cesnet

Architektura připojení pro kritické sítě a služby

Tomáš Košňar
CESNET

12. 6. 2018
CSNOG

Architektura připojení pro kritické služby

- **..k zamyšlení**
  - neexistuje univerzální řešení pro všechny případy
- **..k motivaci**
  - stabilita a spolehlivost služeb má klíč ve „vychytaných“ a ošetřených detailech
  - znalý a kvalitní personál těžko nahradíme úspěšným tendrem nebo dobrou smlouvou.. ;-)
- **..„opakování je matka moudrosti“**

Architektura připojení pro kritické služby

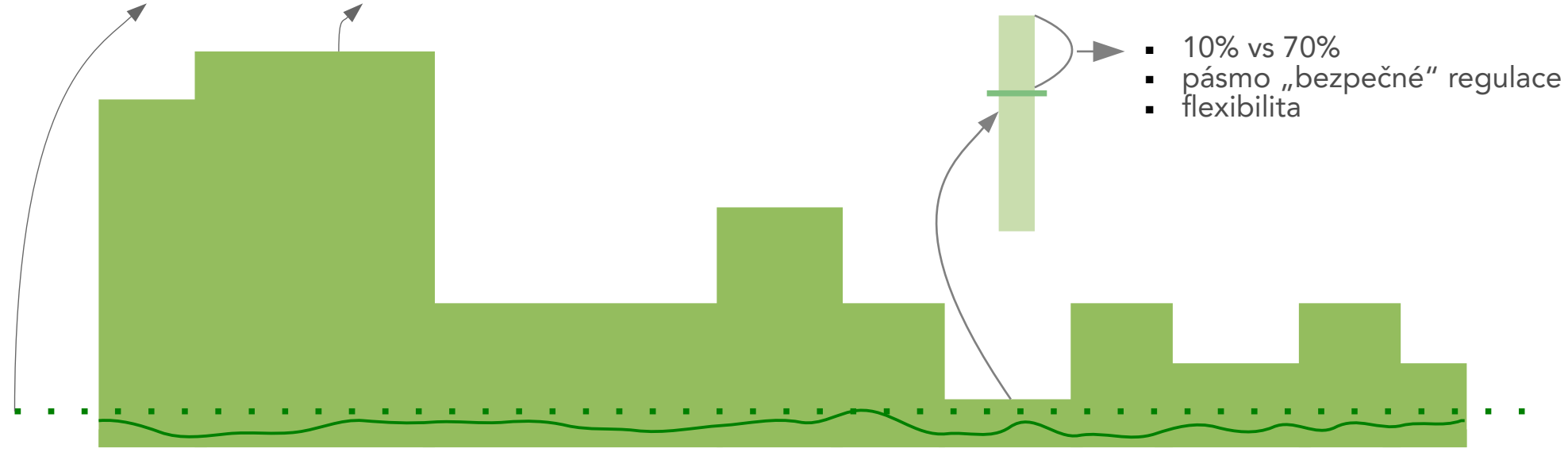
- **modelový příklad**
  - typické články řetězu na cestě ke službě
- **péče zpravidla soustředěna na vlastní aplikaci**
  - výkon front-end, funkce UI, testy výkonu apod.
- **posuzovat komplexně celý síťový „set-up" k/od služby**
  - → „aby se to pokud možno nikde neucpávalo" (nedocházely zdroje)

..a když zdroje docházejí, **regulujme řízeně → strategie** *(„čeho se budu postupně vzdávat")*

  - **rozložme strategicky zátěž pro případ extrémních situacích** mezi dílčí prvky +případně posilme příliš slabé (relativně) články řetězu

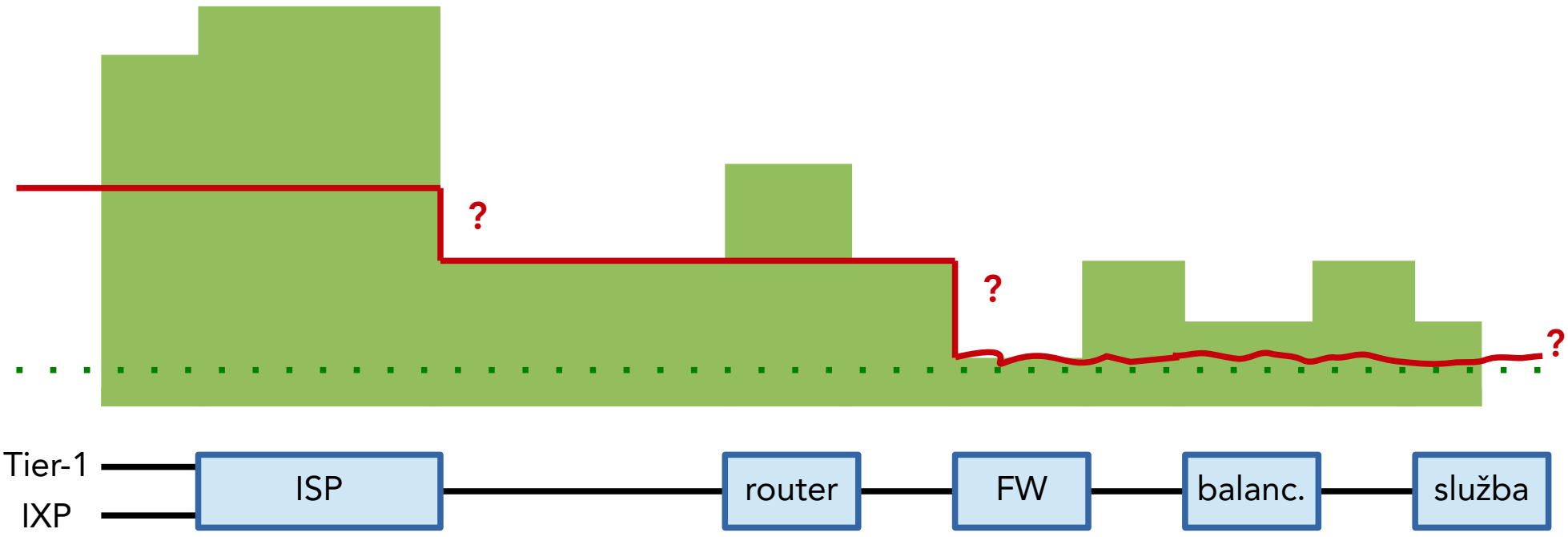
Architektura připojení pro kritické služby

