Welcome to

Simulated DDoS Attacks

breaking the firewall infrastructure

Henrik Lund Kramshøj hlk@zencurity.dk

Slides are available as PDF, kramshoej@Github

Contact information

- Henrik Lund Kramshøj, internet samurai mostly networks, infosec and
- Independent security consultant since January 2003
- Currently employed in a project with lots of health data
- Educated from the Computer Science Department at the University of Copenhagen, DIKU
- Email: hlk@zencurity.dk Mobile: +45 2026 6000

you are welcome to drop me an email afterwards

What is pentest

> A penetration test, informally pen test, is an attack on a computer system that looks for security weaknesses, potentially gaining access to the computer's features and data.[1][2]

Penetration testing is a simulation, with good intentions

People around the world constantly *test your defenses*

Often better to test at planned times

Source: qoute from `https://en.wikipedia.org/wiki/Penetration_test`

Goal

Don’t Panic!

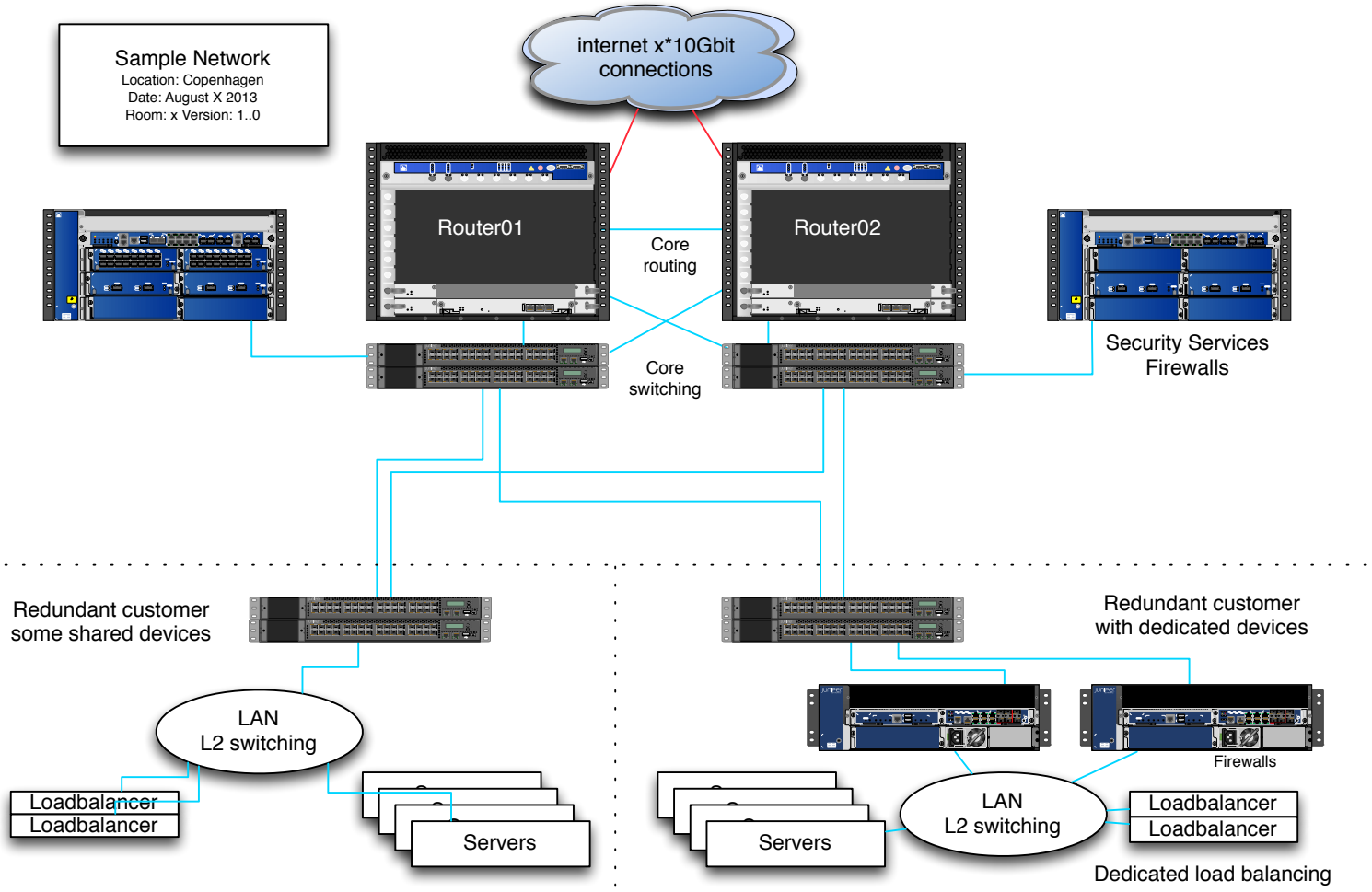
How to create DDoS simulations

Some actual experience with doing this

Evaluate how good is this, value

I use and recommend Kali 2.0 Linux as the base for this

Networks today



Kali Linux the new backtrack

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

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

Kali

Almost 200.000 youtube videos about ”kali hack”

You can learn these tools from their respective home pages:
Like `http://nmap.org`, `http://aircrack-ng.org`

