cesnet

Architektura připojení pro kritické služby a sítě

Tomáš Košňar
CESNET

10. 12. 2020
Kraj Vysočina – odborný seminář ke kyberbezpečnosti

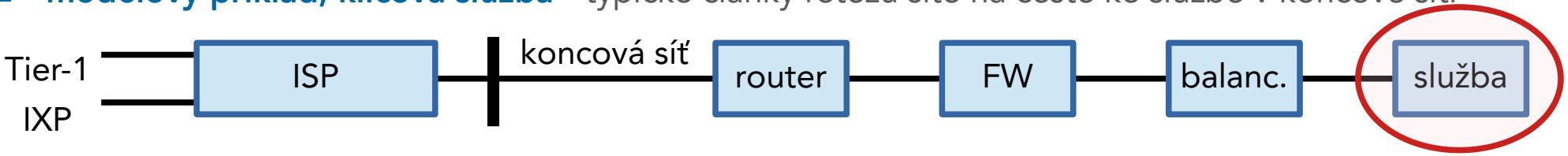
Architektura připojení pro kritické služby a sítě

- **Cíle**
  - **NE konkrétní řešení, ale zdůraznění podstatných aspektů**
    - neexistuje univerzální řešení pro všechny případy ..vždy je třeba cíleně přemýšlet..
  - **Motivovat k aktivitě**
    - stabilita, spolehlivost a odolnost služeb a sítě má klíč v
      - robustní a odolná architektura, systematická správa a promyšlená strategie postupu v krizových situacích
      - „vychytané“ a ošetřené detaily
      - **znalý a kvalitní personál NEnahradíme skvěle připraveným tendrem ani dobrou smlouvou.. ;-)**
      - průběžná analýza a optimalizace ~ „dnes“ špičkové řešení je „zítra“ běžné, „pozítří“ zastaralé ...**„opakování je matka moudrosti“** *..ale kde na to vzít čas ?!?!*
  - **Uvědomit si ;-)**
    - *..bezpečnost a pohodlí nežijí ve stejném vesmíru.. ..děti bez důslednosti dobře nevychováme..*

..místy uchopeno s určitou mírou nadsázky...

Články síťového řetězu

- **modelový příklad, klíčová služba** - typické články řetězu sítě na cestě ke službě v koncové síti



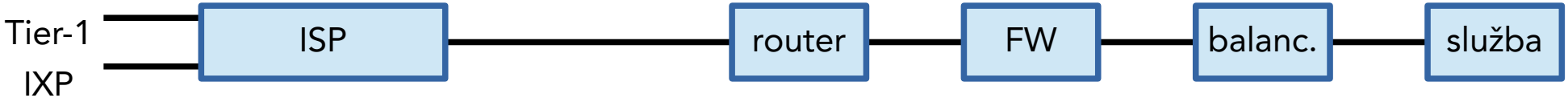
- **při realizaci je nakonec péče zpravidla soustředěna především na vlastní službu/aplikaci**
  - ověření a testy front-end, fce UI, výkon apod. → lokálně/izolovaně - „laboratorní ideální podmínky“
  - *proč to tak končí ?? z praxe ;-)*
    - chtěli jsme to původně jinak, ale ..způsob pořizování, parametry financování, „životnost“ zdrojů, zátěž režijními činnostmi – to nás udolalo.. *a my se nechali ;-)*
    - přestalo být důležité co pořizujeme, podstatné je „jak to pořizujeme“, ..jo a ty PR tlaky ;-)
    - **...nakonec se „každý se stará o to svoje“ ..o celek a vybalancování všech souvisejících komponent málokdo..** už není chuť ani síla ..a dodavatelé si přirozeně chrání kůži *(nám to chodí)* – přirozené, nemůže být zodpovědný za vnější prostředí..
    - a vznikají absurdní schémata, i potenciální „trhliny“ z hlediska bezpečnosti

Články síťového řetězu

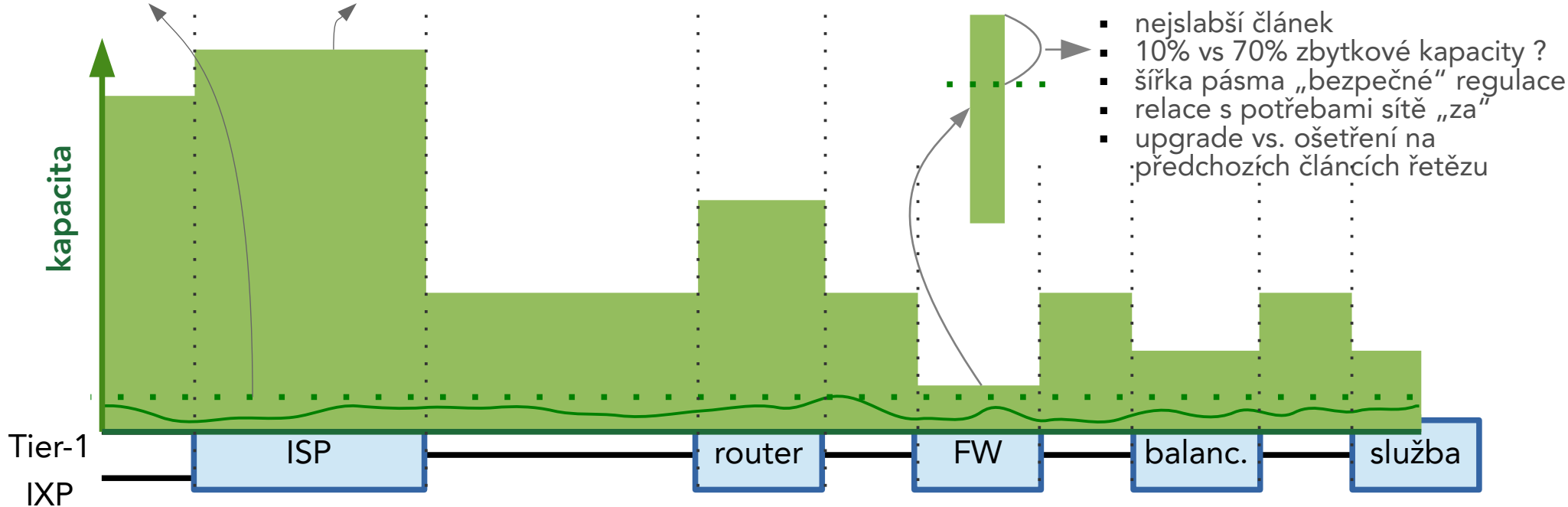
- **zkusme být více důslední..**
- **během celého životního cyklu posuzovat komplexně celý síťový „set-up" k/od služby**
  - **není to o tom, že od začátku musí být vše dokonale zharmonizované, jde o to, že si aktuálně slabé články uvědomujeme, pro jejich řešení/odstranění jsme si nastavili prioritu a strategii** ..vč. toho, že některé můžeme na základě důkladného zvážení akceptovat ~ *ISMS v obecné řeči ;-)*
- **provozně by nám to jako celek mělo fungovat tak**
  - „aby se to pokud možno nikde neucpávalo" (nedocházely zdroje)