- **kapacita, zdroje**
  - **potřebná** vs. **dostupná kapacita** v jednotlivých částech řetězce v **běžném stavu**



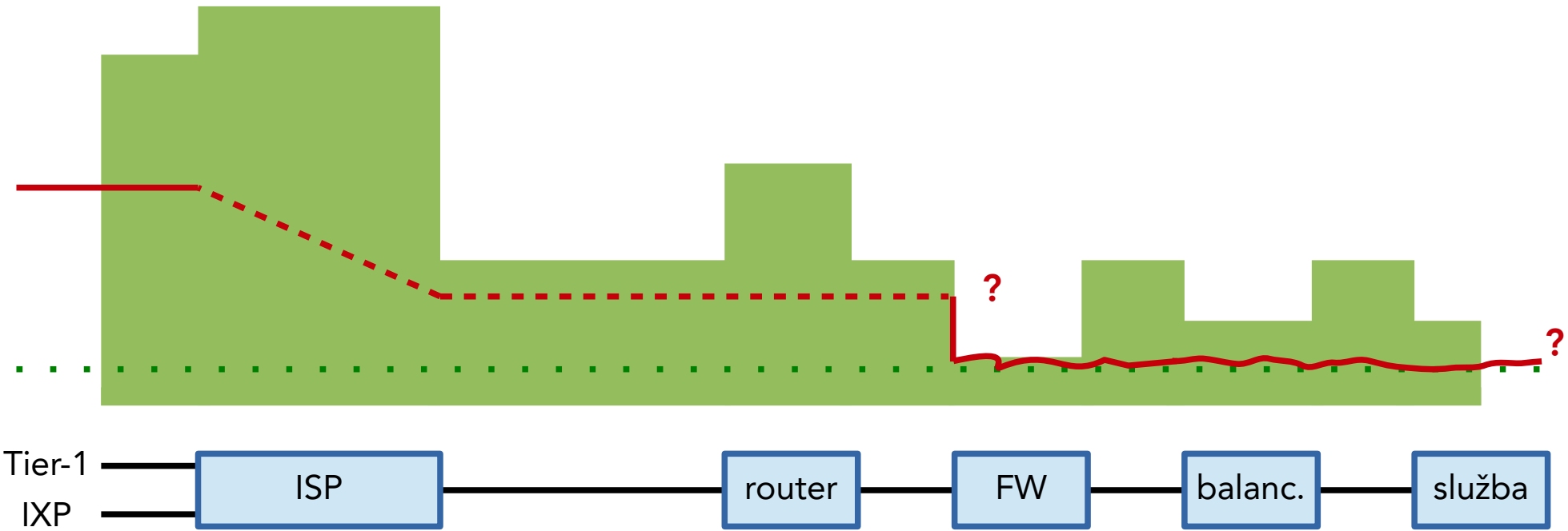
Architektura připojení pro kritické služby

- kapacita, zdroje
  - **bez regulace** v **extrémním stavu** → data zahazována nahodile, neřízeně, služba zpravidla nedostupná



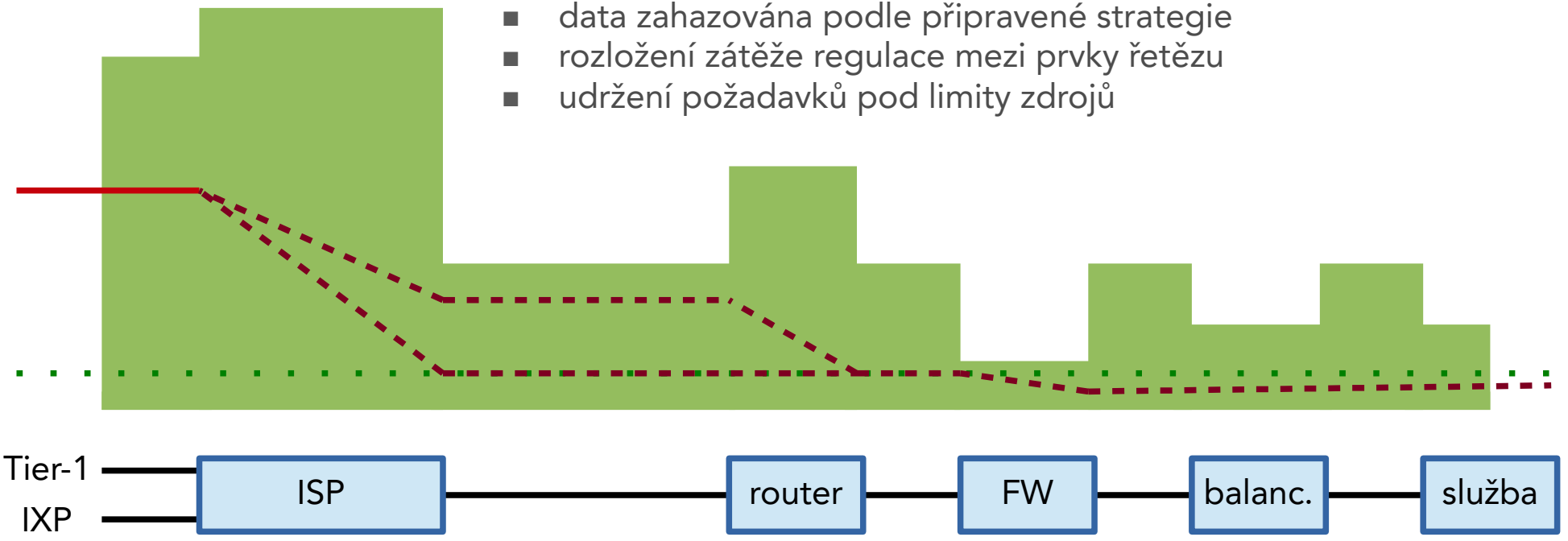
Architektura připojení pro kritické služby

- kapacita, zdroje
  - **částečná regulace** v **extrémním stavu** – **realizace na jednom článku**
  - ISP zabránil „ucpání přípojky“, ale z pohledu FW stejný stav jako v předchozím případě



Architektura připojení pro kritické služby

- **kapacita, zdroje**
  - **řízená regulace** v **extrémním stavu** - realizace na řetězu prvků