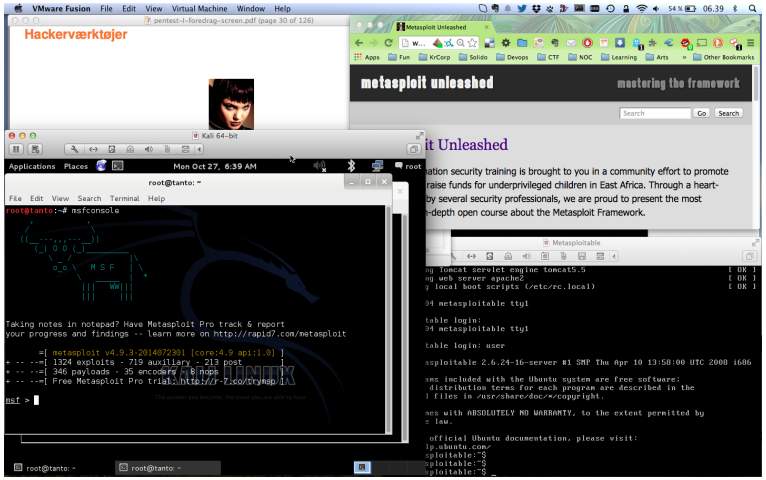
The main site helps with install and VM tools Kali `http://www.kali.org/`

Testing network the legal issues

Straffelovens paragraf 263 Stk. 2. Med bøde eller fængsel indtil 1 år og 6 måneder straffes den, der uberettiget skaffer sig adgang til en andens oplysninger eller programmer, der er bestemt til at bruges i et informationssystem.

- Danish law about hacking
- Please check with your legal department, or be careful
- We **always** contact network between us and the network to be tested
- Be good netizens

Hackerlab setup



- I recommend getting a hackerlab running on your laptop
- Hardware: modern laptop which has CPU virtualization
  Dont forget to check BIOS settings for virtualization
- Software: your favorite OS: Windows, Mac, Linux
- Virtualization software: VMware, Virtual box, HyperV
- Hacker software: Kali as a Virtual Machine `https://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`