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

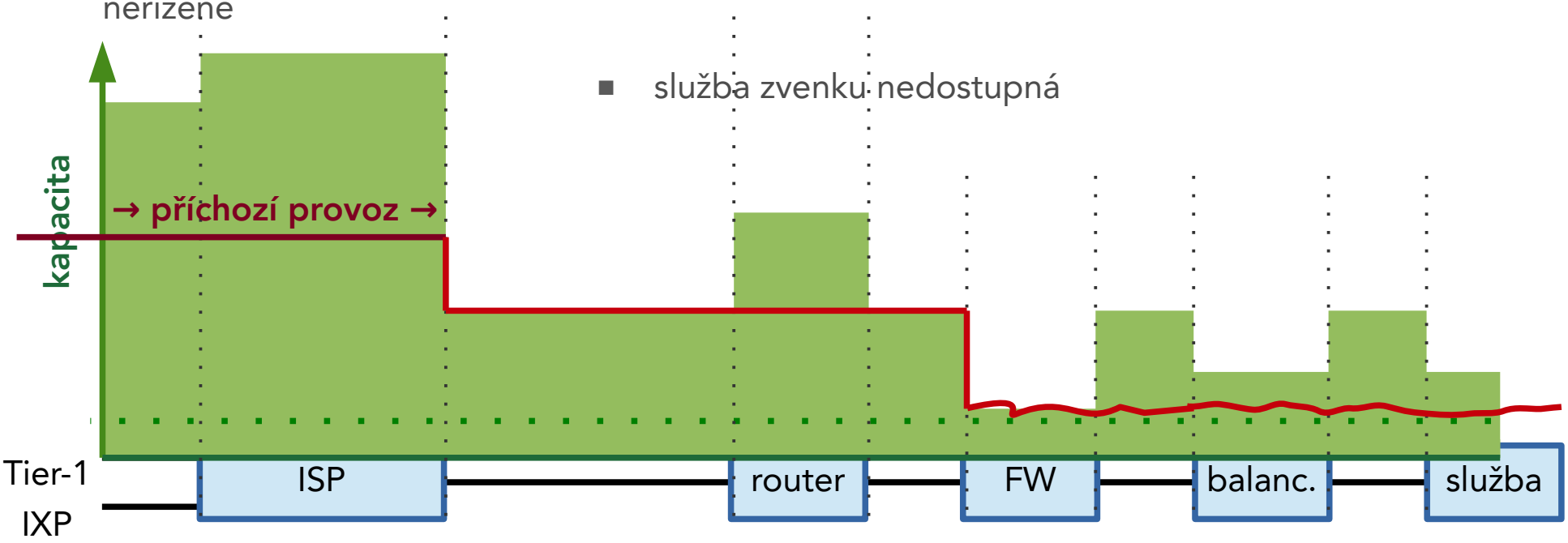
  - **snažíme se dosáhnout strategicky rozložené zátěže při extrémních situací mezi dílčí prvky** + případně posilme příliš slabé (velká relativní odchylka vůči zbytku) články řetězu



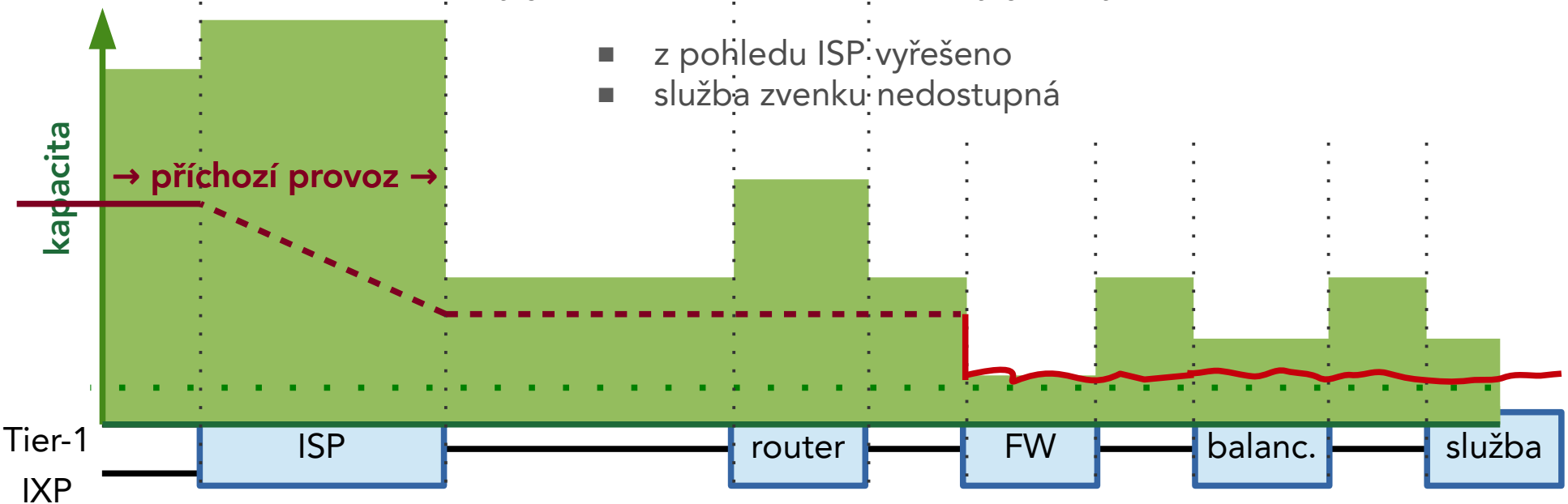
- **síťová kapacita, zdroje**
  - **potřebná** vs. **dostupná kapacita** v jednotlivých částech řetězce v **běžném stavu**