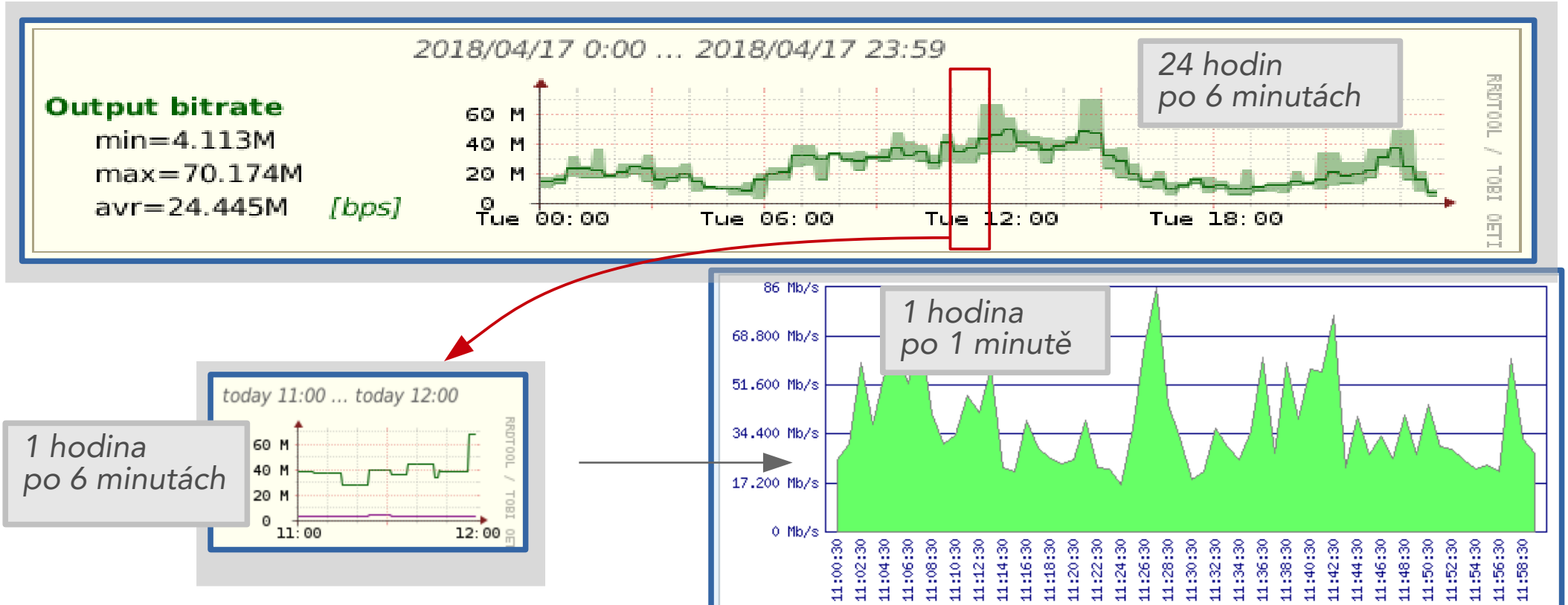


Architektura připojení pro kritické služby

- **typická slabá místa**
  - **specializované prvky FW, balancery,..**
  - složitá logika, uchování stavových informací apod. → velké nároky na vnitřní zdroje
  - **reálná průchodnost závislá na struktuře provozu**
    - objem provozu
    - velikost paketů
    - transportní protokoly ~ např. počet TCP sessions
    - aplikační protokoly
    - …
  - **monitoring**
    - pomůže nalézt slabá místa, ověřovat jaký je poměr dostupných a potřebných zdrojů
    - **podmínka dobrého nastavení a optimalizace celé soustavy**
    - **bez komplexních informací s odpovídající vypovídací hodnotou pouze tápeme**

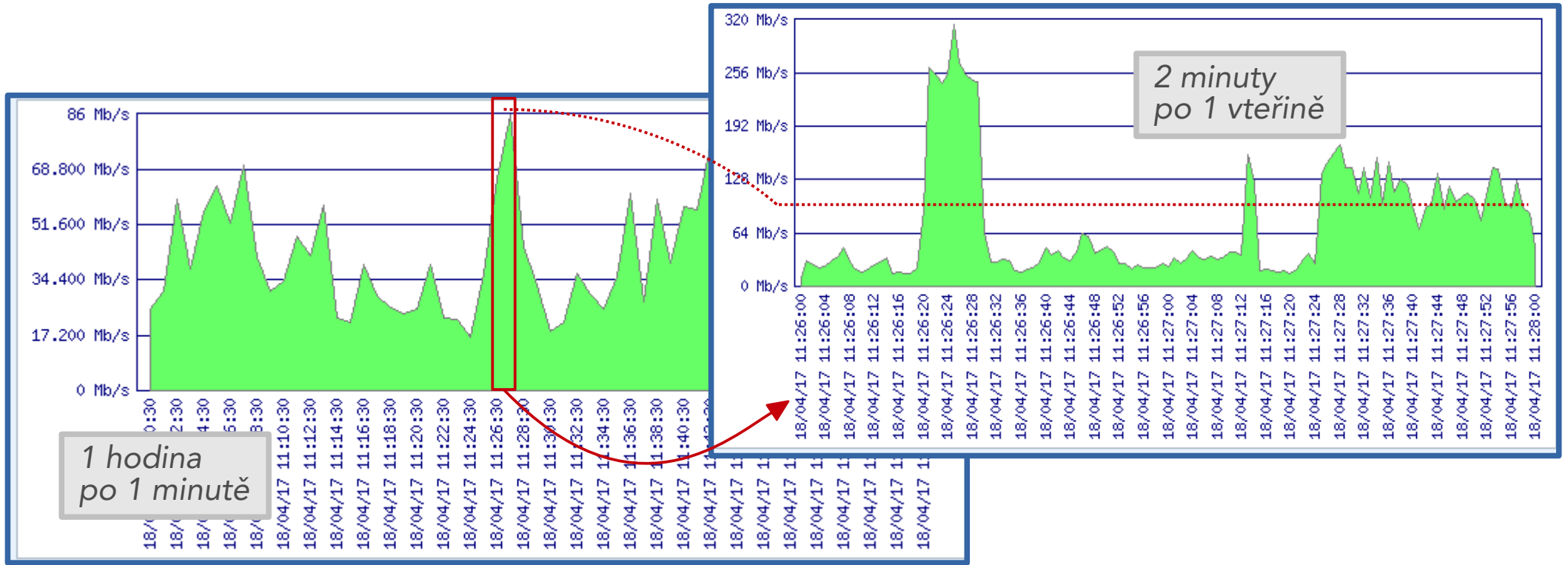
Architektura připojení pro kritické služby

