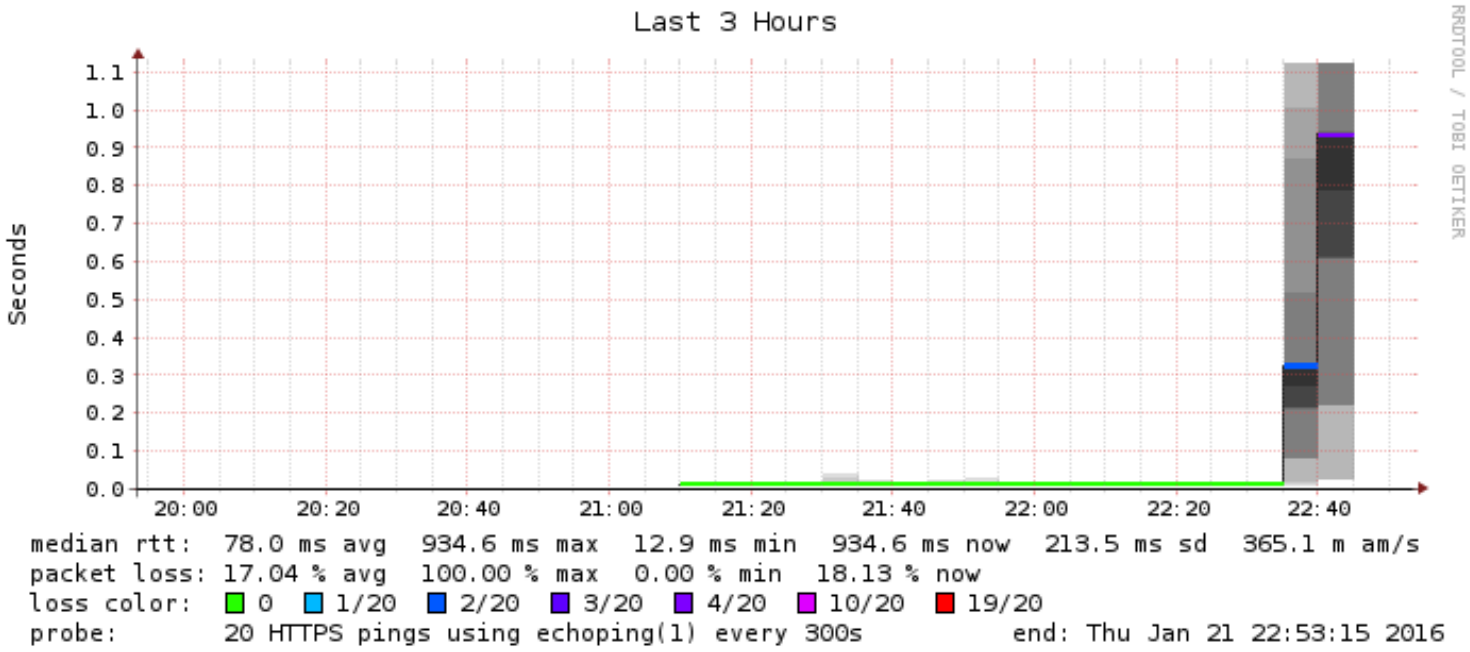
How much bandwidth can big danish companies handle?