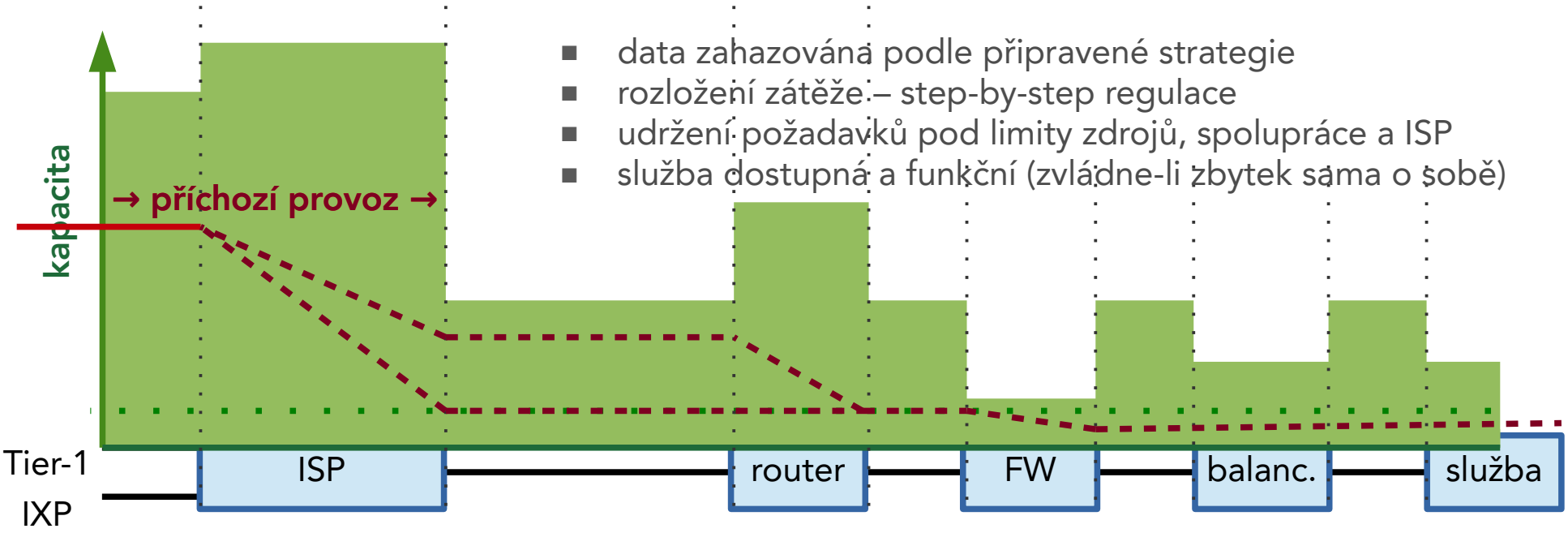
- **síťová kapacita, zdroje**
  - **bez regulace** v **extrémním stavu** (např. volumetrický útok) → data jsou zahazována nahodile, neřízeně
    - služba zvenku nedostupná



- síťová kapacita, zdroje
  - částečná regulace v extrémním stavu – pouze na jednom článku řetězu
  - ISP zabránil „ucpání přípojky“, ale při pohledu na FW stejný stav jako v předchozím případě
    - z pohledu ISP vyřešeno
    - služba zvenku nedostupná



- síťová kapacita, zdroje
  - částečná regulace v **extrémním stavu** – realizace na řetězu prvků



- data zahazována podle připravené strategie
- rozložení zátěže – step-by-step regulace
- udržení požadavků pod limity zdrojů, spolupráce a ISP
- služba dostupná a funkční (zvládne-li zbytek sama o sobě)

Články síťového řetězu

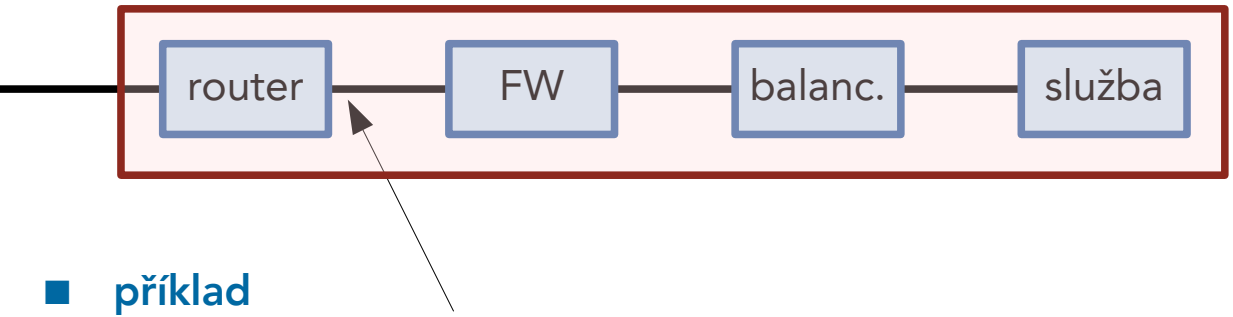
- **typická slabá místa řetězce**
  - **specializované prvky FW, balancery,..**
  - složitá logika, uchování stavových informací apod. → velké nároky na vnitřní zdroje
  - **reálná průchodnost závislá na struktuře provozu**
    - objem provozu
    - velikost paketů
    - transportní protokoly ~ např. počet TCP sessions
    - aplikační protokoly
  - **konfigurace/nastavení ..je velký rozdíl mezi zprovozněním a optimálním nastavením..**

..už zase ty lidské zdroje..