- **odpovídající měření → použitelné výsledky monitoringu**
  - reálně potřebná přenosová kapacita – vliv parametrů měření
  - linkové měření vs. flow-based měření, **vliv časového kroku měření**



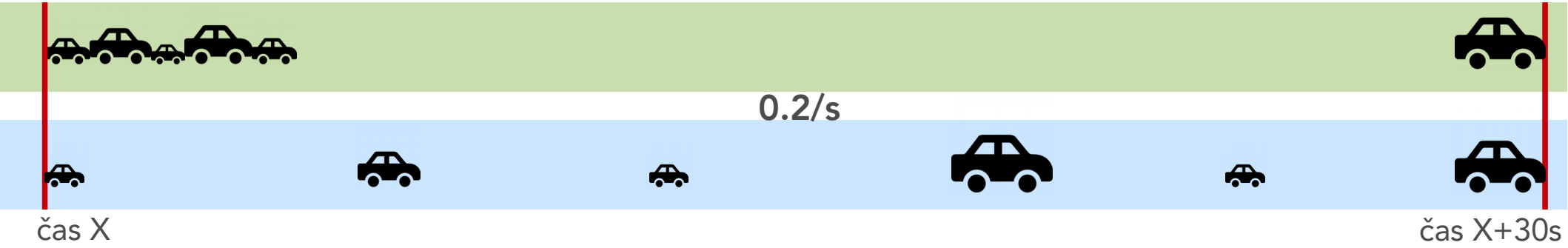
Architektura připojení pro kritické služby

- **odpovídající měření → použitelné výsledky monitoringu**
  - typický „síťařský“ limit – 50% funguje pro rozsáhlé sítě s vysokou mírou agregace provozu
  - samostatná/izolovaná koncová síť/aplikace v „mikro perspektivě“ – potenciálně větší oscilace

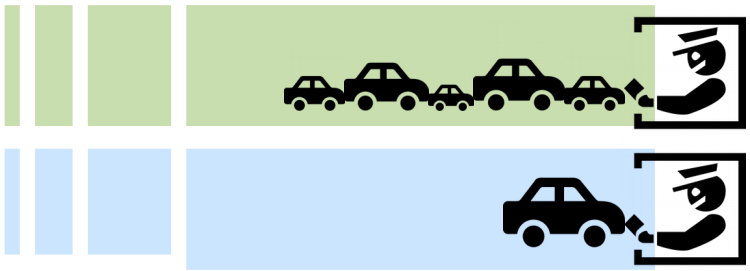


Architektura připojení pro kritické služby

- **odpovídající měření → použitelné výsledky monitoringu**
  - rychlost přenosu je konstantní
  - měříme objem přenesených dat *(počet a velikost paketů)* mezi dvěma po sobě jdoucími „odečty“

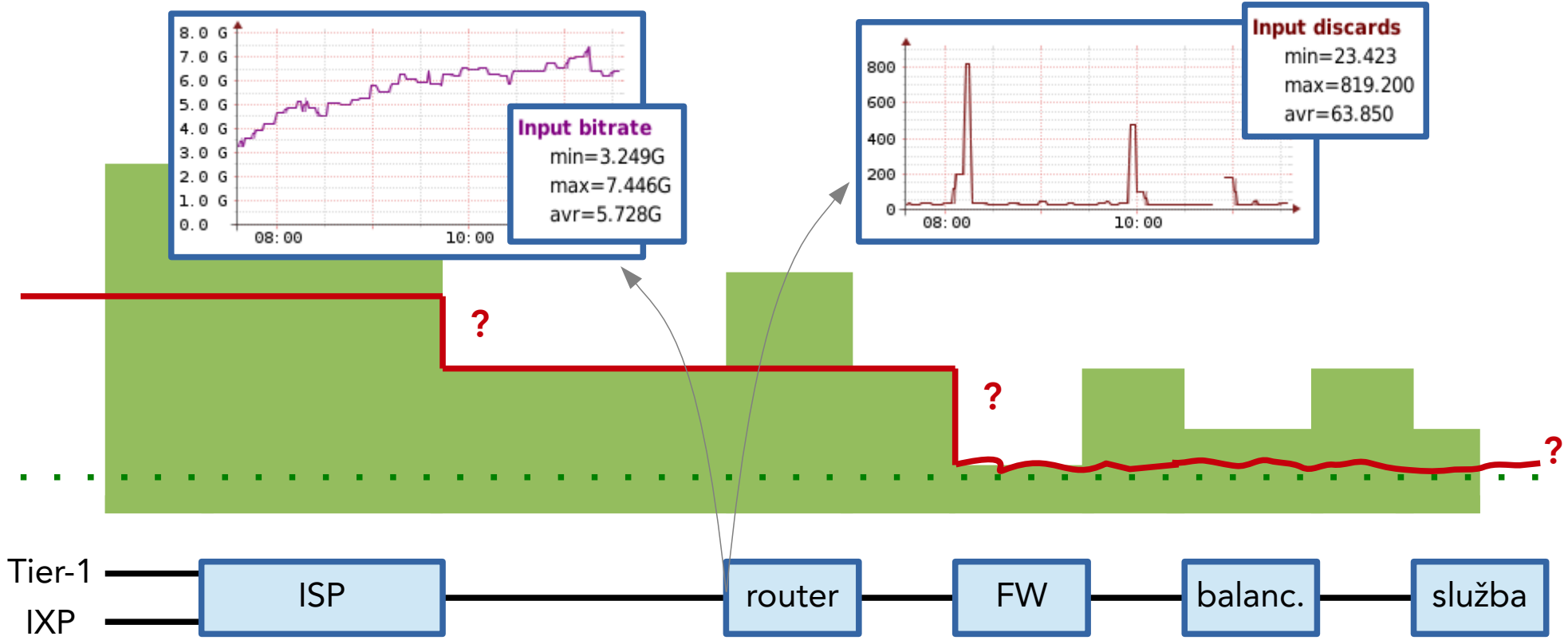


- shluk na trase nevadí
- ale u obslužného systému může být problém
- rychlost obsluhy např. 1 za 5s
  - poslední čeká ~20 s na obsloužení