- A) 10-100Mbps
- B) 100Mbps -1Gbit
- C) Up to 5Gbit easily

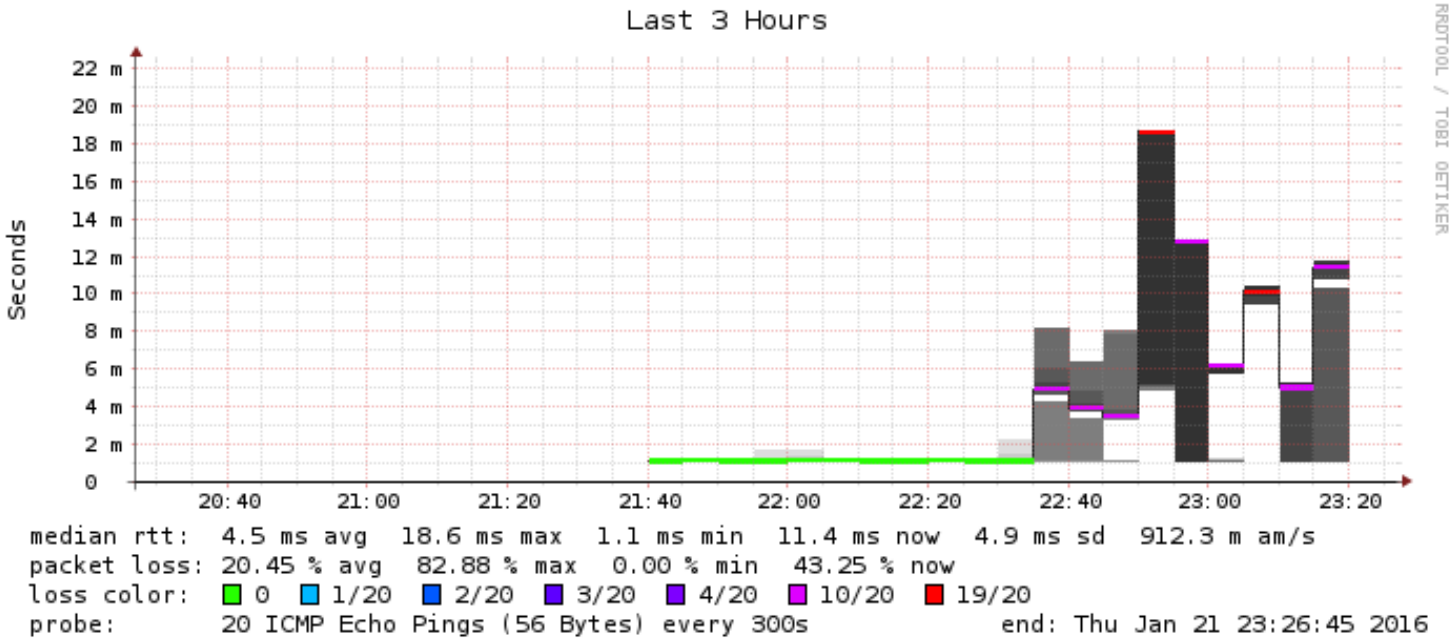
How much abuse in pps can big danish companies handle?

