RWTH Firewall – mehr Bandbreite, mehr Filtern, mehr Deep Inspection

Jens Hektor

IT Center der RWTH Aachen University

68. DFN Betriebstagung, 15.3.2018

Agenda

- Technisches
- Politisches
- Spannendes

Rückblick

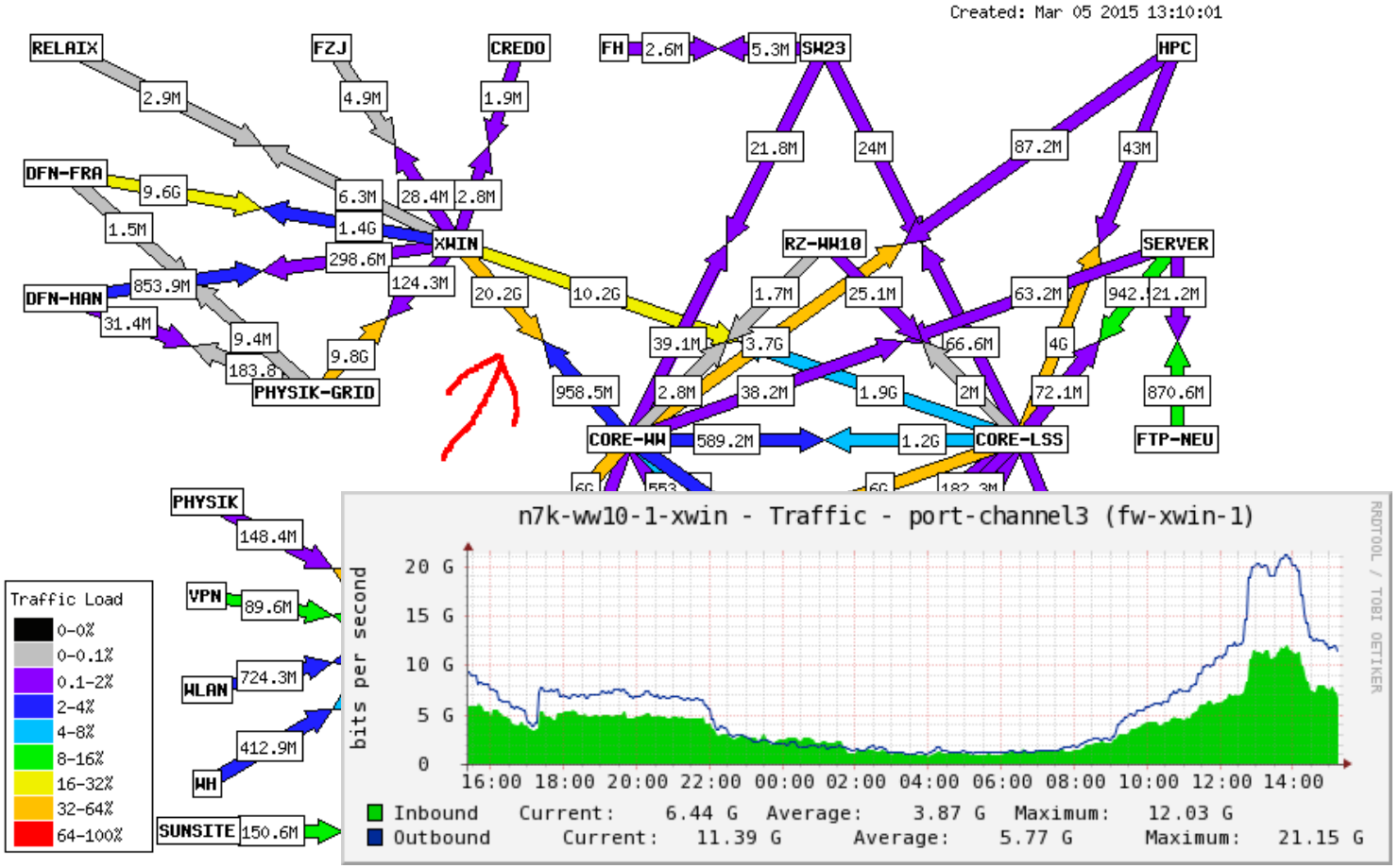
- Anbindungsarchitektur unverändert:
  XWiN-Router (Nexus) – RWTH-Firewall – Core (Nexus) - RWTH