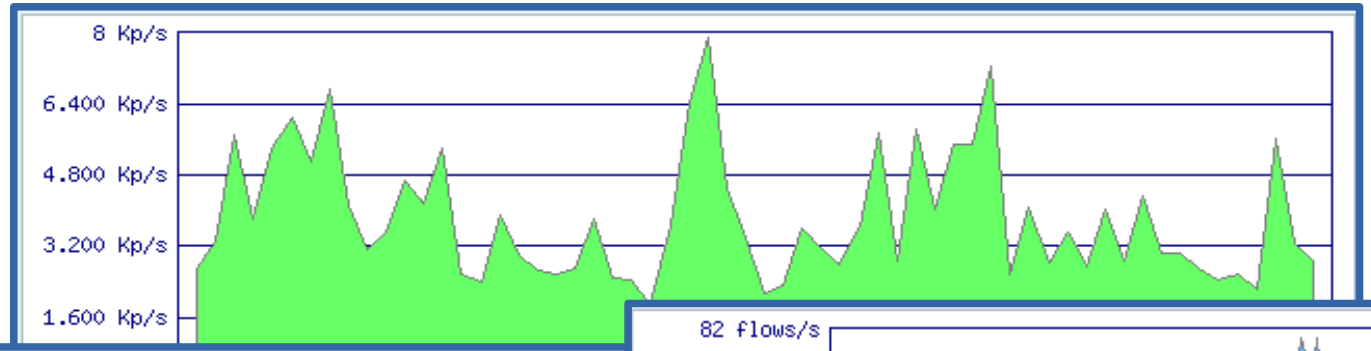
Architektura připojení pro kritické služby

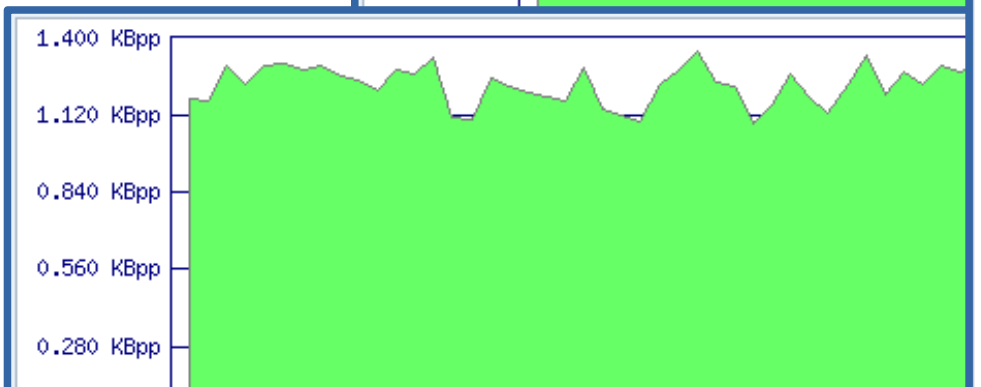
- **odpovídající měření → použitelné výsledky monitoringu**
  - monitoring infrastruktury – ukázka indikace problému (i bez saturace)

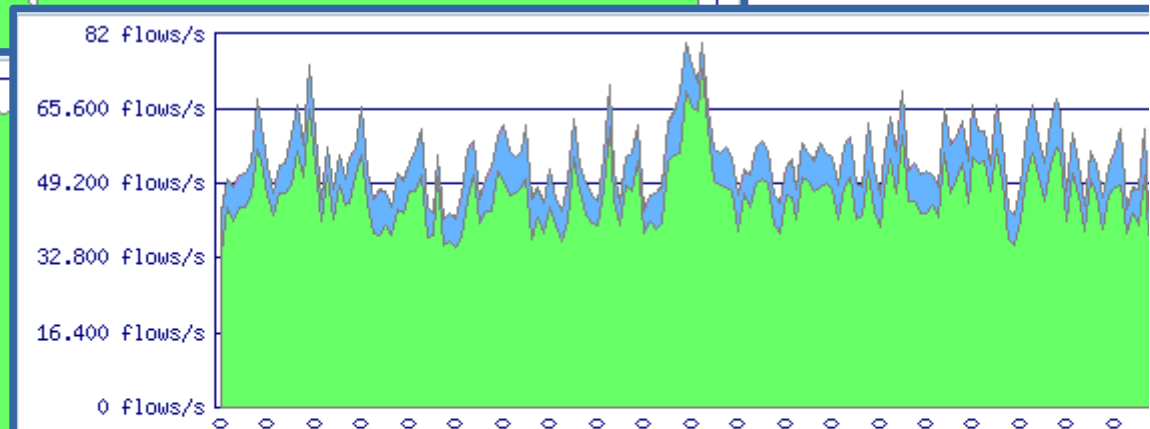


Architektura připojení pro kritické služby

- **odpovídající měření → použitelné výsledky monitoringu**
  - četnost a průměrná délka paketů
  - např. limity FW závislé na
    - délce paketů, transportu (TCP vs. UDP), počtu TCP sessions v případě TCP