- A) 10.000 - 50.000 pps
- B) 50 - 500k pps
- C) Up to 5 million pps

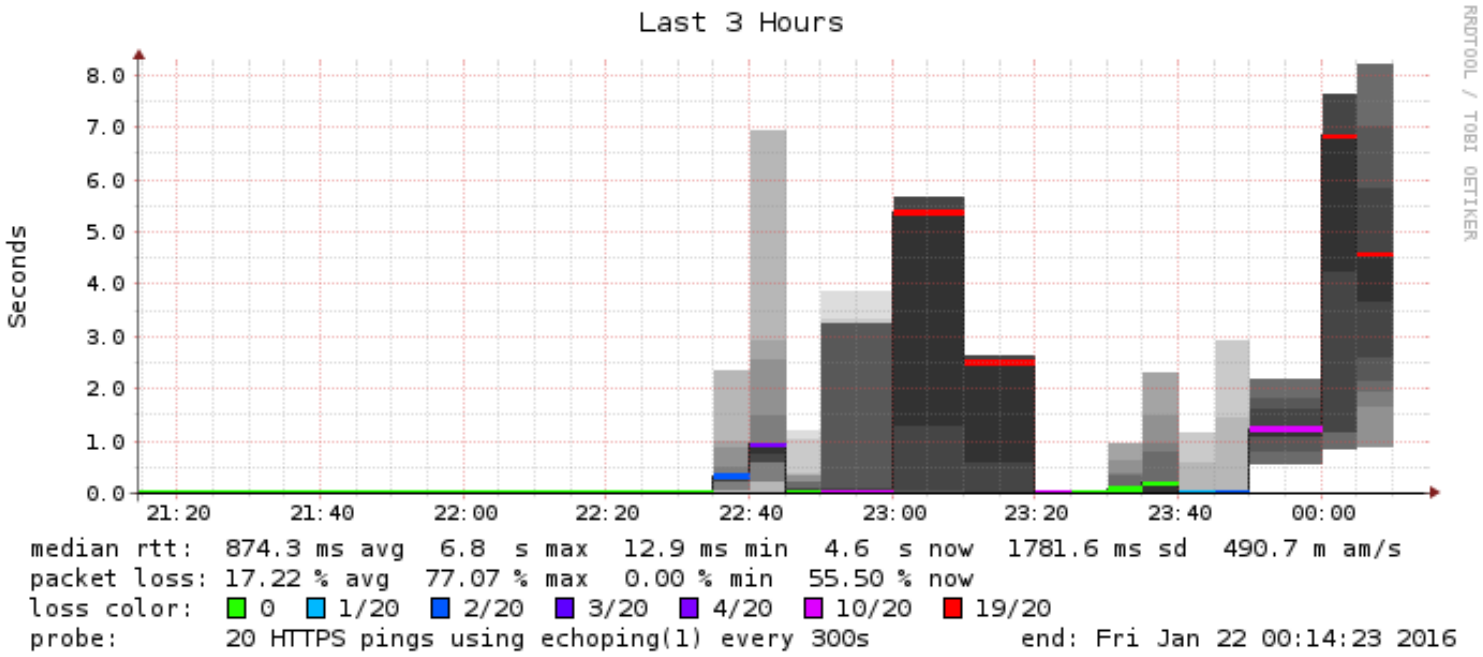
Rocky Horror Picture Show - 1



Rocky Horror Picture Show - 2



Rocky Horror Picture Show - 3



Experiences from testing

How much bandwidth can big danish companies handle!

- B) **100Mbps -1Gbit**

How much abuse in pps can big danish companies handle!

- B) **50 - 500k pps**

Even the DDoS protection services are a bit too small, can handle perhaps 10G?

and also multiple times admins lost access to network, VPN, log overflow etc.

Note: attackers can send full 10Gbit 14mill pps from Core i7 with 3 cores ...

Improvements seen after testing

Turning off unneeded features - free up resources

Tuning sesions, max sessions src / dst

Tuning firewalls, max sessions in half-open state, enabling services

Tuning network, drop spoofed src from inside net ☺

Tuning network, can follow logs, manage network during attacks

...

And organisation has better understanding of DDoS challenges

Including vendors, firewall consultants, ISPs etc.

