How to Ruin Your Weekend (and your Business) in few simple steps

PRZEMEK JAROSZEWSKI
CERT POLSKA / NASK

29. ANNUAL FIRST CONFERENCE. SAN JUAN, PUERTO RICO. JUNE 14, 2017

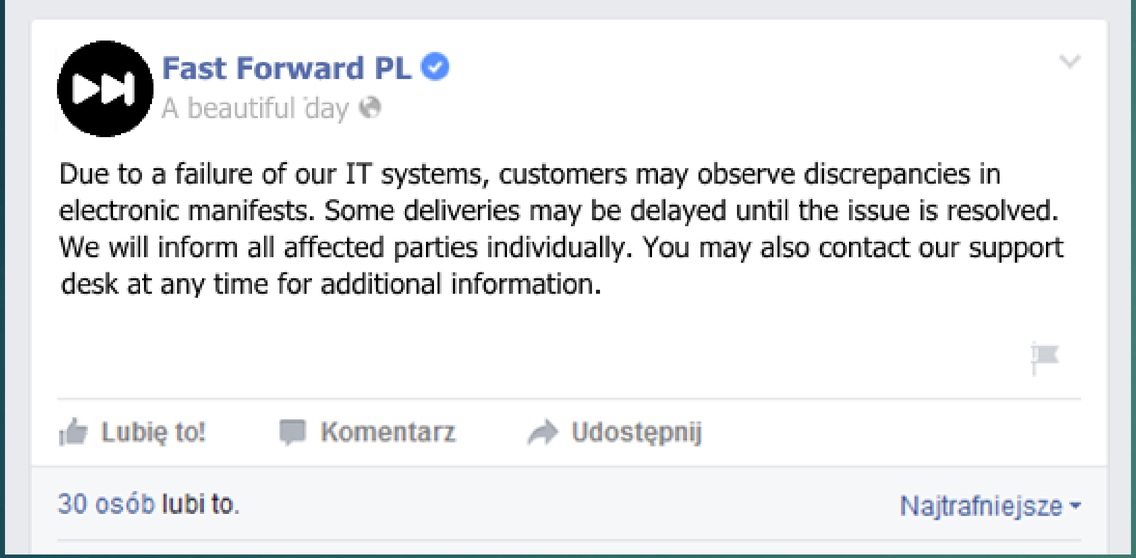
CERT.PL>_

Chapter I

Fast Forward

- FAST FORWARD is a logistic company that handles many types of shipments, such as:
  - Food supplies (HORECA)
  - Medical (Pharmacies and Hospitals)
  - Documents (Legal and Consulting)