- Alte Firewall (40 Gbit/s): 2x (4 x 10) Gbit/s
- „Preiswerte“ Supermicro Boards
  BIOS „seltsam“

- vorgestellt hier am 4.3.2015, Aussage im Fazit:

  „dieses Jahr > 20 Gbit/s erwartet (Beseitigung Bottlenecks)“
- Dazu folgendes Bild vom 5.3.2015

Rückblick II



Handlungsbedarf

- DFN Bandbreite seitdem auf 2x 100 Gbit/s gestiegen
- „alte“ RWTH-Firewall wird „seltsam“:
  bei Policy Updates Freeze eines der Knotens
  Firewall-Cluster steht, Hard Reset über LOM
- Scheint Hardware zu sein, andere Firewalls OK

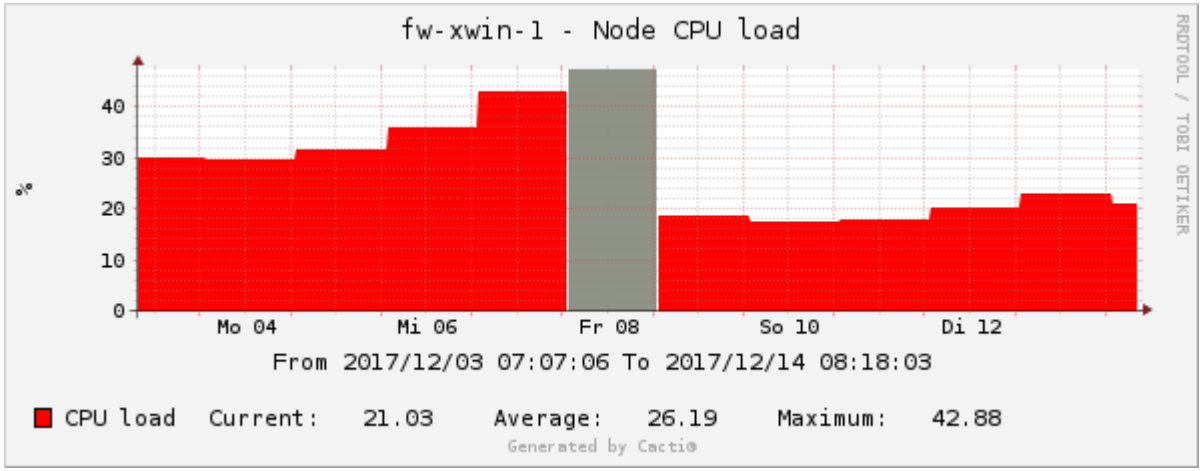
- Also: nächste Generation RWTH-Firewall
  (das macht man so alle 2-3 Jahre)

Auswahl, Hindernisse und Implementierung

- Software damals: Intel Security / McAfee / Stonesoft
- Heute: Forcepoint / Websense (Raytheon)
- Support Backend Finnland: gleichbleibend hohe Qualität
- Lizenzkuddelmuddel (RWTH-Spezifisch)
- Hardware: 2x Cisco UCS C240 M4S, je 4x 40 Gbit/s: 80 Gbit/s
- Software verweigert Installation
  Disk wird nicht richtig erkannt
- BIOS Update: Installation läuft, Firewall läuft
- MTU 9180: Jumbo Frames