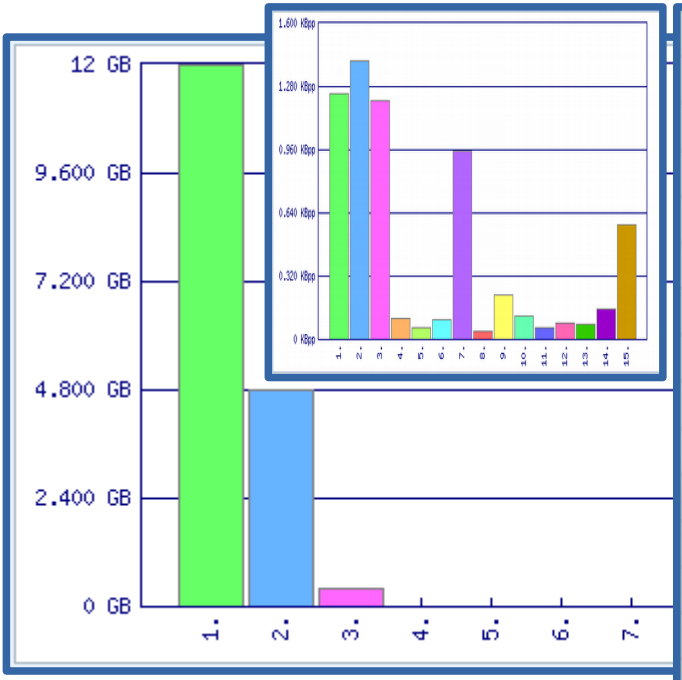






Architektura připojení pro kritické služby

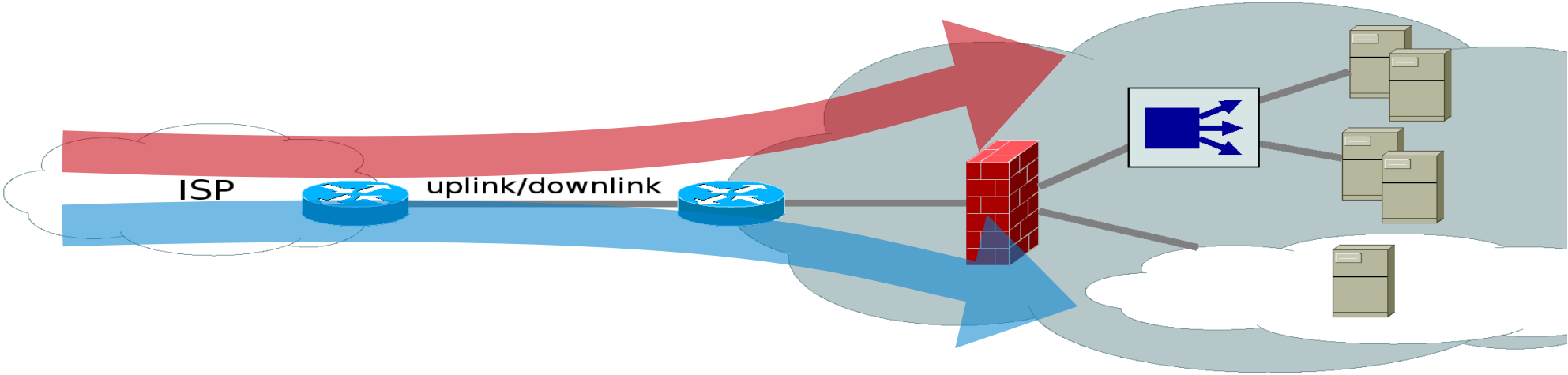
- **odpovídající měření → použitelné výsledky monitoringu**
  - struktura provozu – protokoly, čísla portů, objemy v „ustáleném“ stavu
  - znalost chování služby, komunikace s podpůrnými službami → optimalizace nastavení



o	>	Protocol	Src-Port	TOS-flags	TCP-flags	Bytes-estimated
1.	>	tcp (6)	https (443)	11111111	fin(1), syn(2), rst(4), push(8), ack(16)	11.989 GB ~ 69.768%
2.	>	tcp (6)	http (80)	11111110	fin(1), syn(2), rst(4), push(8), ack(16)	4.796 GB ~ 27.909%
3.	>	udp (17)	443	00000000		380.770 MB ~ 2.216%
4.	>	udp (17)	domain (53)	11101100		14.670 MB ~ 0.085%
5.	>	tcp (6)	1197	00000100	push(8), ack(16)	1.360 MB ~ 0.008%
6.	>	tcp (6)	smtp (25)	11100100	fin(1), syn(2), rst(4), push(8), ack(16)	1.137 MB ~ 0.007%
7.	>	tcp (6)	pop3s (995)	00000000	fin(1), syn(2), rst(4), push(8), ack(16)	290.560 KB ~ 0.002%
8.	>	tcp (6)	ssh (22)	00001010	push(8), ack(16)	229.146 KB ~ 0.001%
9.	>	tcp (6)	imaps (993)	00000000	fin(1), syn(2), rst(4), push(8), ack(16)	143.220 KB ~ 0.001%
10.	>	udp (17)	1193	00000000		95.096 KB ~ 0.001%
11.	>	icmp (1)	Echo-reply (0)	00000000		92.056 KB ~ 0.001%
12.	>	tcp (6)	bgp (179)	11000000	push(8), ack(16)	60.976 KB ~ 0.000%
13.	>	udp (17)	ntp (123)	11111100		39.216 KB ~ 0.000%
14.	>	tcp (6)	urd (465)	00000000	fin(1), syn(2), push(8), ack(16)	36.990 KB ~ 0.000%
15.	>	tcp (6)	1428	00000010	fin(1), syn(2), push(8), ack(16)	31.218 KB ~ 0.000%

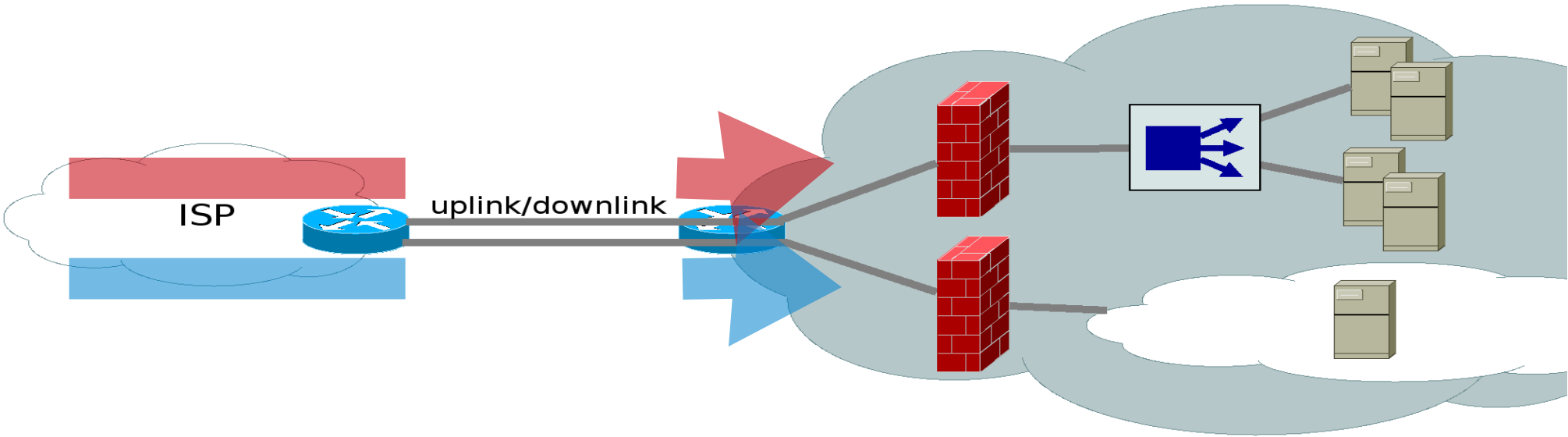
Architektura připojení pro kritické služby