A lazy Sunday afternoon in summer

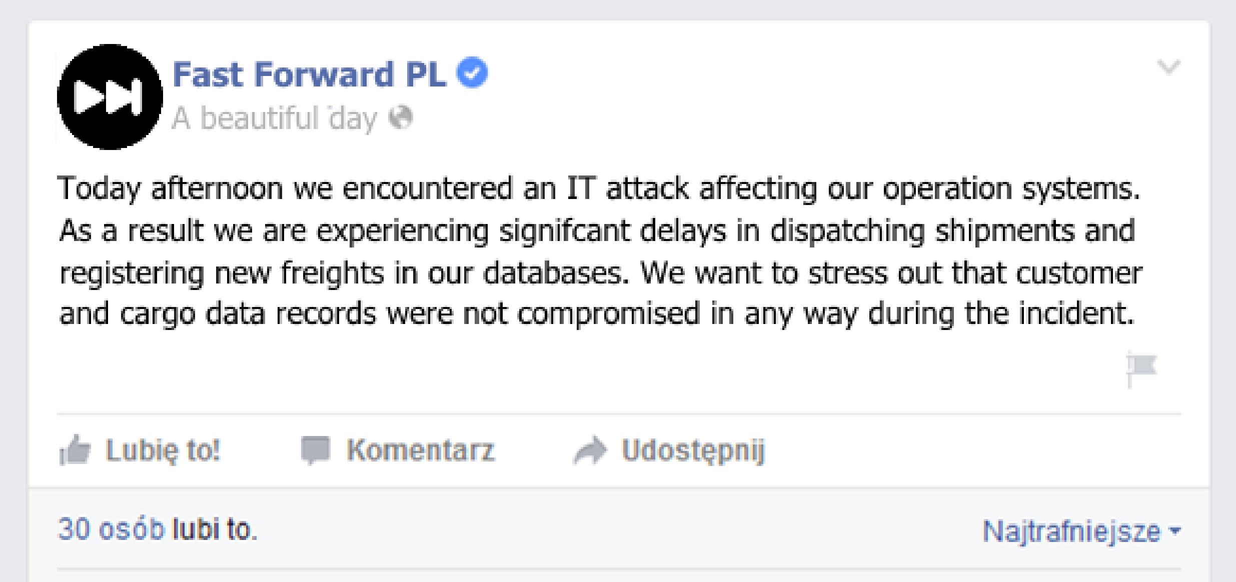


Fast Forward PL ✓

A beautiful day

Due to a failure of our IT systems, customers may observe discrepancies in electronic manifests. Some deliveries may be delayed until the issue is resolved. We will inform all affected parties individually. You may also contact our support desk at any time for additional information.

3 hours later…



Fast Forward PL ✓

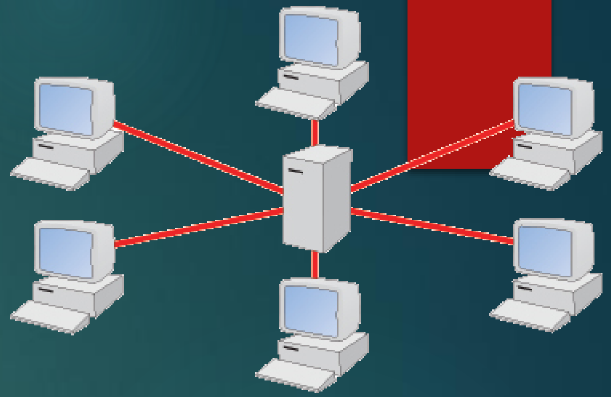
A beautiful day

Today afternoon we encountered an IT attack affecting our operation systems. As a result we are experiencing signifcant delays in dispatching shipments and registering new freights in our databases. We want to stress out that customer and cargo data records were not compromised in any way during the incident.

What was officially ”known”

- Attacks disrupted IT systems used for planning and delivery of manifests to central databse
- Other systems were not affected
- Attacks ”blocked Fast Forward’s network”. In effect, manifests could not be submitted to coordination office and shipment plans were not generated.
- The incident was mitigated within twenty-four hours.
- 200+ businesses were affected, understocked or unable to provide daily operations