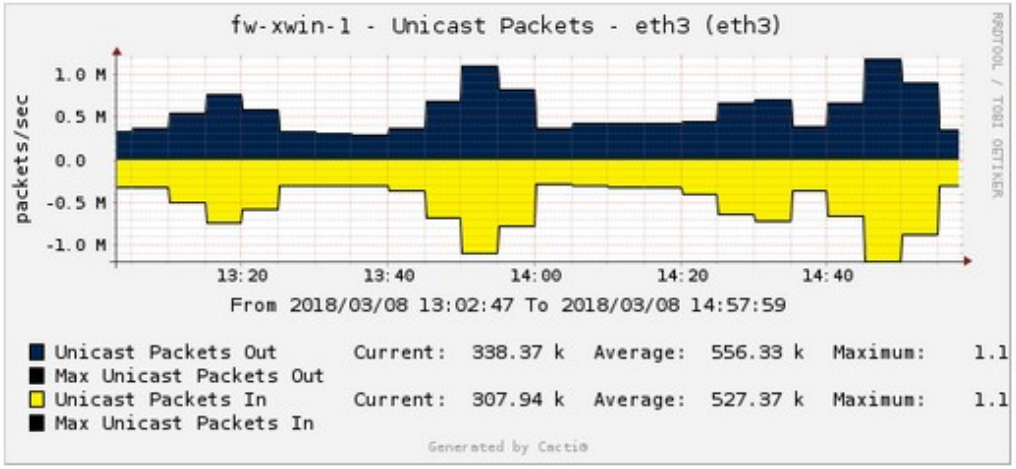
Leistungsdaten I

- CPU load: 20% statt bisher 30%



Leistungsdaten II

- Packets/s: 1.2Mp/s (Tests mit 2 Fluke Etherscope Series II)
  IP to IP, RFC 2544: UDP Pakete mit definierter Bandbreite
  1 Gbit/s: 256 Bytes/p, 128 Bytes/p, 64 Bytes/p*



*: wg. „Akku leer“ im Fluke wiederholt

Zwischenfazit Technik

- Bandbreite verdoppelt
- Paketraten verdoppelt
- Neuere Hardware liefert Luft nach oben (CPU cycles)

Policyänderungen I

- RWTH Firewall sperrte „well-known“ Ports
  alle Ports < 1200 + bekannte „Problemfälle“
- Immer wieder neue Ports dazu
- Policy wird unübersichtlich

- Schrittweise Sperrung aller Ports bis
  3000 (25.10.2016)
  8000 (29.11.2016)
  10000 (7.4.2017)
  20000 (19.6.2017)
  40000 (17.11.2017)

Policyänderungen II

- Letzter Schritt 40000 – 65535 in Q2/2018
- Jeder Schritt vorbereitend mindestens 2 Mann-Tage Arbeit
- Daten zu großen Teilen aus Router-ACLs
- Anmeldungen der Admins
- Nachmeldungen

- Hohe Akzeptanz in der Administratorengemeinde

  (alle Änderungen der Policy mit mindestens einem Monat Vorlauf angekündigt)

Policyänderungen III

- Blacklisting bekannter „böser“ IP-Adressen
- Zunächst: „Emerging Threats“ von Shadowserver
- Dann: Internet Storm Center
- Weitere: Talos (Cisco), CINS (Sentinel IPS), Binary Defense, SANS Top 100, Alienvault, blocklist.de
- IP-Adressen „uniqed“: ~50k

- Alle öffentlich verfügbar, wird täglich aktuell via API in Firewall gepushed

- Impacts? CPU: nein, Beschwerden: nein, externe Honeypots(?)

Next Generation I

- CPU hat Luft: Deep Inspection für HTTP (~ 1k Server)
- Ebenfalls Inspection ausgehender Traffic der Server!
- Impact auf CPU: nicht messbar

- Deep Inspection ICMP, DNS, SSH, RDP

- Geplant: HTTPS (s. Vortrag C. Strauf)

Next Generation II

- 67. DFN BT:
  H. Walter: Selbstgebaute IPS Signaturen und Einsatzszenarien

- SSH brute force blacklisting auch für RDP brute force im Einsatz
  Impact: Informatik Institut zur Klausur auf Ski-Hütte
  Rsync via SSH (Tab Completion)
- HTTP deep inspection Logs zeigen Einsatz von Scan-Tools:
  OpenVAS, ZmEu, MuieBlackcat, Dfind, SQL Ninja

- IMCP Timestamp requests gepaart mit HTTP(S) probing
- Bei einsprechenden Counts wird geblacklisted (i.d.R. 1h)

Next Generation III

- Geo-IP basierte Freigaben (AS680, DE, EU, …)
- URL basierte Freigaben:

  Verboten:
  http://www.x.rwth-aachen.de/wp-admin/
  Erlaubt:
  http://www.x.rwth-aachen.de/

- Kommend: User-basierte Freigaben (Agents auf Client)

Fazit

- 80 Gbit/s
  Ausbau auf 160 Gbit/s in den nächsten Monaten
- Policy geht Richtung Vollfilterung
- Blacklisting zur Reduktion der Angriffsfläche
- Aktives Blacklisting mit Next Generation Features
- Firewalls werden „smarter“
  … und Firewalling spannender

Eine Woche in der Hochschule