- **monitoring**
- slabá místa ?, dostupnost/nedostupnost zdrojů ? odhad potřebných zdrojů v celém řetězci ?
- **prerekvizita pro dobré nastavení a optimalizaci celé soustavy**
- **bez komplexních informací s odpovídající vypovídací hodnotou pouze tápeme**
- **vypovídací hodnota**
  - způsob, rozsah a místa pozorování monitoringu v relaci s tím, co potřebujeme zjistit
  - vyvážené pokrytí celé hierarchie
    - síťová infrastruktura
    - provoz přenášený sítí
    - koncová aplikace/služba
  - interpretace dat z monitoringu v souladu s parametry monitoringu

Monitoring ~ síťová infrastruktura

- **síťová infrastruktura, ~HW infrastruktura**
  - kde měřit: celý „viditelný“ řetězec, prakticky všechny aktivní prvky sítě
  - jak měřit: snmp, telemetrie, low-level host monitoring



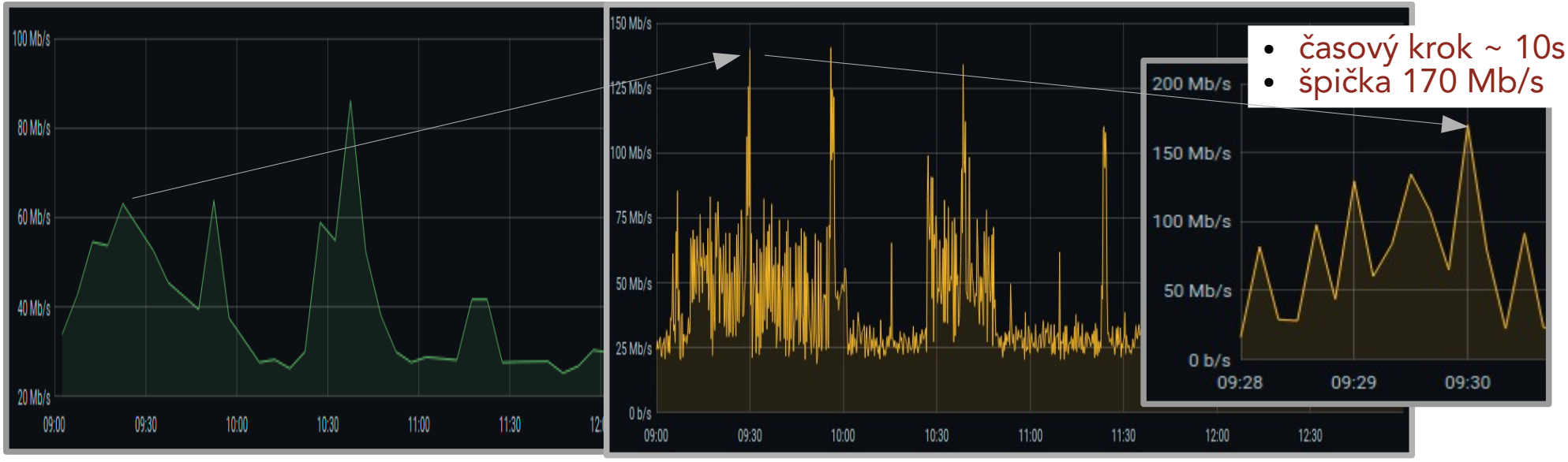
- **příklad**
  - rozhraní směrovače směrem k FW
  - stav a reálně využitá přenosová kapacita, klidový stav → odhad celkové potřebné kapacity
  - **vliv parametrů měření**

- **příklad: vliv časového kroku měření**
  - monitoring využití kapacity linky → využitá přenosová kapacita
  - proč ???

- časový krok měření ~ 6-7 minut
- špička 64 Mb/s, „posun“ v čase

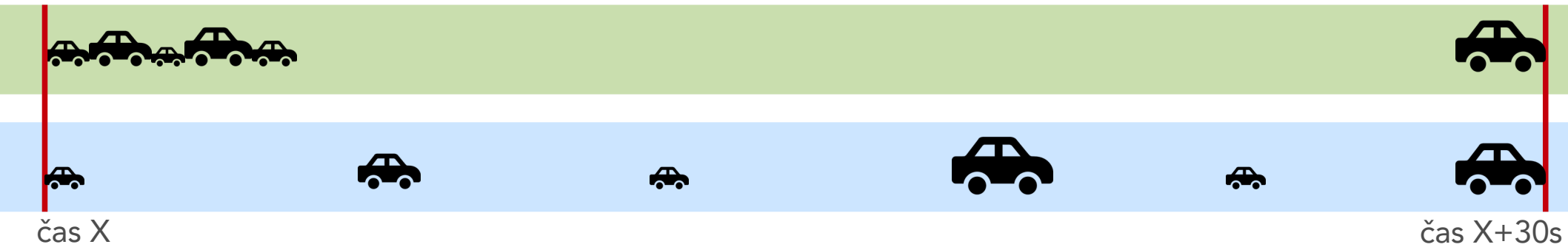
- časový krok ~ 20s
- špička 140 Mb/s

- časový krok ~ 10s
- špička 170 Mb/s



Monitoring ~ síťová infrastruktura

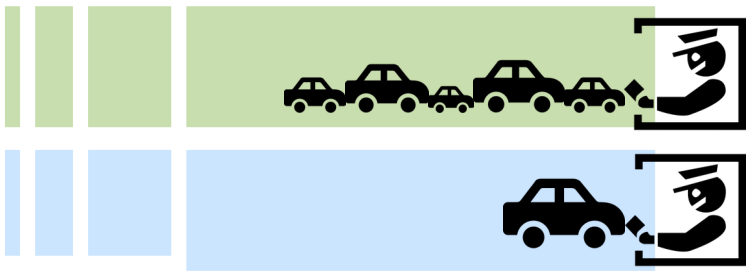
- **příklad: vliv časového kroku měření**
  - technicky získáváme informace o objemu přeneseném mezi dvěma body na časové ose → dvěma po sobě jdoucími „sběry“ monitorovacích dat → z principu jsme schopni vyjádřit pouze průměrné využití mezi dvěma měřeními
  - příklad níže: monitoring s krokem sběru informací 30s → v obou případech stejné využití kapacity → 6 aut za 30s ~ 0.2 auta/s
  - **shluk na lince/silnici nevadí…ale**