Fast Forward operations

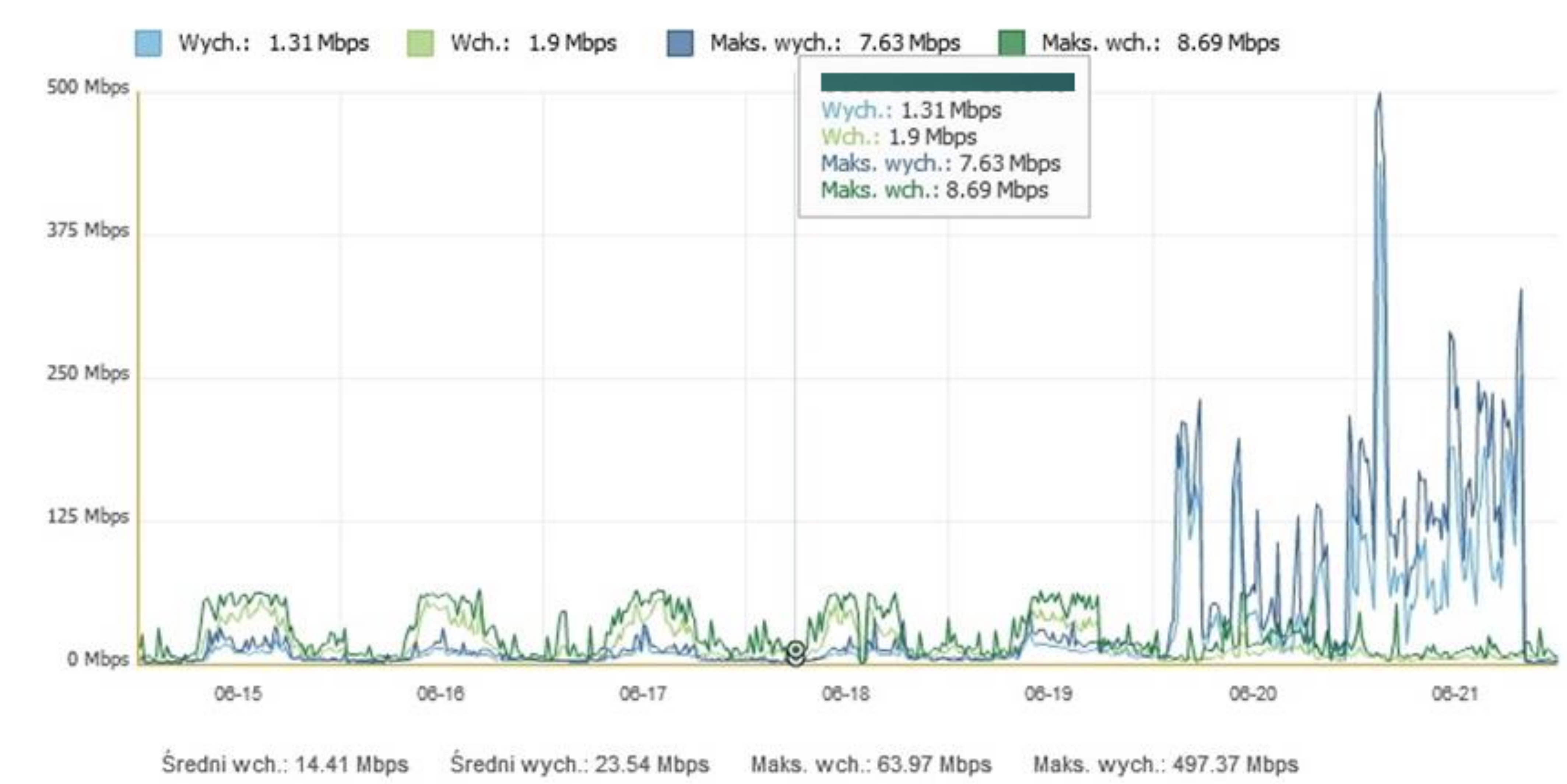


- Each regional office submits tickets based on customer schedules and individual orders
  - To a dedicated server application via WEB API
  - Over VPN (gateway at the central office)
- Shipments are bundled and coordinated at the central office within certain constraints, based on:
  - Availability of supplies at different locations
  - Route optimization
  - Time efficiency
- Plans are sent to local offices which dispatch vehicles to collect and deliver shipments