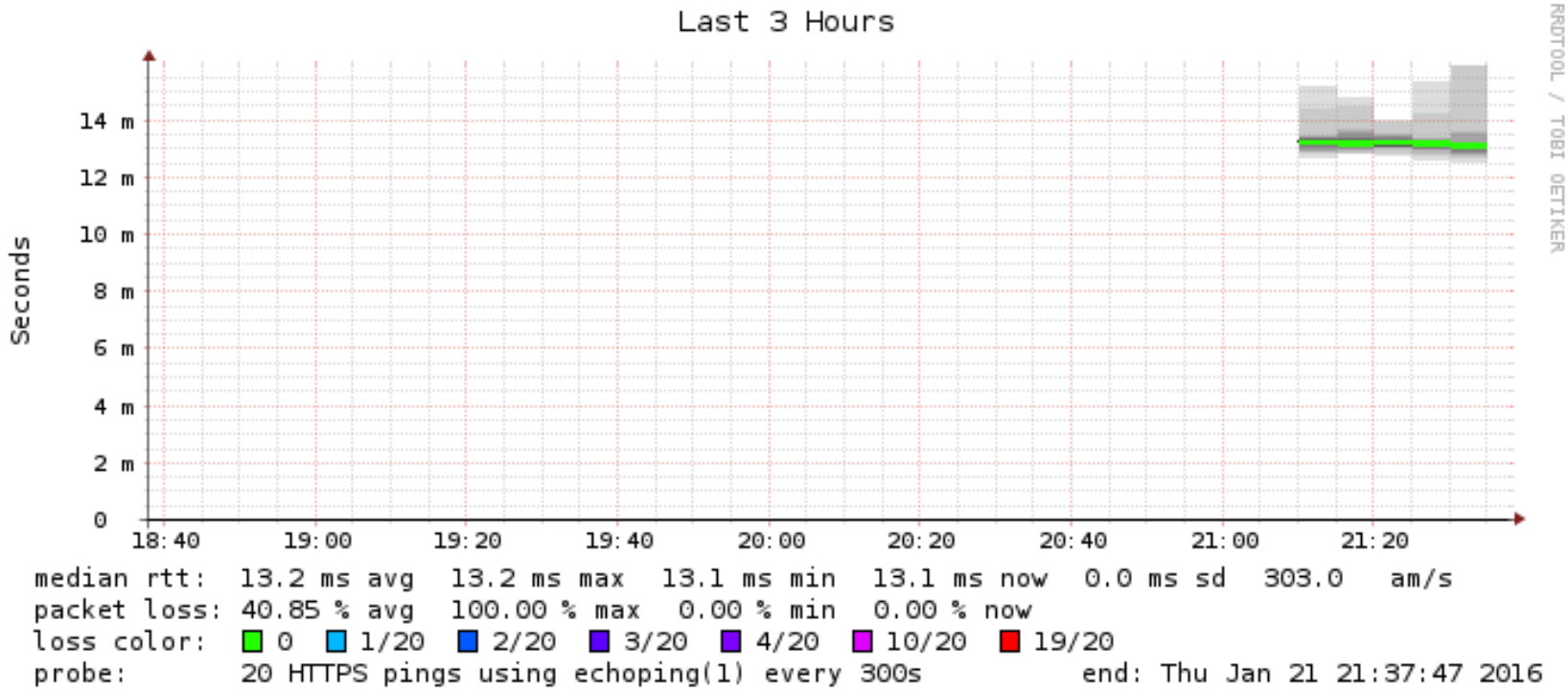
t50 packet generator

```
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 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`

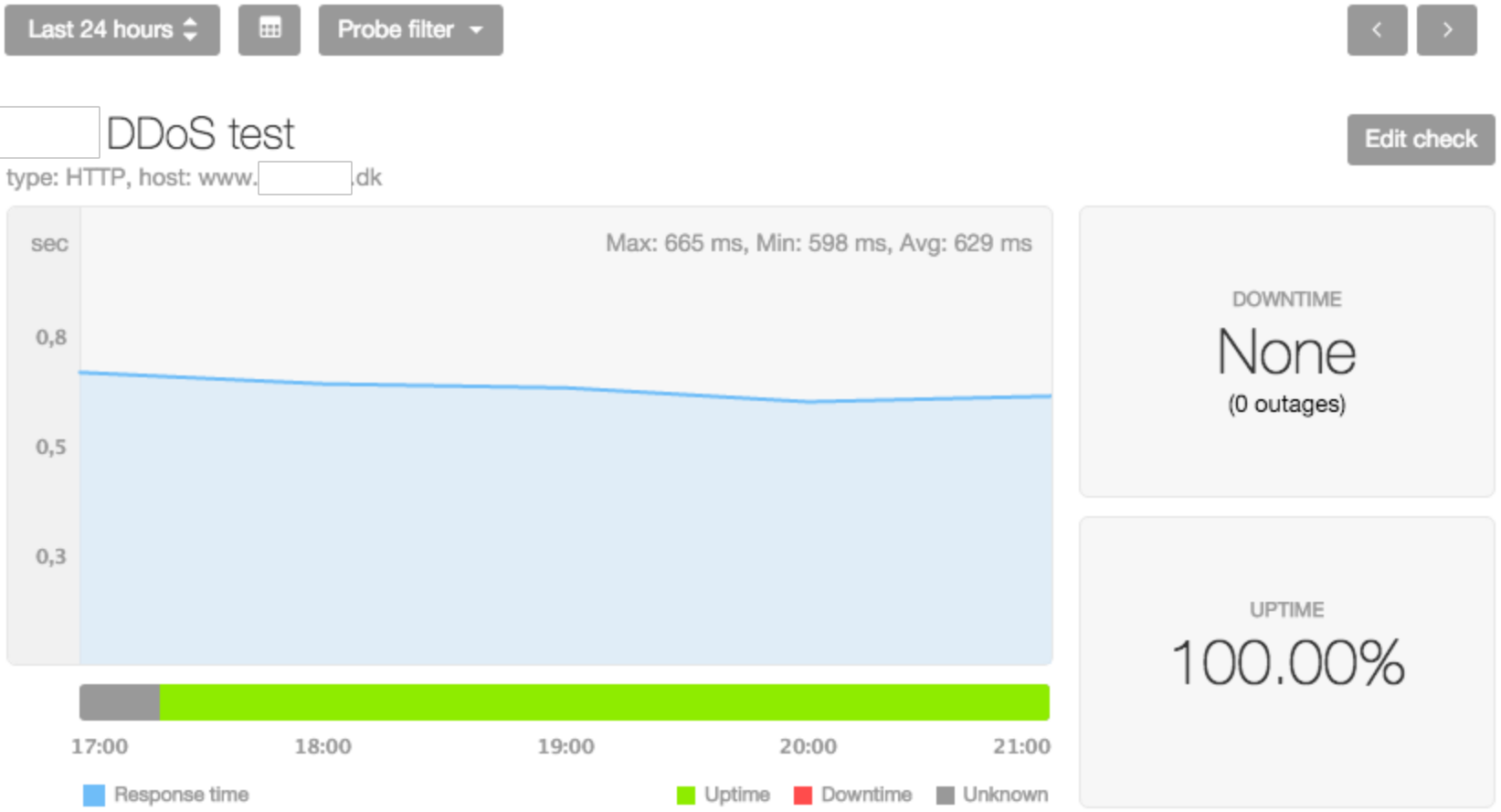
Before testing: Smokeping

HTTPS check www. .26



Before DDoS testing use Smokeping software

Before testing: Pingdom



Another external monitoring from Pingdom.com

Process: monitor, attack, break, repeat

- Monitoring setup - from multiple points
- 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
  `hping3 --flood -1` and `hping3 --flood -2`
- Have a common chat with network operators/customer to talk about symptoms and things observed
- Any information resulting from testing is good information

Ohh we lost our VPN into the environment, ohh the fw console is dead