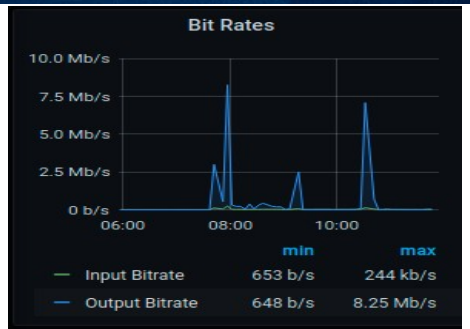
Monitoring ~ síťová infrastruktura

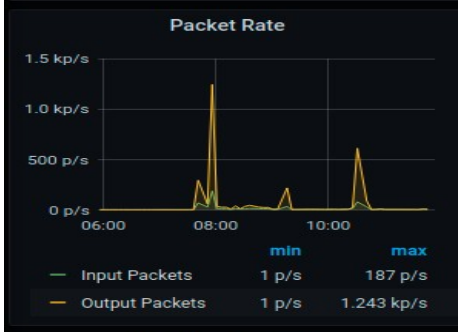
- možný dopad shluku na obslužné místo
  - vznik front, čekání na obsluhu
  - přeplnění vstupní paměti FW apod..

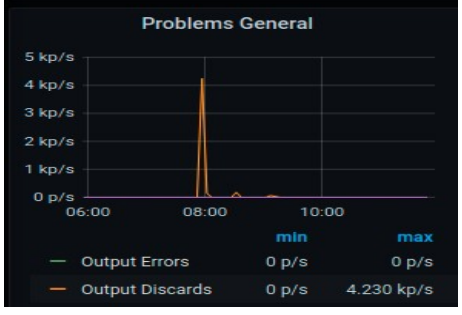
    → zahazování paketů

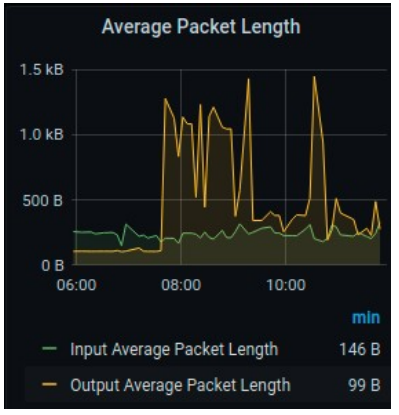


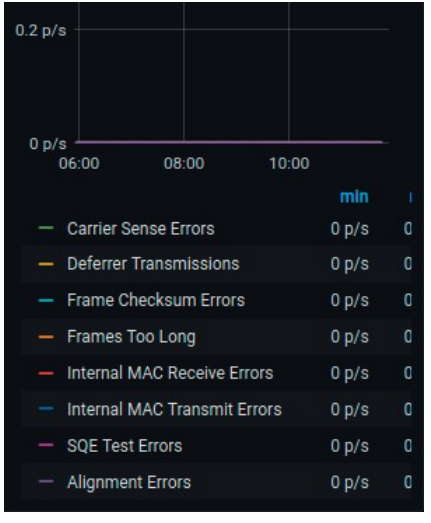
- samotné měření přenesených objemů nestačí
  - je třeba sledovat více parametrů











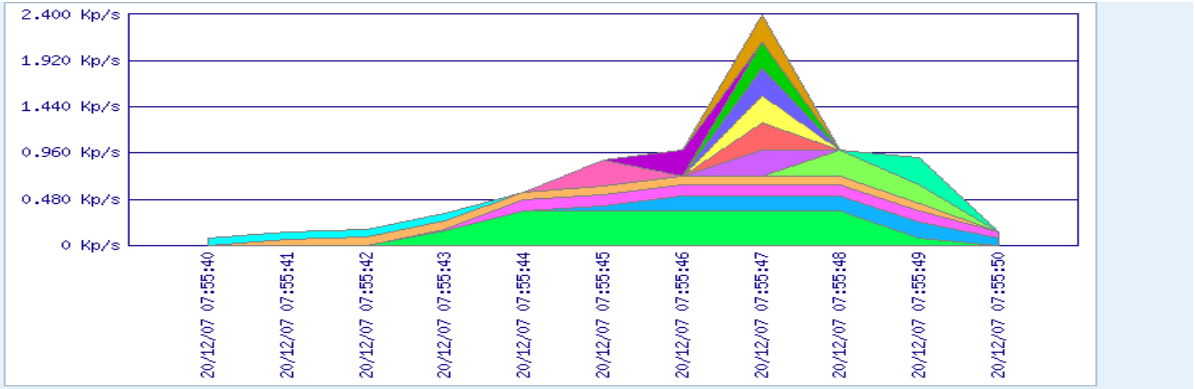
- **provoz přenášený sítí**
  - kde měřit: důležitá místa sítě – perimetr, FW, WLAN přípojka,..
  - jak měřit: monitoring na bázi toků (~ netflow)
  - informace z hlaviček transportních protokolů
    - vyňaté z přenášených paketů, průběžně agregované; které vrstvy ? ; co user data ?

egress	Forwarded not Fragmented	185.8.x.x	195.178.x.x	udp (17)	35506	65432	156	384	0x60000000	0x6000000b
egress	Forwarded not Fragmented	185.8.x.x	195.178.x.x	udp (17)	36069	65535	156	384	0x60000000	0x6000000b
egress	Forwarded not Fragmented	185.8.x.x	195.178.x.x	tcp (6)	49606	mysql (3306)	156	384	0x60000000	0x6000000b
egress	Forwarded not Fragmented	185.8.x.x	195.178.x.x	tcp (6)	49604	mysql (3306)	156	384	0x60000000	0x6000000b
ingress	Forwarded	195.178.x.x	185.8.x.x	tcp (6)	mysql (3306)	49604	384	156	0x6000000b	0x60000000
egress	Forwarded not Fragmented	185.8.x.x	205.220.x.x	icmp (1)	Echo-reply (0)	Port Unreachable (771)	156	384	0x60000000	0x6000000b
ingress	Terminate	2001:718:x:600:x:x:x:x	2001:718:x:600:x:x:x:x	tcp (6)	35168	bgp (179)	384	0	0x6000000b	0x00000000
egress	Forwarded not Fragmented	2001:718:x:600:x:x:x:x	2001:718:x:600:x:x:x:x	tcp (6)	bgp (179)	35168	0	384	0x00000000	0x6000000b
egress	Forwarded not Fragmented	185.8.x.x	195.178.x.x	udp (17)	53874	65533	156	384	0x60000000	0x6000000b