Chapter II

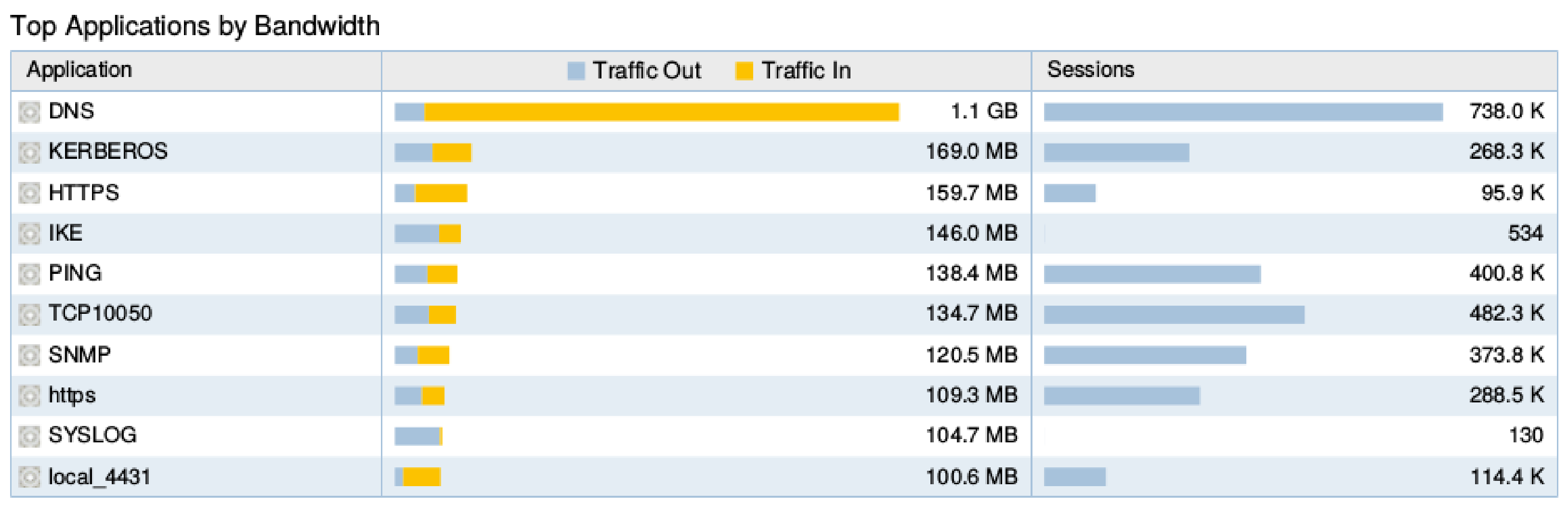
The story unfolds…

- Fast Forward was in the process of migration of its firewalls (from different vendor).
- Volume of traffic to ISPs was increasing within days after the new firewall was in production environment.
- Day -1. The network is congested. This is addressed by filtering a number of ”attacking” hosts on the firewall.
- Day 0. The network becomes unresponsive.
- Day 1. Old firewalls are restored which resolves the problem.


Wych.: 1.31 Mbps
Wch.: 1.9 Mbps
Maks. wych.: 7.63 Mbps
Maks. wch.: 8.69 Mbps
Wych.: 1.31 Mbps
Wch.: 1.9 Mbps
Maks. wych.: 7.63 Mbps
Maks. wch.: 8.69 Mbps
500 Mbps
375 Mbps
250 Mbps
125 Mbps
0 Mbps
06-15
06-16
06-17
06-18
06-19
06-20
06-21
Średni wch.: 14.41 Mbps
Średni wych.: 23.54 Mbps
Maks. wch.: 63.97 Mbps
Maks. wych.: 497.37 Mbps

The Firewall

- Logs are not much help ☹
  - Logging was initially disabled for most rules.
  - Storage space not correctly configured on the analyzer.
  - We had about 7 minutes of logs.
- Summary reports show that most traffic was outgoing DNS via UDP.

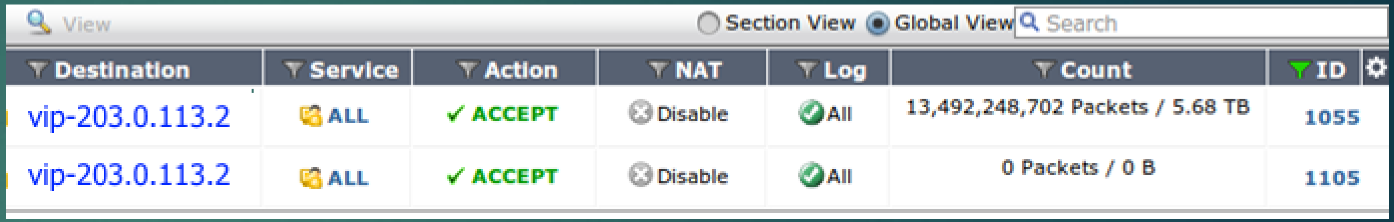


Top Applications by Bandwidth

Application	🟦 Traffic Out 🟨 Traffic In	Sessions
DNS	1.1 GB	738.0 K
KERBEROS	169.0 MB	268.3 K
HTTPS	159.7 MB	95.9 K
IKE	146.0 MB	534
PING	138.4 MB	400.8 K
TCP10050	134.7 MB	482.3 K
SNMP	120.5 MB	373.8 K
https	109.3 MB	288.5 K
SYSLOG	104.7 MB	130
local_4431	100.6 MB	114.4 K

Let’s go deeper…

- FortiGate has rule counters



Destination	Service	Action	NAT	Log	Count	ID
vip-203.0.113.2	ALL	✓ ACCEPT	Disable	All	13,492,248,702 Packets / 5.68 TB	1055
vip-203.0.113.2	ALL	✓ ACCEPT	Disable	All	0 Packets / 0 B	1105