Running Attacks with 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 ☺

Recommendations During Test

Run each test for at least 5 minutes, or even 15 minutes
Some attacks require some build-up before resource run out

Take note of any change in response, higher latency, lost probes

If you see a change, then re-test using the same parameters, or a little less first

We want to know the approximate level where it breaks

If you want to change environment, then wait until all scenarios tested

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.

- We can also monitor logs when running a single test-case
- Gain knowledge about supporting infrastructure
- Can your syslog infrastructure handle 800.000 events in $<$ 1 hour?

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

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

Test-cases / Scenarios

The minimal run contains at least these:

- SYN flood: `hping3 -q -c 1000000 -i u60 -S -p 80 $CUST_IP &`
- SYN+ACK: `hping3 -q -c 1000000 -i u60 -S -A -p 80 $CUST_IP &`
- ICMP flood: `hping3 -q -c --flood -1 $CUST_IP &`
- UDP flood: `hping3 -q -c --flood -1 $CUST_IP &`

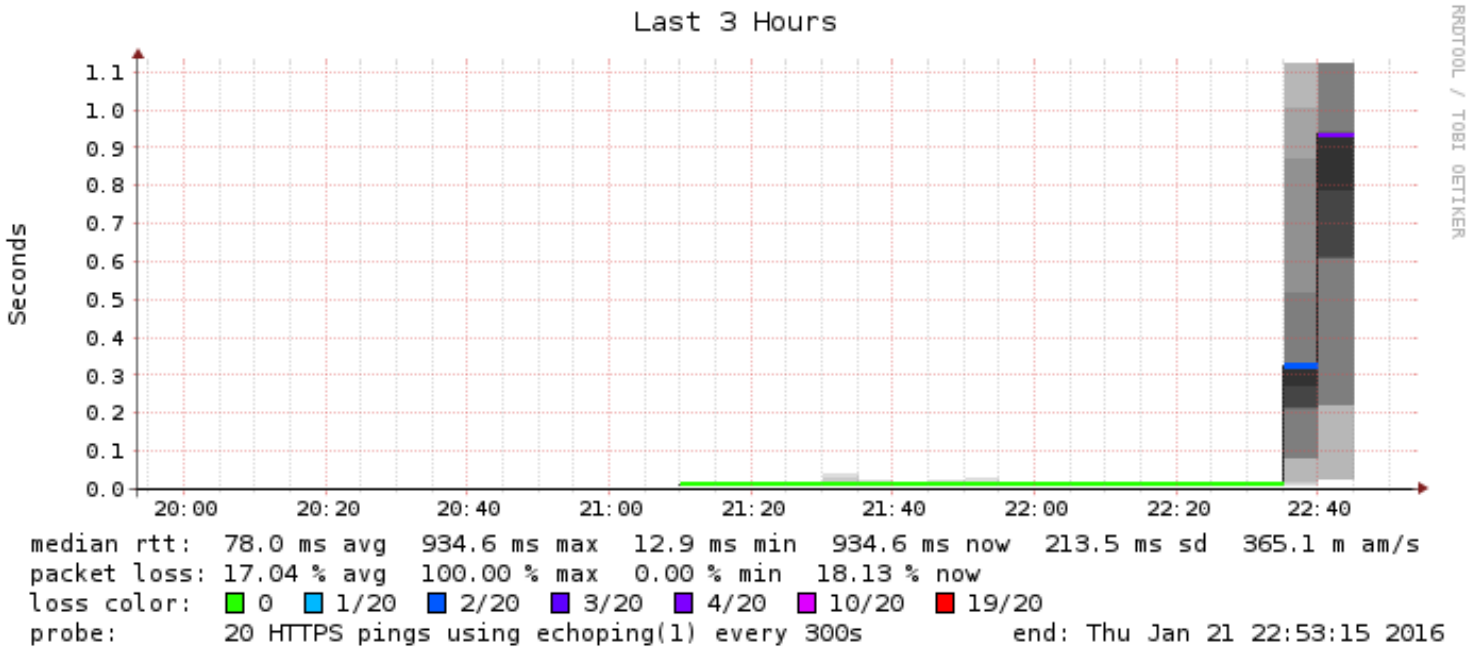
Vary the speed using the packet interval `-i u60` up/down

Use –flood with caution, max speeeeeeeeeeeed ☺

TCP testing use a port which is allowed through the network, often 80/443

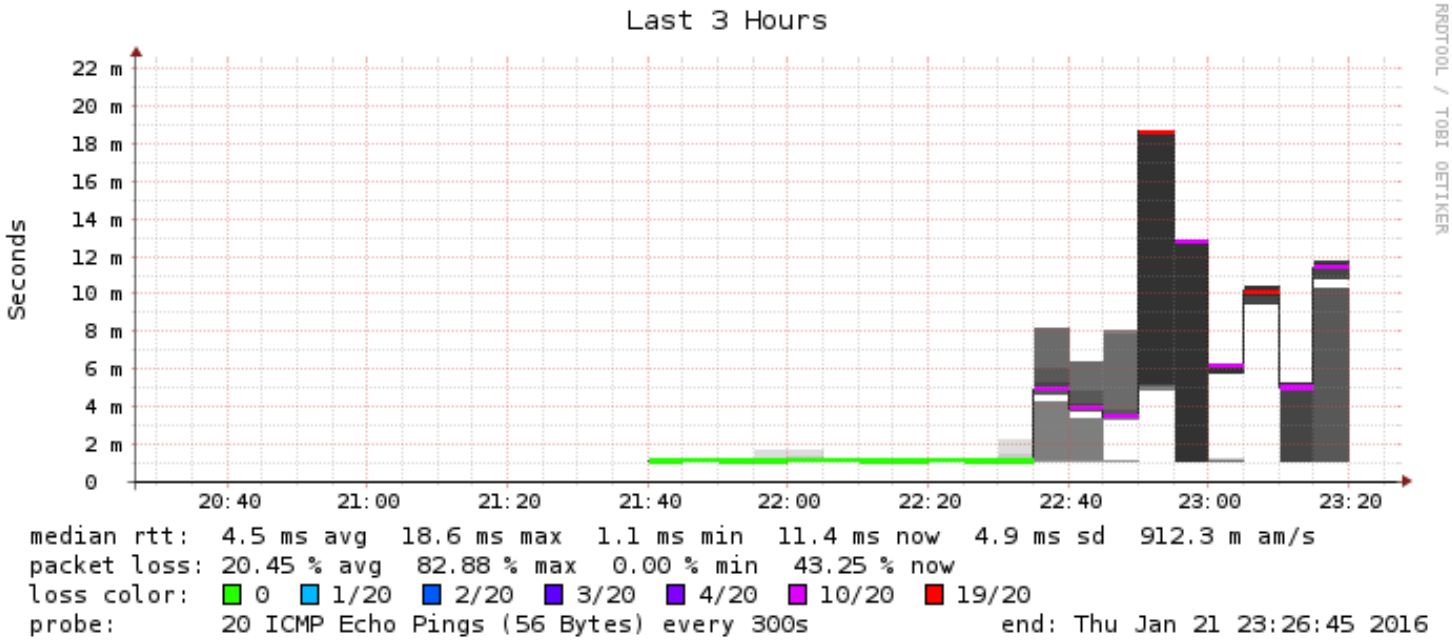
Focus on attacks which are hard to block, example TCP SYN must be allowed in

Rocky Horror Picture Show - 1



Really does it break from 50.000 pps SYN attack?

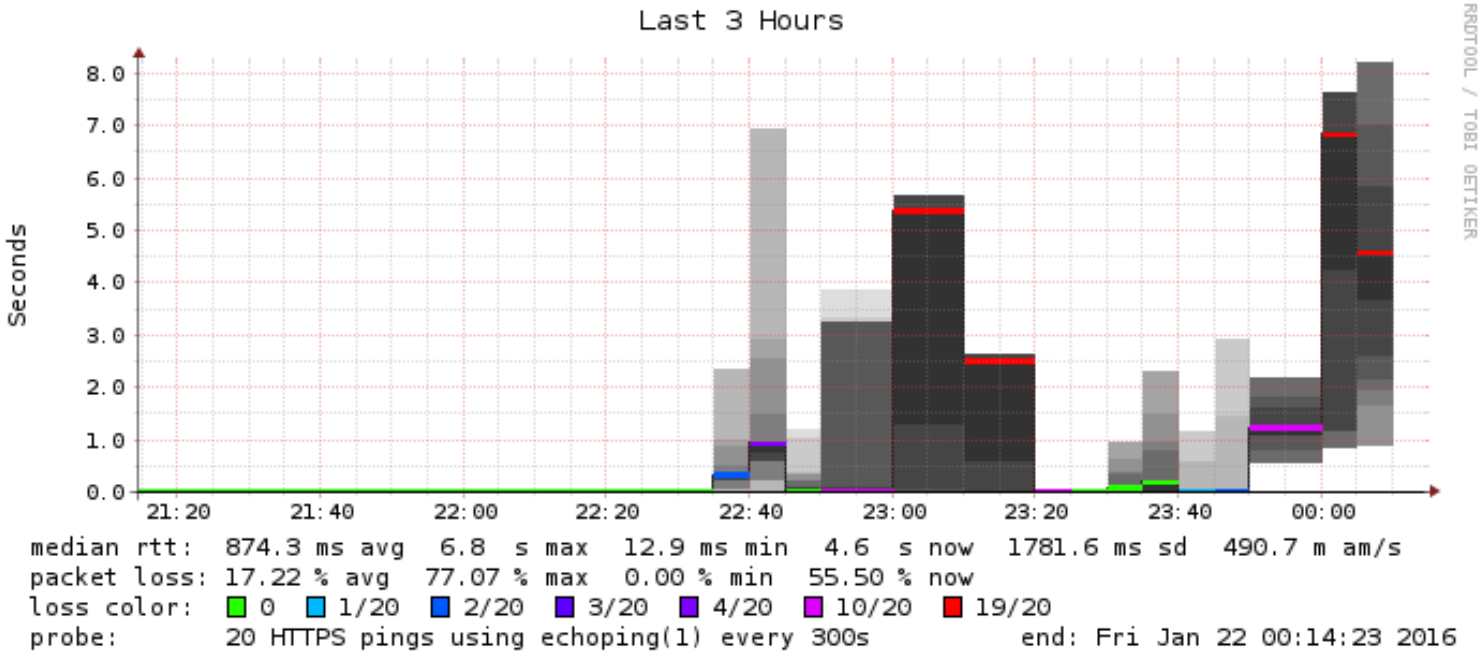
Rocky Horror Picture Show - 2



Oh no 500.000 pps UDP attacks work?

