AVSYSTEM

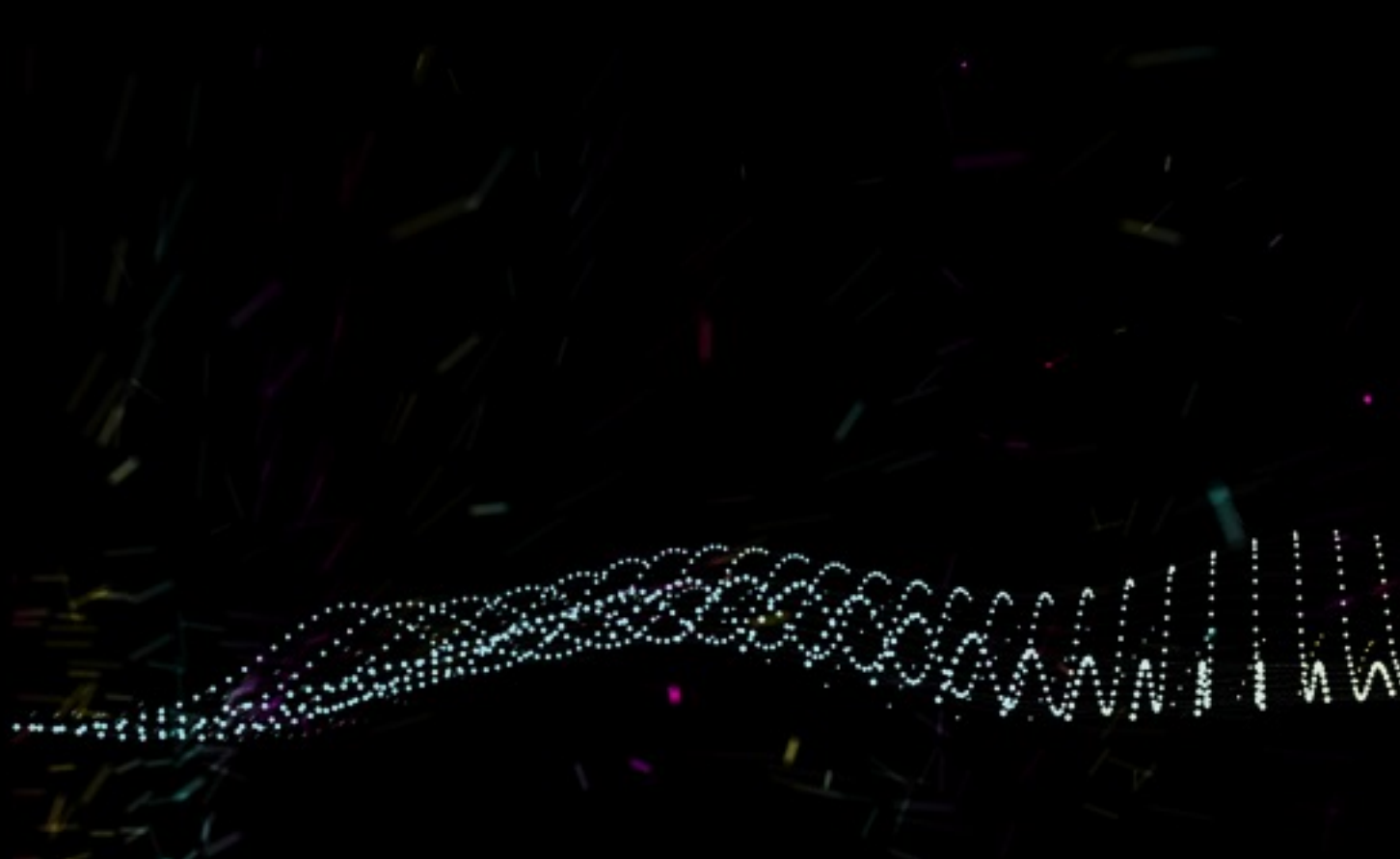
DANIEL ANTAS - SRE

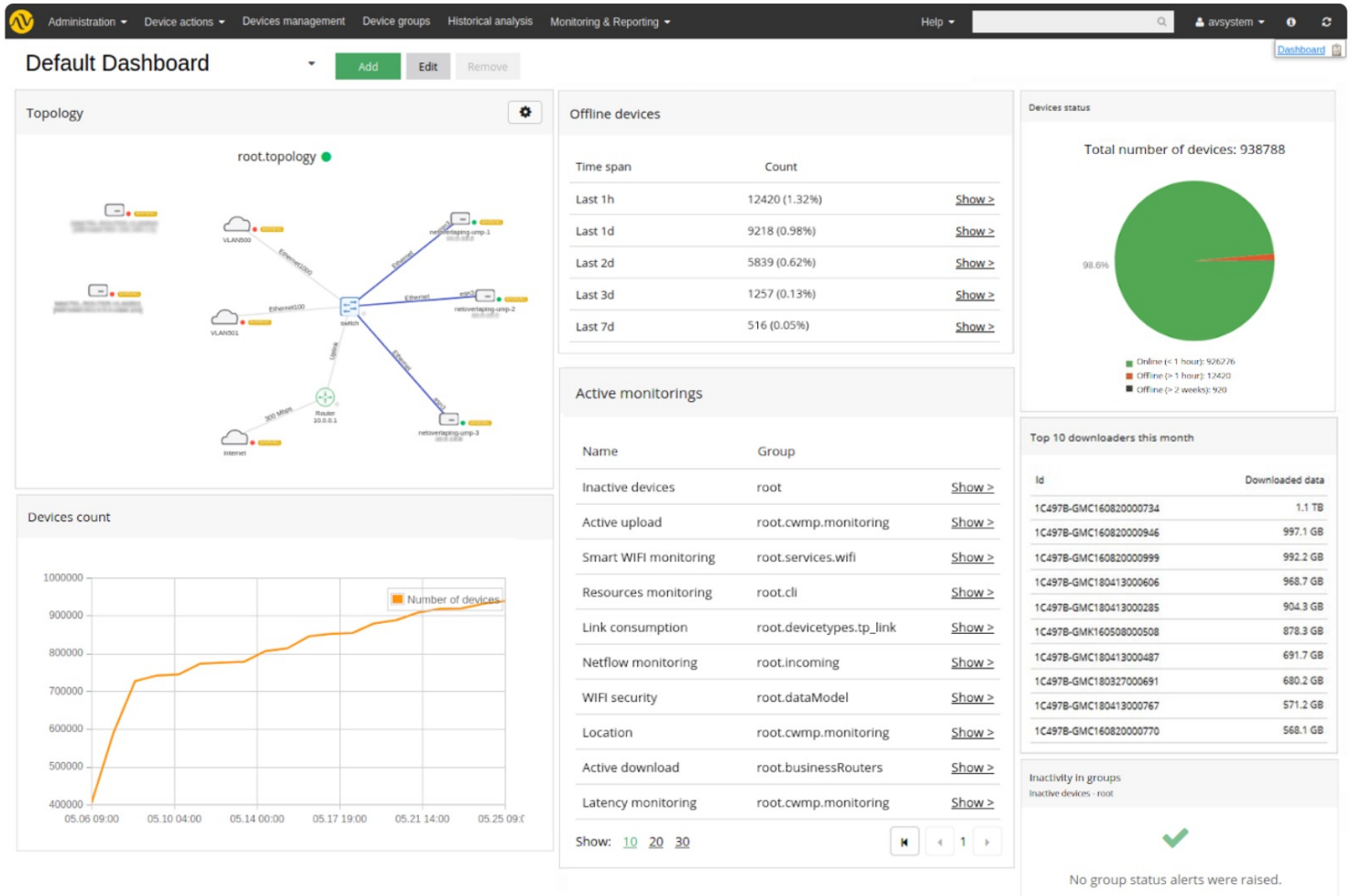
SSL OFFLOAD PRZY UŻYCIU NGINX



AGENDA

1. Od czego się zaczęło?
2. Jak do tego podejść?
3. Sposoby rozwiązania
4. Wybór technologii
5. POC
6. Q&A



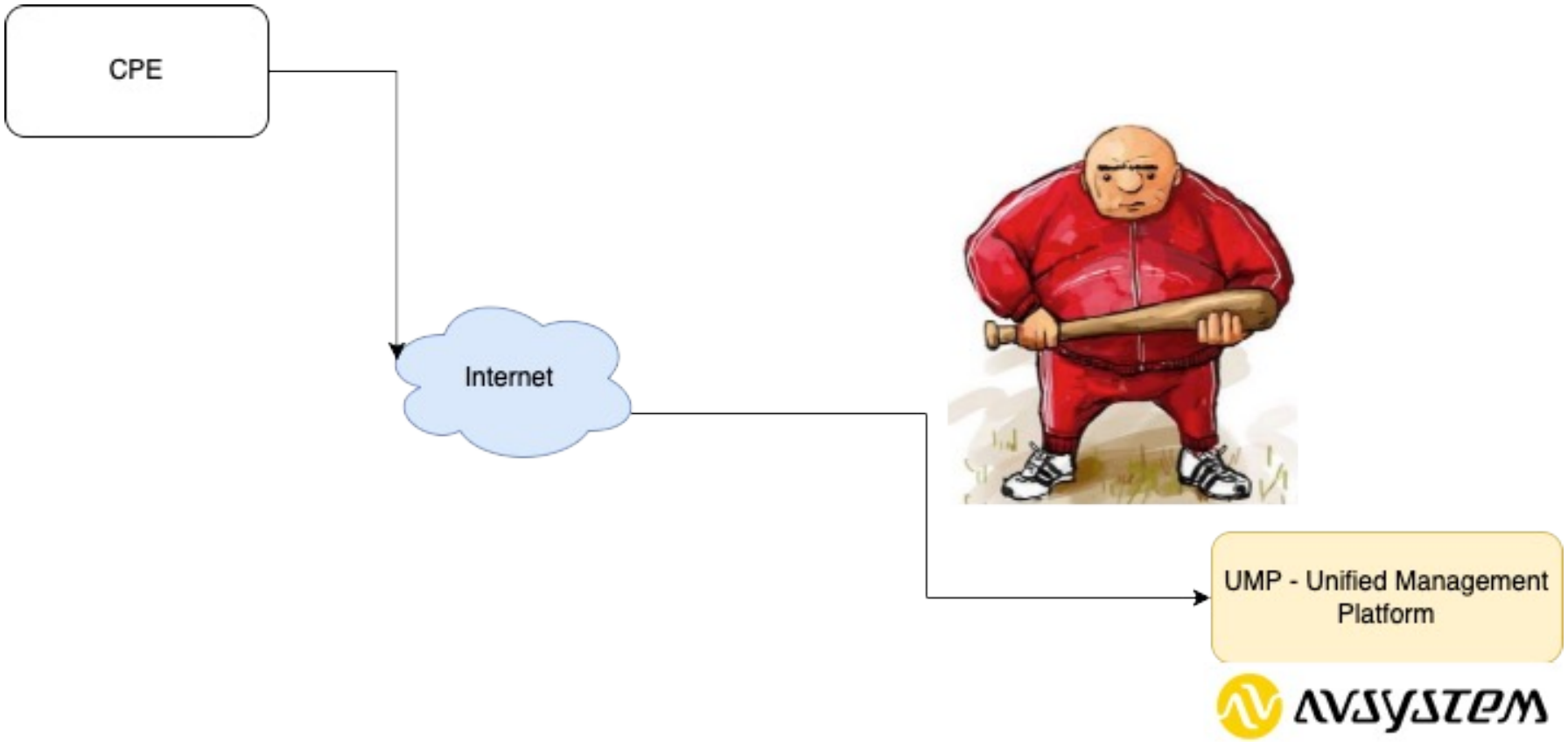


Easily configure and activate new services