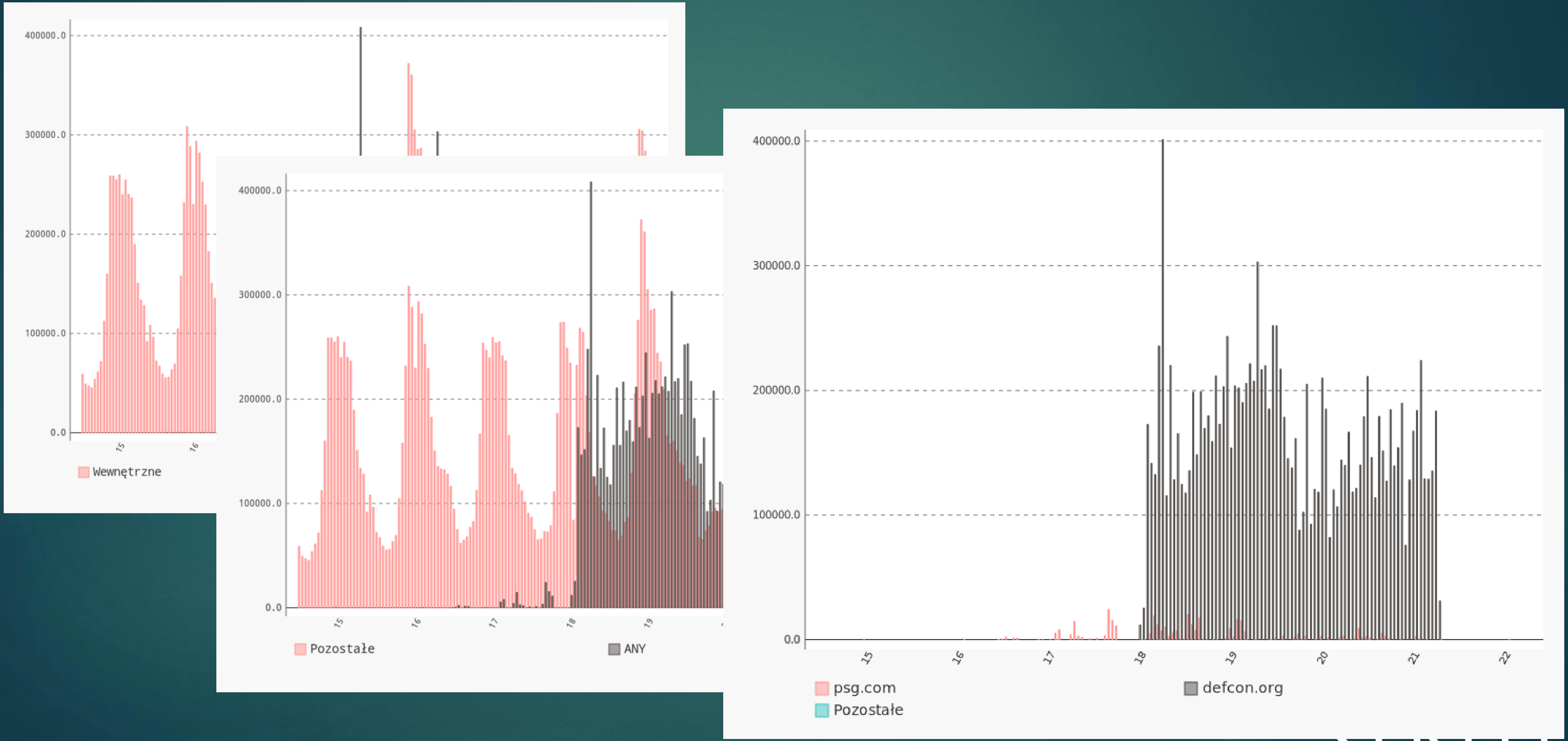
```
config firewall vip
          edit "vip-203.0.113.2"
          set uuid 3034c832-e61a-51b4-a925-f4fe0e4d3728
          set extip 203.0.113.2
          set extintf "any"
          set mappedip "10.23.80.9"
          next
end

config firewall policy
          edit 1055
          set uuid def93232-fa43-91e4-40a6-a6ee99322b5a
          set srcintf "any"
          set dstintf "any"
          set srcaddr "all"
          set dstaddr "vip-203.0.113.2"
          set action accept
          set schedule "always"
          set service "ALL"
          set logtraffic disable
          next
```

What is 203.0.113.2?