Rocky Horror Picture Show - 3

Oh no spoofing attacks work?



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) **50.000 - 500k pps** TCP attacks
- B) **500.000 - 1mill pps** UDP or ICMP attacks
- Ohhh and often we can spoof using their addresses in the first test

Even the DDoS protection services are a bit too small, can handle perhaps only 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

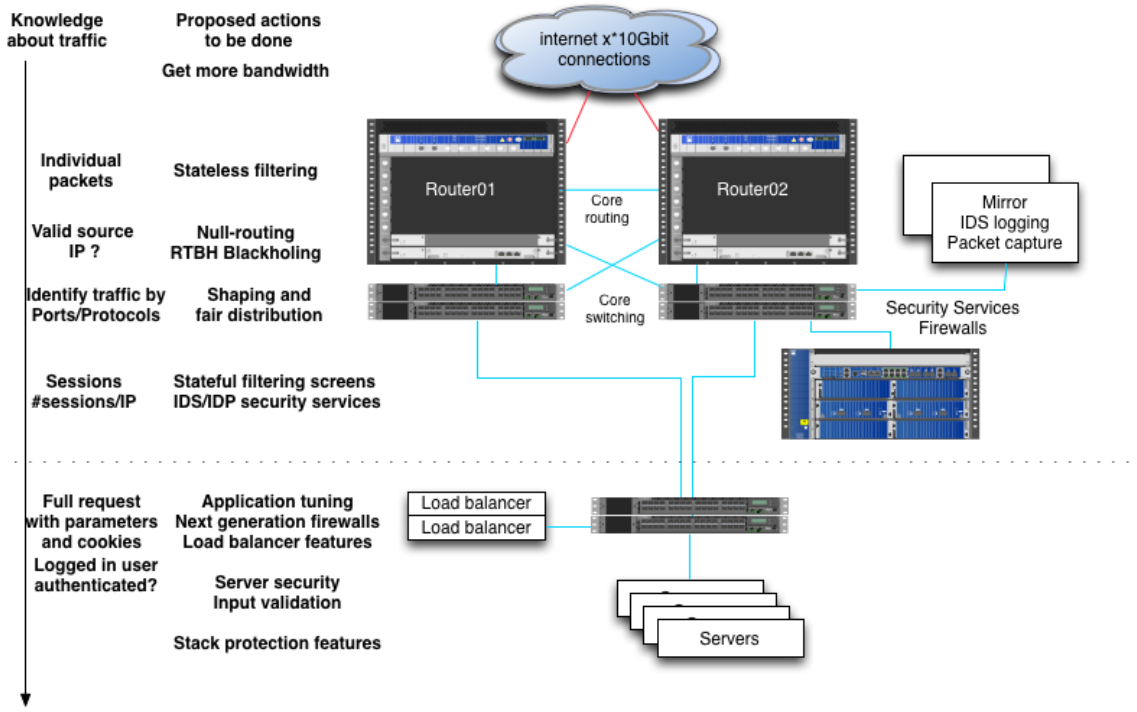
Conclusion

.

You really should try testing

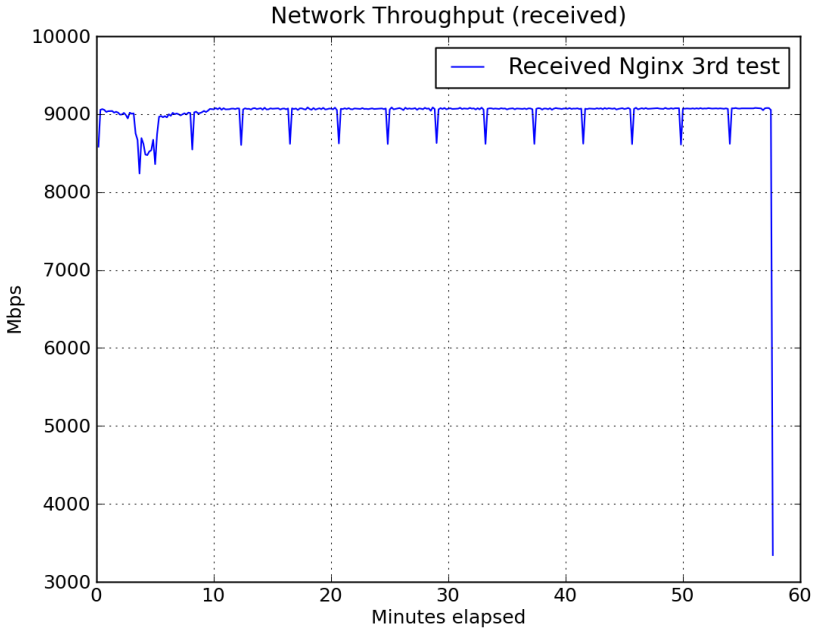
Investigate your existing devices
all of them, RTFM, upgrade firmware

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

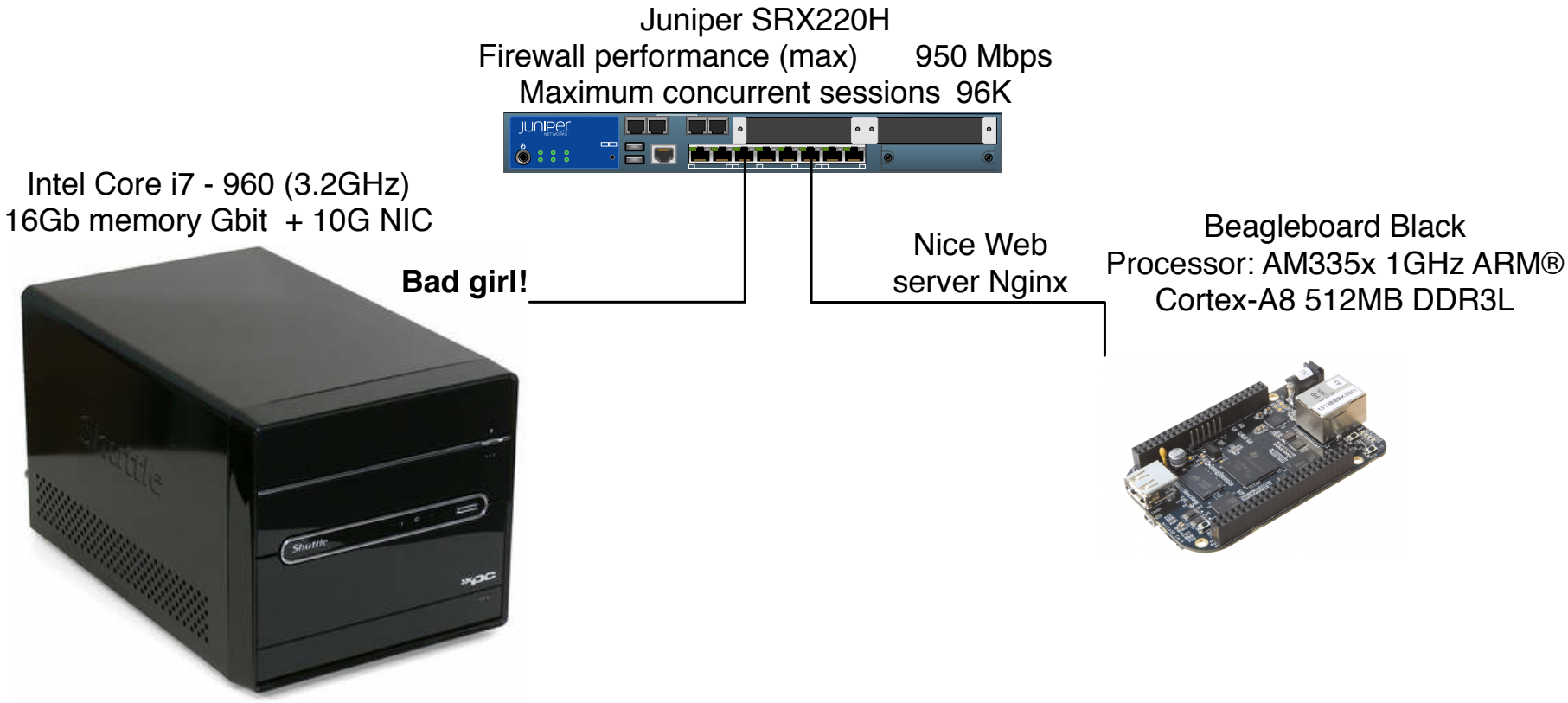
Need DDoS testing or pentest, ask me!

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