Transition from tedious manual configuration to service activation using zero-touch provisioning. Easily manage and upgrade the firmware on both your new and legacy devices in a secure, automated and unified fashion regardless of the underlying technology.

Check features

JAK DO TEGO DOSZŁO?



WIRESHARK

```
SSLv2        198  Client Hello
TCP           62  28443 → 47962 [ACK] Seq=1 Ack=143 Win=28032 Len=0
TLSv1.2       63  Alert (Level: Fatal, Description: Handshake Failure)
```



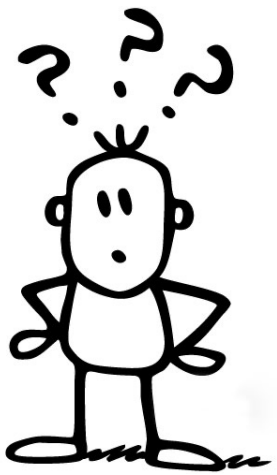

```
Transport Layer Security
  TLSv1.2 Record Layer: Alert (Level: Fatal, Description: Handshake Failure)
      Content Type: Alert (21)
      Version: TLS 1.2 (0x0303)
      Length: 2
    Alert Message
        Level: Fatal (2)
        Description: Handshake Failure (40)
```

JAK ROZWIĄZAĆ PROBLEM?