- **topologie**
  - **vliv okolí, sdílení zdrojů**
  - služba v koncové síti organizace, všechny instance FW sdílí stejné HW zdroje (pomíjím HA)



Architektura připojení pro kritické služby

- **topologie**
  - zmenšení vlivu okolí a sdílení zdrojů, oddělené linky, FW na oddělených HW zdrojích

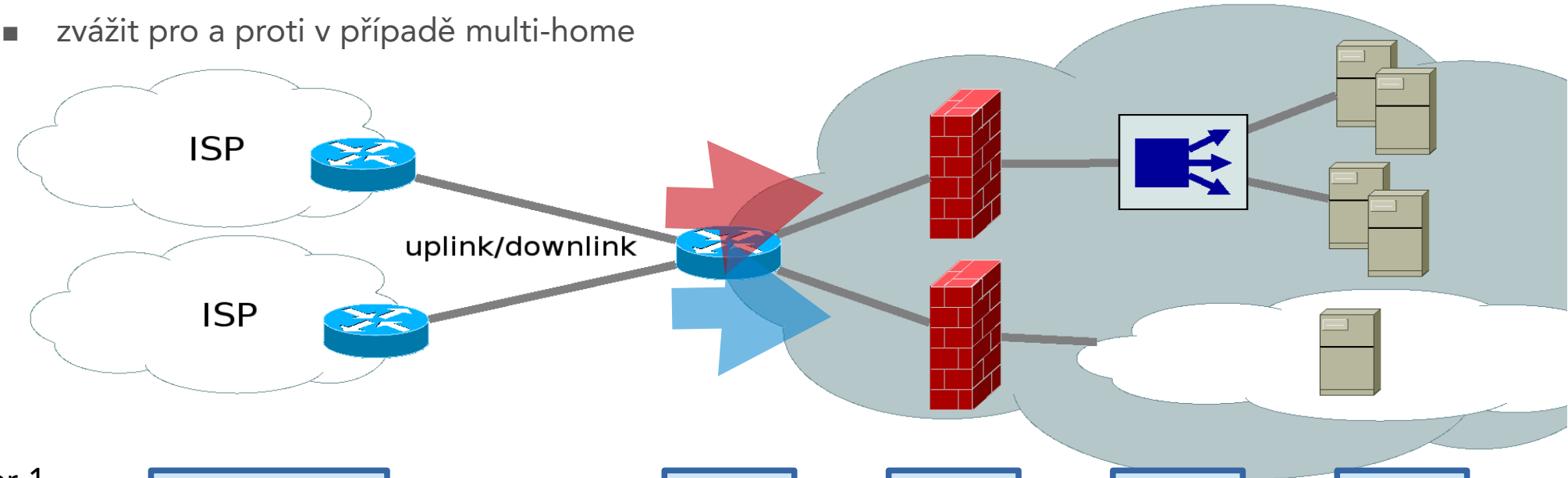


Tier-1
IXP

ISP → router → FW → balanc. → služba

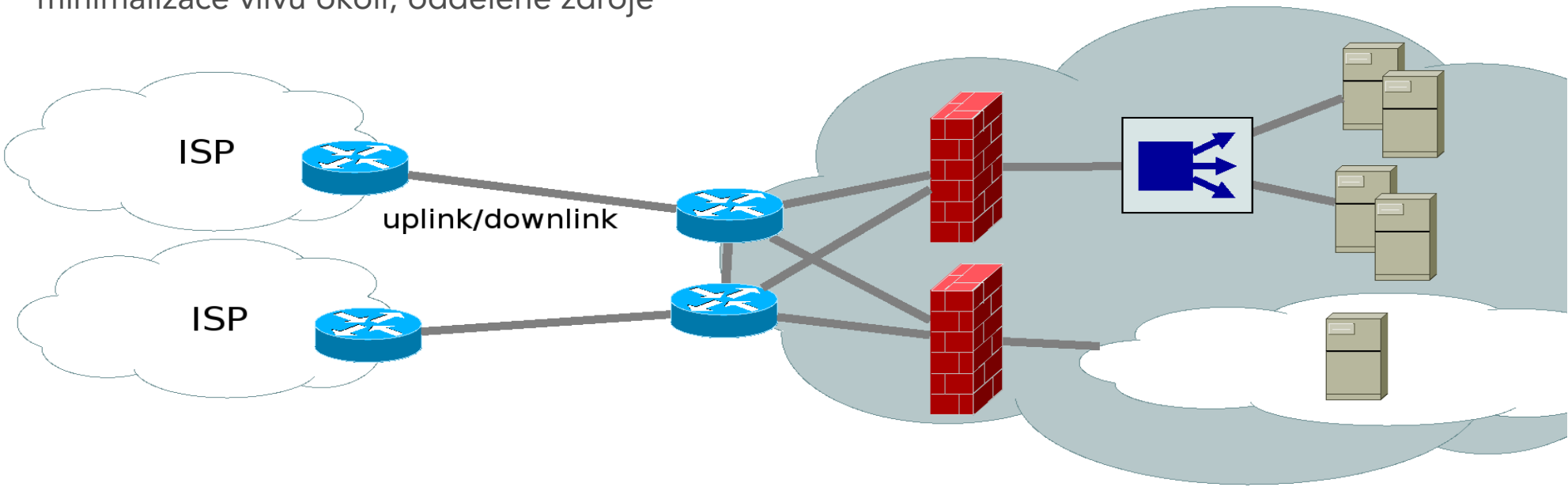
Architektura připojení pro kritické služby

- **topologie**
  - zmenšení vlivu okolí a sdílení zdrojů, oddělené hraniční prvky ISP nebo multi-home
  - zvážit pro a proti v případě multi-home