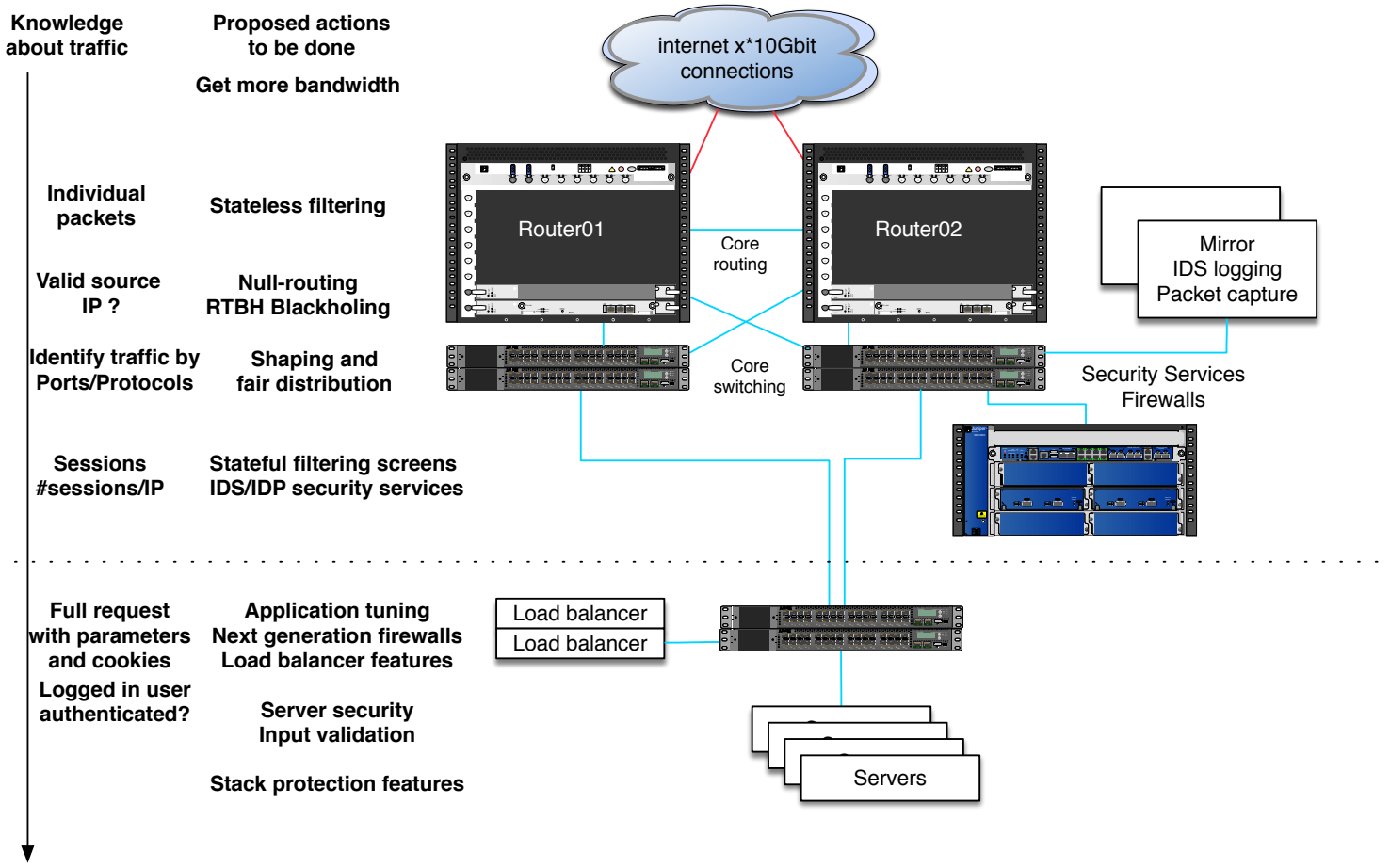
Extras if needed or questions arise

Demo network



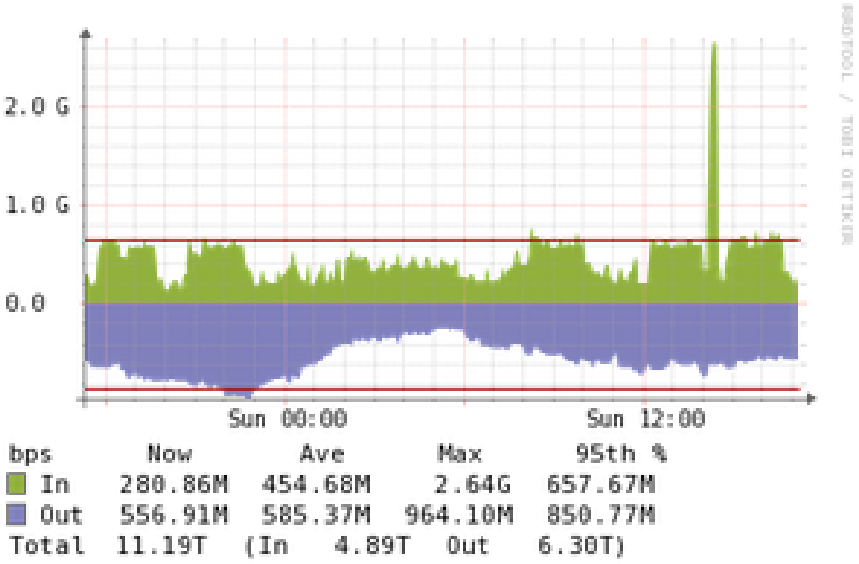
I use this when doing on-site demos

Defense in depth - multiple layers of security



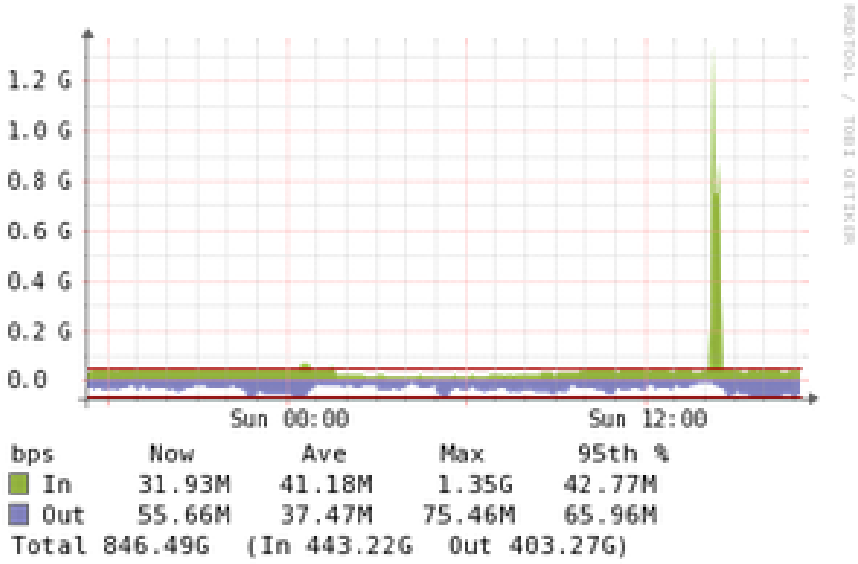
DDoS traffic before filtering

Level3 CPH



bps	Now	Ave	Max	95th %
In	280.86M	454.68M	2.64G	657.67M
Out	556.91M	585.37M	964.10M	850.77M
Total	11.19T	(In 4.89T	Out 6.30T)	

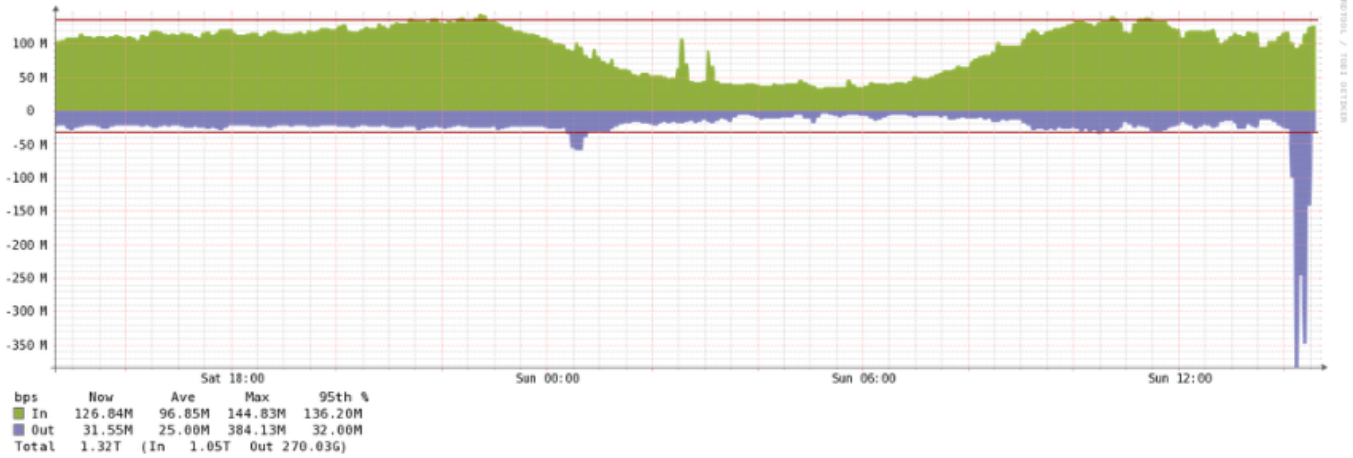
NGDC



bps	Now	Ave	Max	95th %
In	31.93M	41.18M	1.35G	42.77M
Out	55.66M	37.47M	75.46M	65.96M
Total	846.49G	(In 443.22G	Out 403.27G)	

Only two links shown, at least 3Gbit incoming for this single IP

DDoS traffic after filtering



Link toward server (next level firewall actually) about 350Mbit outgoing

Stateless firewall filter throw stuff away