- ”Good question! We’re not quite sure.”
- mercury.fastforward.pl – used to be an all-purpose server ”back in the old days”, handling mail, DNS, etc.
- For legacy reasons the original firewall translated its address to the internal DNS server, but **only for DNS traffic from internal networks and VPNs**.
- The ”rule 1055” was apparently a mistranslation…

Let’s look at DNS server logs



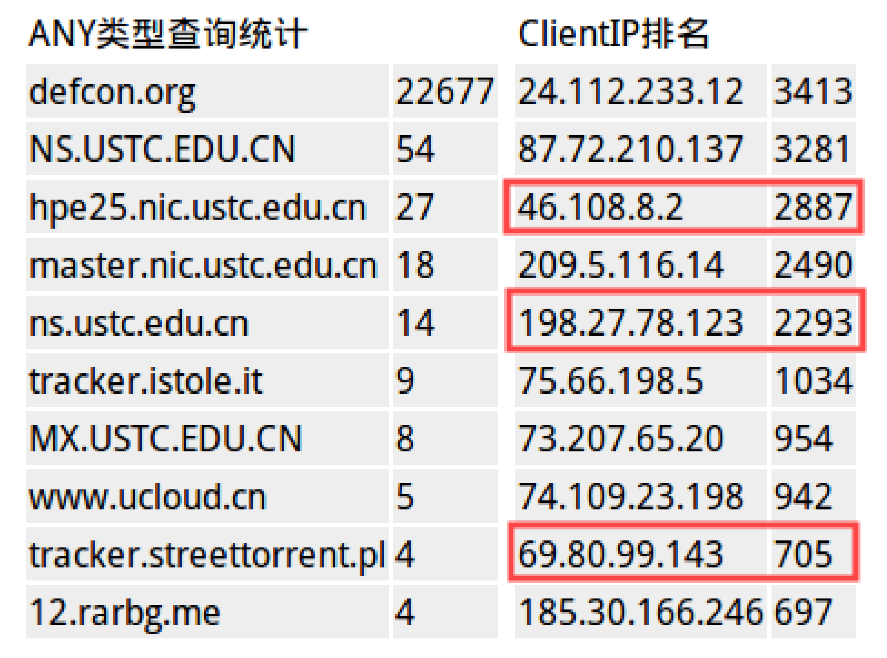
Wrap up (for now)

- Confirmed that DNS amplification killed the network.
- DNS amplification was done on an internal DNS server, never meant to speak to the world.
- The mistranslated rule was not picked up by tests.
  - It was the fourth attempt to push to production.
  - Everyone was focused on getting the traffic they want through. (Not on checking whether new holes are opened).
  - Full tests, tweaks like traffic shaping etc. were scheduled for later.
- Switching back to the old firewall was accepted as solution.