X 15 000

1 500 000 zł





Wymiana urządzeń

Wymyślcie coś innego

WYMAGANIA

1. Tanie
2. Szybkie
3. Obsługuje SSLv2
4. Bezpieczne
5. Linux



SSL OFFLOADING

HTTPS (SSLv2)

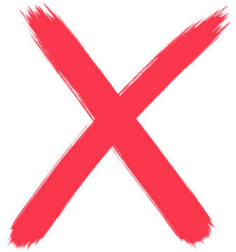


HTTP

JAKA TECHNOLOGIA

HAProxy

- ✓ Tani
- ✓ Szybki
- X Obsługuje SSLv2

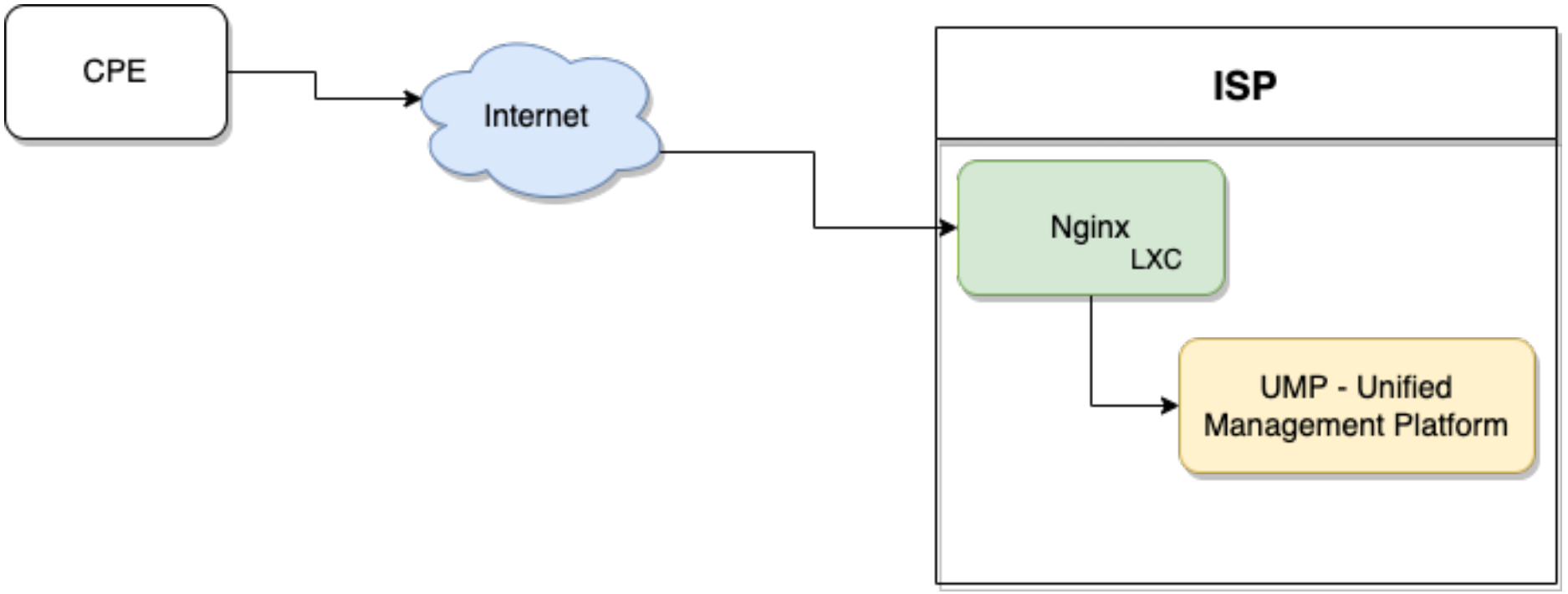


Nginx

- ✓ Tani
- ✓ Szybki
- ✓ Obsługuje SSLv2
- ✓ Bezpieczny
- ✓ Linux



POC


CPE
Internet
ISP
Nginx
LXC
UMP - Unified
Management Platform

THANK YOU FOR YOUR TIME