After tuning of **existing devices/network** improves results 10-100 times

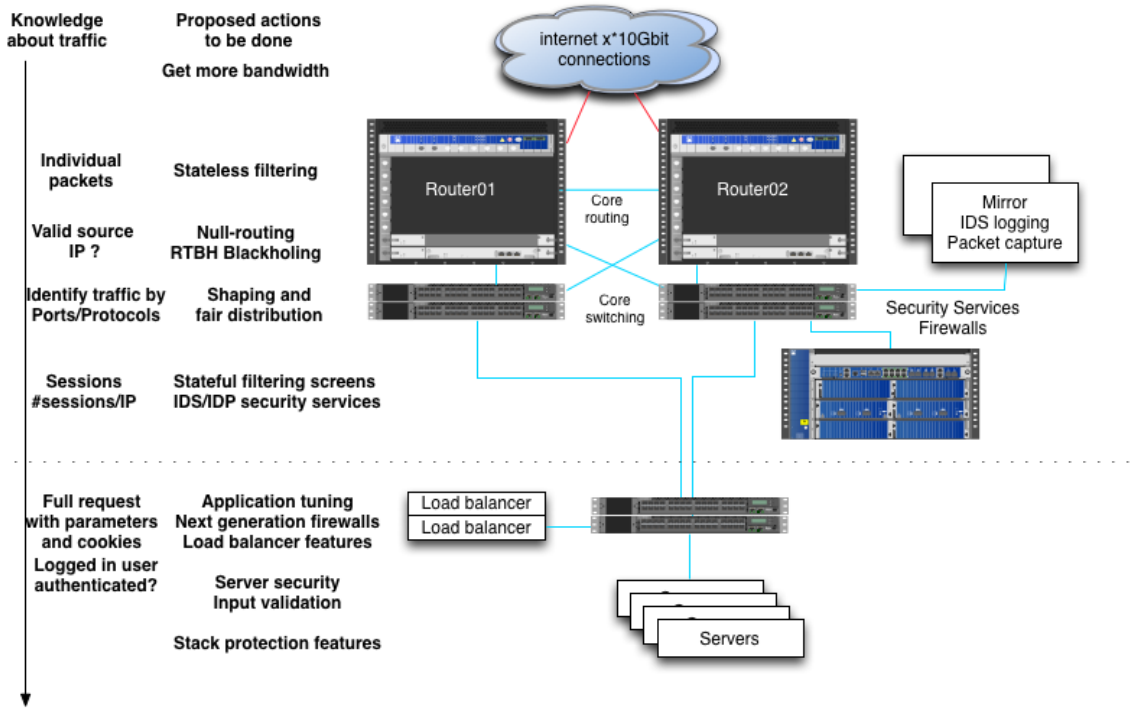
Conclusion

.

You really should try testing

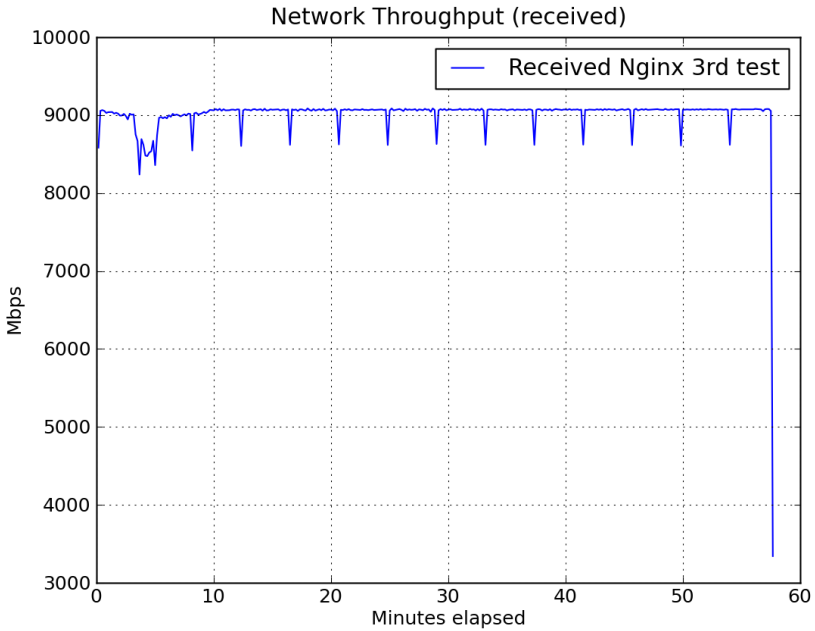
Investigate your existing devices
all of them, RTFM, upgrade firmware

Choose which devices does which part - discard early to free resources for later devices to dig deeper



And dont forget that DDoS testing is as much a firedrill for the organisation

More application testing



We covered only lower layers - but helpful layer 7 testing programs exist

Tsung can be used to stress HTTP, WebDAV, SOAP, PostgreSQL, MySQL, LDAP and Jabber/XMPP servers `http://tsung.erlang-projects.org/`

Questions?

Henrik Lund Kramshøj hlk@zencurity.dk

Need DDoS testing or pentest, ask me!

You are always welcome to send me questions later via email

Did you notice how a lot of the links in this presentation use HTTPS - encrypted