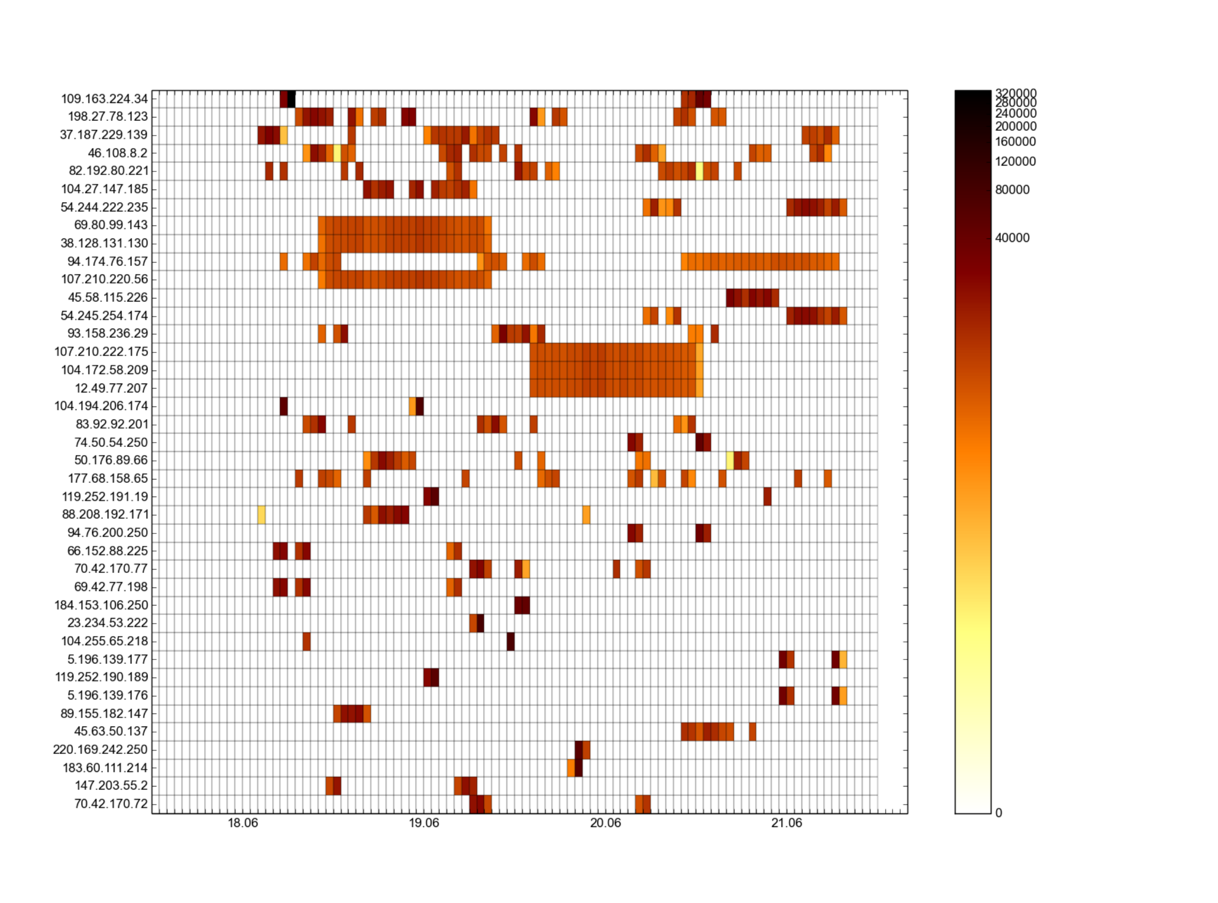
Chapter III

Let’s go even deeper…

- Was Fast Forward targeted? Likely not.



ANY类型查询统计		ClientIP排名	
defcon.org	22677	24.112.233.12	3413
NS.USTC.EDU.CN	54	87.72.210.137	3281
hpe25.nic.ustc.edu.cn	27	46.108.8.2	2887
master.nic.ustc.edu.cn	18	209.5.116.14	2490
ns.ustc.edu.cn	14	198.27.78.123	2293
tracker.istole.it	9	75.66.198.5	1034
MX.USTC.EDU.CN	8	73.207.65.20	954
www.ucloud.cn	5	74.109.23.198	942
tracker.streettorrent.pl	4	69.80.99.143	705
12.rarbg.me	4	185.30.166.246	697



How could this be prevented?

the less obvious observations

- A cheap laptop with a 3G modem would be a perfect workaround for communication with central office.
- Network monitoring goes long ways!
  - Open DNS server at 203.0.113.2 was reported in data feeds (including n6!) within hours after new firewall was put in production… and three weeks earlier, during failed attempts.
  - Login attempts (failed) to SSH root account were in the server logs.

Organisational issues

- IT maintenance and monitoring was outsourced to Company X
- Firewall migration was contracted to Company Y
- Company X was aware of firewall migration, yet it did not pick up any signs of incoming problems
- Each company had its contractual obligations, but clearly nobody was enforcing them

Chapter IV

Open questions

- How to deal with monitoring and incident response when IT is almost completely outsourced?
- Why was this particular DNS server so heavily exploited?
  - Are there any ranks of identified open amplifiers?

How to contact us

- web: www.cert.pl, n6.cert.pl
- mail: info@cert.pl
- twitter: @CERT_Polska, @CERT_Polska_en
- facebook: fb.com/CERT.Polska
- youtube: CERTPolska

- Przemek.Jaroszewski@cert.pl