

## Zákazník

 Univerzita Tomáše Bati ve Zlíně

## Obor činnosti

Věda, výzkum a vzdělávání

## Výzvy

- ▶ Zajištění dostupnosti on-line služeb, které jsou pro chod univerzity klíčové
- ▶ Rychlé odhalování provozních a bezpečnostních incidentů za NATem
- ▶ Rozsáhlá heterogenní IT infrastruktura
- ▶ Časté útoky z internetu do interní sítě i naopak

## Přínosy řešení

- ▶ Viditelnost veškerého provozu, včetně historie za několik let
- ▶ Rychlá lokalizace problémů v infrastruktuře
- ▶ Automatická detekce atypického chování
- ▶ Pravidelný reporting a detailní pohled do provozu sítě
- ▶ Zdroj dat pro automatizaci procesů

## Nasazené produkty

- ▶ Flowmon kolektor 12000
- ▶ Flowmon sonda 40000

## Kontakt

Ing. Petr Vojtek

Ing. Petr Skovajsa

[www.utb.cz](http://www.utb.cz)

## Univerzita Tomáše Bati ve Zlíně (UTB)

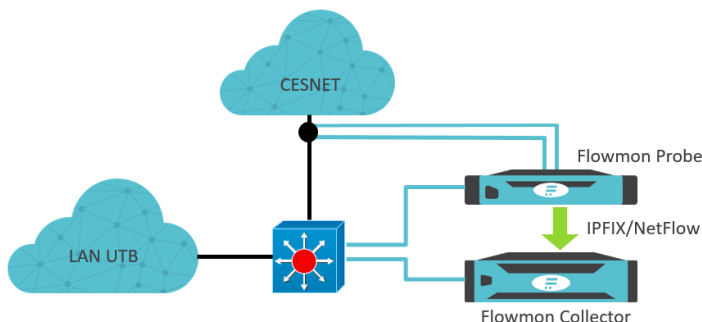
UTB je dynamicky se rozvíjející vysoká škola. S více než deseti tisíci uživateli, řadou informačních systémů a infrastrukturou závislou od správné funkčnosti sítě, je viditelnost do síťového provozu klíčová.

## Situace

IT infrastruktura UTB je rozmístěna v patnácti objektech v rámci města Zlína a jednom detašovaném areálu v Uherském Hradišti. Páteří sítě má hvězdicovou topologii na technologii 10 Gbps ethernetu. Některé menší objekty jsou připojeny rychlostí 1 Gbps. K Internetu je síť připojena rychlostí 10 Gbps prostřednictvím infrastruktury CESNETu. Kromě provozních problémů řeší správci sítě UTB také bezpečnostní incidenty nebo porušování autorských práv, když studenti neoprávněně sdílí multimediální obsah. Současně je nezbytná nepřetržitá kontrola datových toků, aby se zabránilo neoprávněnému vytěžování sítě na úkor ostatních uživatelů. Flowmon správcům pomáhá se s těmito problémy efektivně vypořádat.

## Nasazení řešení Flowmon

Monitorování sítě zajišťuje jedna sonda se čtyřmi 10G monitorovacími rozhraními. Vnitřní komunikace je monitorována s využitím jednoho 10 GbE SPAN/mirror portu na centrálním L3 switchi Cisco Catalyst 6500, který je zapojen do jednoho monitorovacího portu sondy. Pro sledování příchozí/odchozí komunikace se sítí CESNET je využito zapojení prostřednictvím optického TAPu zapojeného do dvou monitorovacích portů sondy. Dlouhodobé uložení dat a jejich analýzu zajišťuje Flowmon kolektor disponující kapacitou 12 TB a hardwarem Raid 6.



## Vyjádření zákazníka

Administrátoři sítě UTB ve Zlíně, Ing. Petr Vojtek a Ing. Petr Skovajsa, hodnotí více než šestiletou zkušenost s řešením Flowmon takto:

„Řešení Flowmon využíváme k dohledu nad aktuálním stavem sítě. Výrazně nám zjednodušuje analýzu síťového provozu a detekci anomálií. Díky Flowmon ihned odhalíme vznikající problém, který by mohl negativně ovlivnit provoz celé sítě, např. zařízení generující nadměrný síťový provoz. V případech, kdy jsme požádáni o součinnost při řešení bezpečnostního incidentu, nám Flowmon šetří hodiny strávené nad ručním dohledáváním údajů o podezřelých aktivitách v síti. Data uložená na Flowmon kolektoru využíváme také pro automatizaci procesů spojených se správou sítě.“