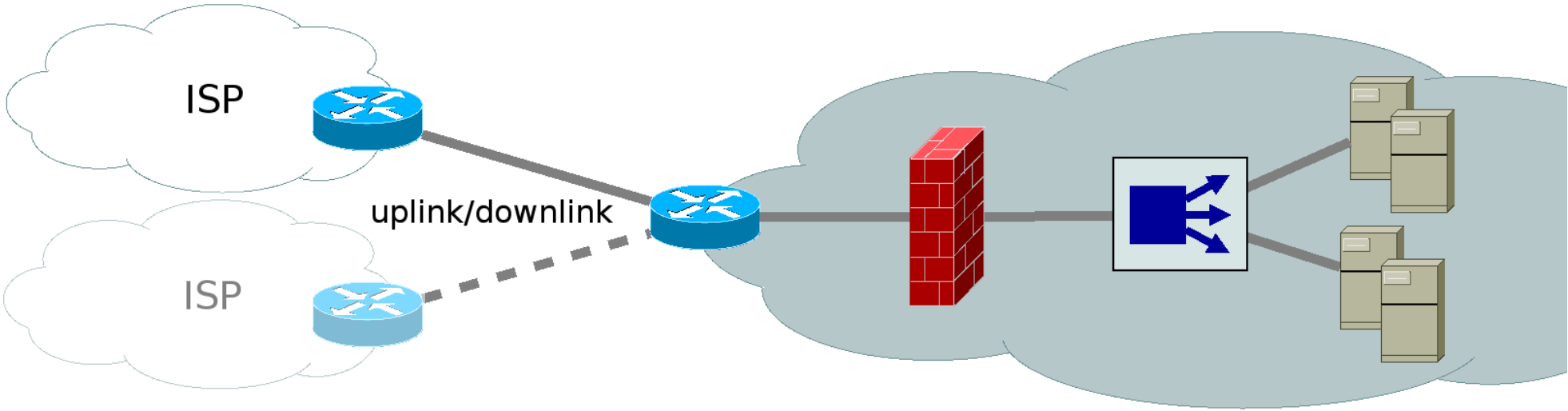
Architektura připojení pro kritické služby

- **topologie**
  - minimalizace vlivu okolí, oddělené zdroje



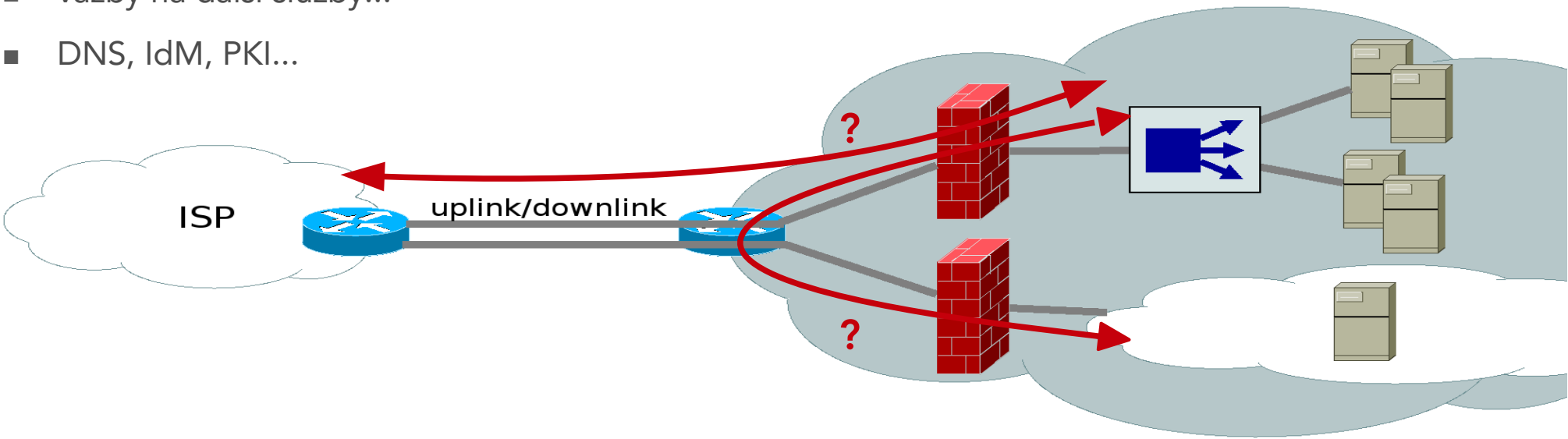
Architektura připojení pro kritické služby

- **topologie**
  - minimalizace vlivu okolí, samostatná síť pro službu



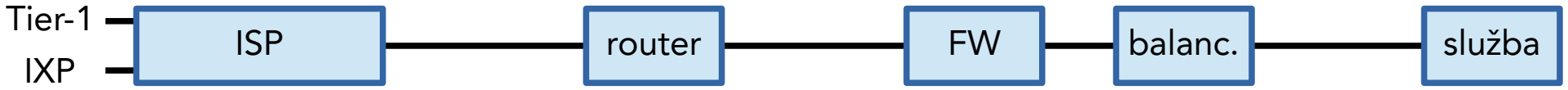
Architektura připojení pro kritické služby

- **závislosti na dalších službách**
  - vazby na další služby...
  - DNS, IdM, PKI...



Architektura připojení pro kritické služby

- **možná opatření**



..předchozí články řetězu se pokusí zajistit, aby se na vstupu následujících neobjevilo víc požadavků než kolik tam máme zdrojů..

- *filtrace provozu*
  - *na cíle/zdroje*
- *rate limit policy*
  - *selektivně/plošně*
  - *zahození/označení*
- *čištění provozu*
- *RTBH*

- *filtrace provozu*
  - *na cíle/zdroje*
- *rate limit policy*
  - *selektivně*
  - *plošně*
  - *zahození*

- *filtrace provozu*
  - *inteligentní*
- *vyvážení provozu ke službě*

- *on-host FW*

Architektura připojení pro kritické služby

- **shrnutí**
  - řešme vždy komplexně
  - vytvořme si podmínky (viz. architektura sítě + sdílení zdrojů) pro možnost samostatného ošetření jednotlivých služeb (ne vše najednou) → ke službě pouštějme pouze provoz, který je jí relevantní
  - regulace provozu → strategie
    - co a jak budu postupně zahazovat
      - analýza provozu služby → znalost charakteru provozu → stanovení priorit provozu + rozložení úkolů mezi články soustavy → implementace + ověření funkce (testy)
    - v případě útoků
      - ..to už musí být nakonfigurované a odzkoušené !!!
      - věnujeme se tomu, co jsme nedokázali predikovat
      - po skončení útoku vyhodnotíme efektivitu implementované strategie → optimalizace/modifikace
  - příprava „nového set-upu“ služby → znalost provozu + monitoring stávajícího set-upu → redesign architektury+volba vhodných prvků (prognóza zdrojů, které budeme potřebovat na konci plánované životnosti daného celku * bezpečnostní koeficient) → implementace → provoz + monitoring...
  - spolupráce s ISP → začít včas !!!

cesnet

Děkuji za pozornost...