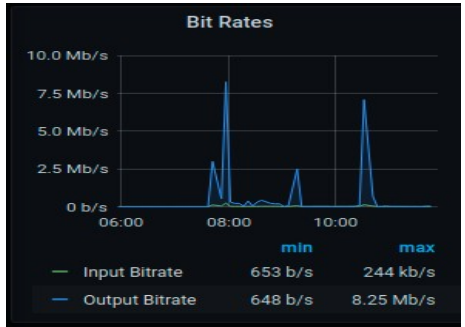
00000000		20/12/07 13:29:15.485	20/12/07 13:38:06.360	5.130 KB	18.000 p
00001000	push(8), ack(16)	20/12/07 13:32:56.659	20/12/07 13:37:57.087	3.300 KB	6.000 p
00001000	push(8), ack(16)	20/12/07 13:28:29.828	20/12/07 13:37:59.872	3.020 KB	40.000 p
00001000	push(8), ack(16)	20/12/07 13:28:30.300	20/12/07 13:38:00.345	2.640 KB	20.000 p
11000000		20/12/07 13:29:08.748	20/12/07 13:37:25.595	1.768 KB	26.000 p
11000000	push(8), ack(16)	20/12/07 13:28:37.563	20/12/07 13:37:39.173	1.390 KB	20.000 p
11000000	push(8), ack(16)	20/12/07 13:28:37.765	20/12/07 13:37:38.972	1.390 KB	20.000 p
00000000		20/12/07 13:35:01.727	20/12/07 13:36:59.200	1.093 KB	4.000 p

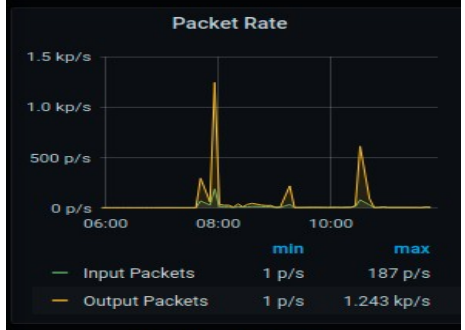
Src-IP	*Dst-IP*	*Src-PostNAT-IP*	*Dst-PostNAT-IP*	*Protocol*	*Src-Port*	*Dst-Port*	*Src-PostNAPTPort*	*Dst-PostNAPTPort*
93.184.x.x	195.113.x.x	93.184.x.x	195.113.x.x	tcp (6)	http (80)	33309	http (80)	33309
77.75.x.x	195.113.x.x	77.75.x.x	195.113.x.x	tcp (6)	https (443)	49708	https (443)	49708
157.240.x.x	195.113.x.x	157.240.x.x	195.113.x.x	tcp (6)	https (443)	44189	https (443)	44189
195.113.x.x	64.233.x.x	195.113.x.x	64.233.x.x	tcp (6)	49583	submissions (465)	49583	submissions (465)
195.113.x.x	173.194.x.x	195.113.x.x	173.194.x.x	tcp (6)	49582	imaps (993)	49582	imaps (993)
157.240.x.x	195.113.x.x	157.240.x.x	195.113.x.x	tcp (6)	https (443)	46130	https (443)	46130
195.113.x.x	88.198.x.x	195.113.x.x	88.198.x.x	tcp (6)	http (80)	58056	http (80)	58056

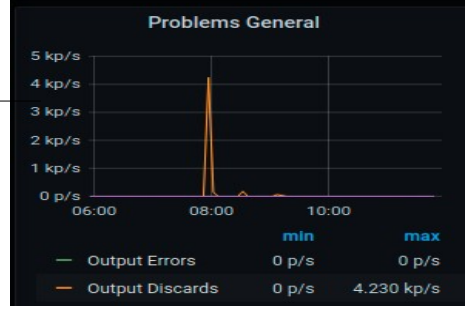
- **simulovaný příklad využití u analýzy dříve zjištěného jevu na jiné vrstvě**
  - co mohlo způsobit výskyt „output discards“ v předchozím příkladu
  - např. přetížení FW pomocí TCP SYN burst