```
hlk@MX-CPH-02> show configuration firewall filter all | no-more
/* This is a static sample, perhaps better to use BGP flowspec and RTBH */
term edgeblocker {
    from {
        source-address {
            84.180.xxx.173/32;
...
            87.245.xxx.171/32;
        }
        destination-address {
            91.102.91.16/28;
        }
        protocol [ tcp udp icmp ];
    }
    then {
        count edge-block;
        discard;
    }
}
```

Hint: can also leave out protocol and then it will match all protocols

Stateless firewall filter limit protocols

```
term limit-icmp {
    from {
        protocol icmp;
    }
    then {
        policer ICMP-100M;
        accept;
    }
}
term limit-udp {
    from {
        protocol udp;
    }
    then {
        policer UDP-1000M;
        accept;
    }
}
```

Routers have extensive Class-of-Service (CoS) tools today

Strict filtering for some servers, still stateless!

```
term some-server-allow {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol tcp;
        destination-port [ 80 443 ];
    }
    then accept;
}
term some-server-block-unneeded {
    from {
        destination-address {
            109.238.xx.0/xx;
        }
        protocol-except icmp;
    }
    then {
        discard;
    }
}
```

Wut - no UDP, yes UDP service is not used on these servers

Firewalls - screens, IDS like features

When you know regular traffic you can decide:

```
hlk@srx-kas-05# show security screen ids-option untrust-screen
icmp {
    ping-death;
}
ip {
    source-route-option;
    tear-drop;
}
tcp {    Note: UDP flood setting also exist
    syn-flood {
        alarm-threshold 1024;
        attack-threshold 200;
        source-threshold 1024;
        destination-threshold 2048;
        timeout 20;
    }
    land;
}
```

Always select your own settings YMMV