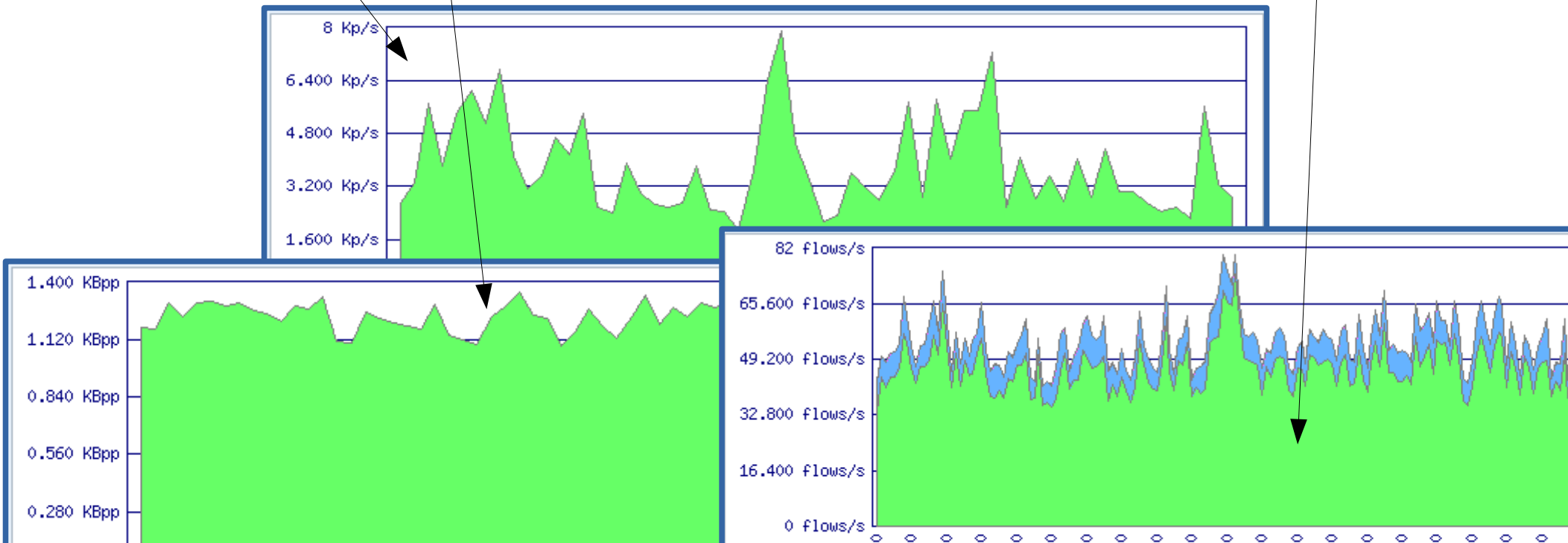
o	>	Flow-Direction	FWD-Status	Src-IP	Protocol	Src-Port	Dst-Port	TOS-flags	TCP-flags	Pkts-estimated
1.	>	ingress	Forwarded	172.x.x.x	tcp (6)	65432	http (80)	00000000	syn(2)	2.000 Kp
2.	>	ingress	Forwarded	172.x.x.x	tcp (6)	65432	http (80)	00000000	syn(2)	1.400 Kp
3.	>	ingress	Forwarded	172.x.x.x	tcp (6)	65432	http (80)	00101000	syn(2)	1000.000 p
4.	>	ingress	Drop RPF	51.x.x.x	tcp (6)	53550	telnet (23)	00000000	syn(2)	720.000 p
5.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	64202	00000000	syn(2)	480.000 p
6.	>	ingress	Forwarded	94.x.x.x	tcp (6)	44128	61016	00000000	syn(2)	320.000 p
7.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	57225	00000000	syn(2)	280.000 p
8.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	59835	00101000	syn(2)	280.000 p
9.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	58536	00101000	syn(2)	280.000 p
10.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	56783	00101000	syn(2)	280.000 p
11.	>	ingress	Forwarded	185.x.x.x	tcp (6)	54874	64607	00000000	syn(2)	280.000 p



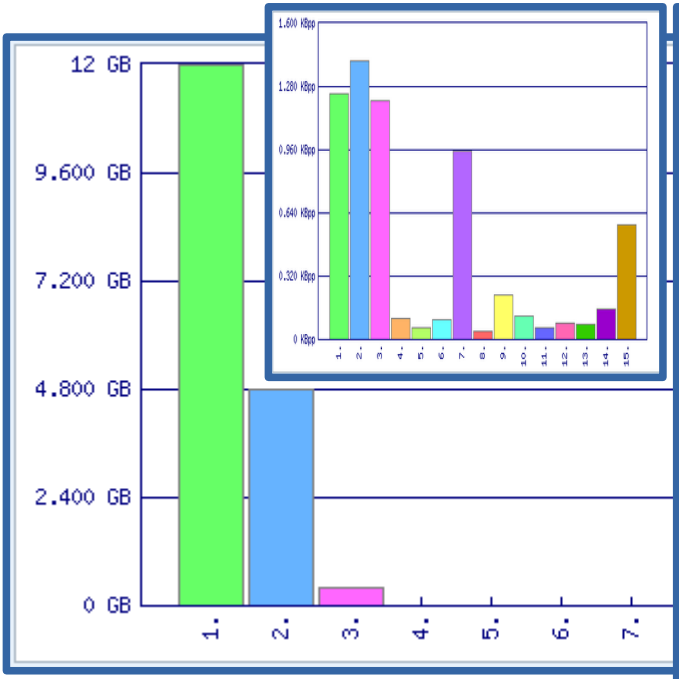




- **dostatečný potenciální výkon FW ?**
  - paketová rychlost, délka paketů, typ transportu (TCP, UDP), počet TCP sessions v případě TCP (analogie s počtem toků v rámci TCP transportu)

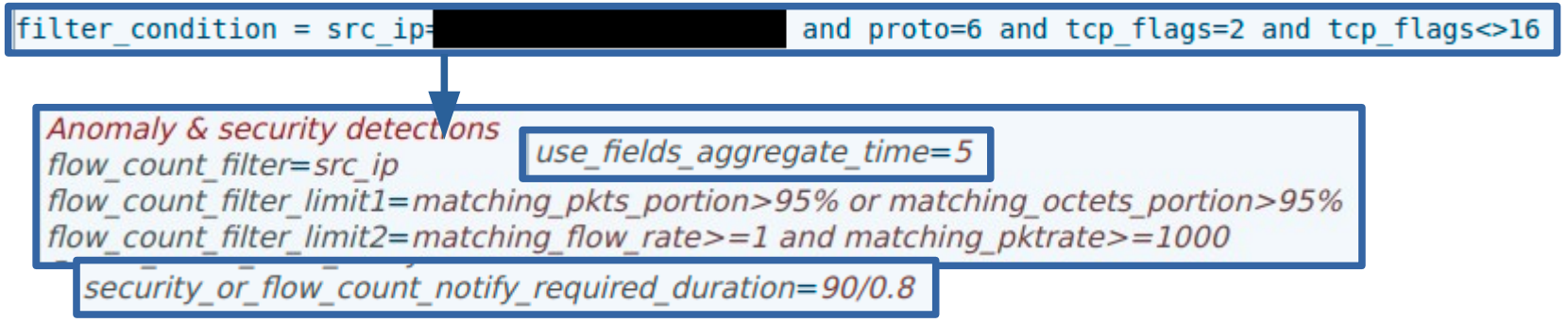


- **obecná charakteristika provozu i detailní analýza na úrovni jednotlivých toků**
  - struktura provozu – protokoly, čísla portů, objemy v „ustáleném“ stavu
  - znalost chování služby, komunikace s podpůrnými službami → optimalizace nastavení



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%

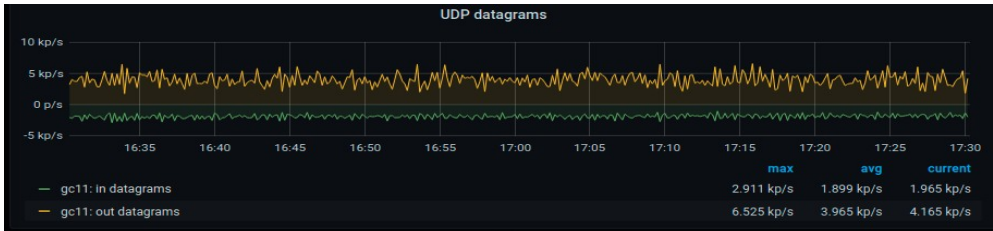
- **vhodné pro detekci základních síťových anomálií**
  - princip vzniku na bázi agregace základních parametrů toku z protokolárních hlaviček
  - agresivní/dlouhodobé scany, amplifikační útoky
  - příklad principu detekce na bázi technologických limitů – nestandardní výskyt konkrétního jevu

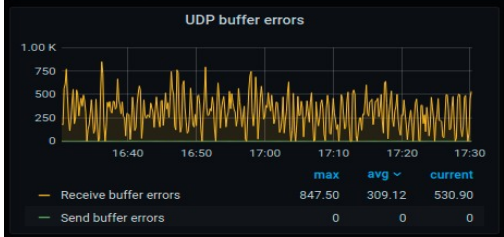


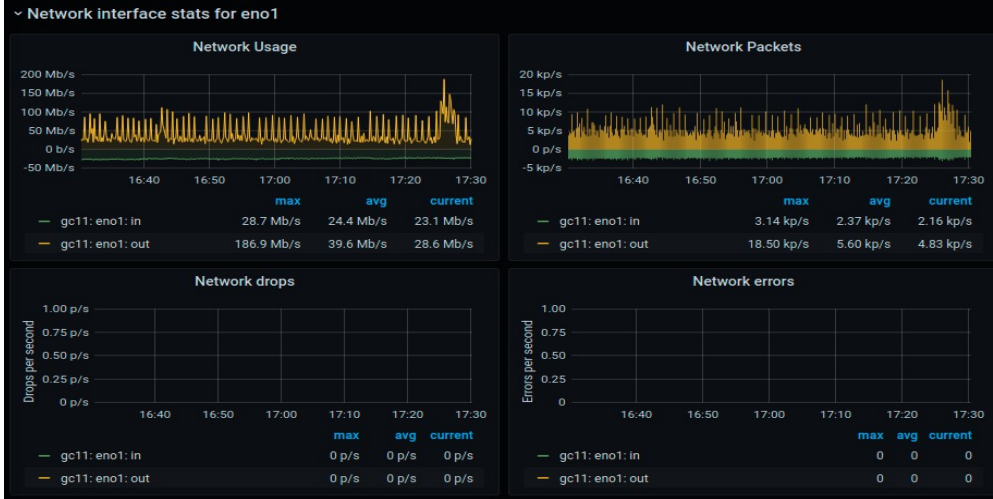
  - vs. např. tzv. behaviorální detekce ~ matematicky výjádřené průměrné chování vs. odchylky
  - vhodnost metod ← charakter provozu ~ cílové prostředí (ISP, data-centrum, e-shop, e-infrastruktura)
  - možná automatizace – provázání s regulačními mechanismy (RTBH, BGP FlowSpec, přesměrování na čistící infrastrukturu apod.)

- **služba – HW hostitele, OS, aplikace, podpůrné služby...**
  - detailní monitoring OS, požadavky na zdroje, CPU, mem, storage, síťový stack, systémové logy, ...limitery, on host FW, aplikační logy, … - asi netřeba blíže rozebírat..

- služba – HW hostitele, OS, aplikace, podpůrné služby…

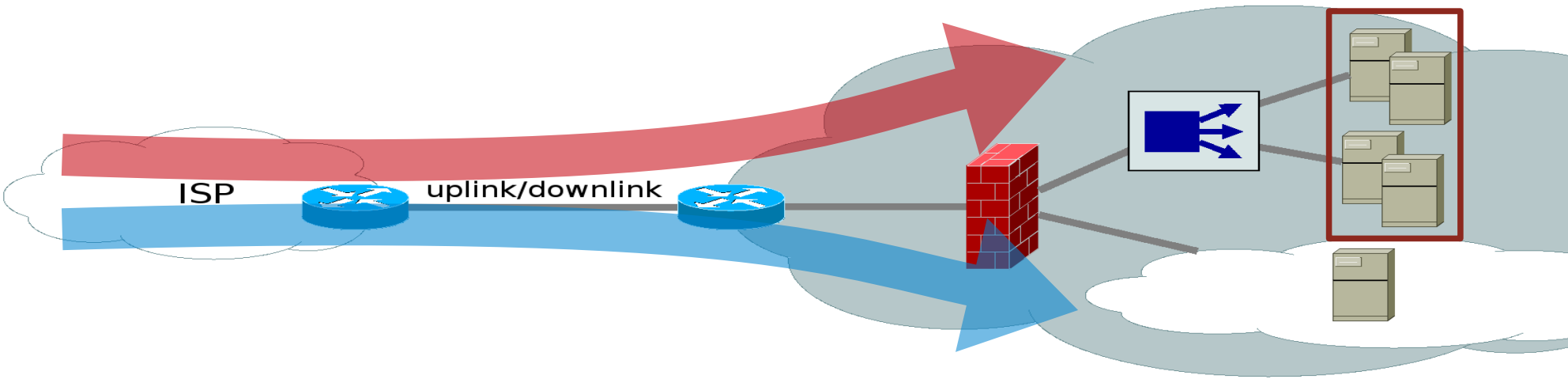






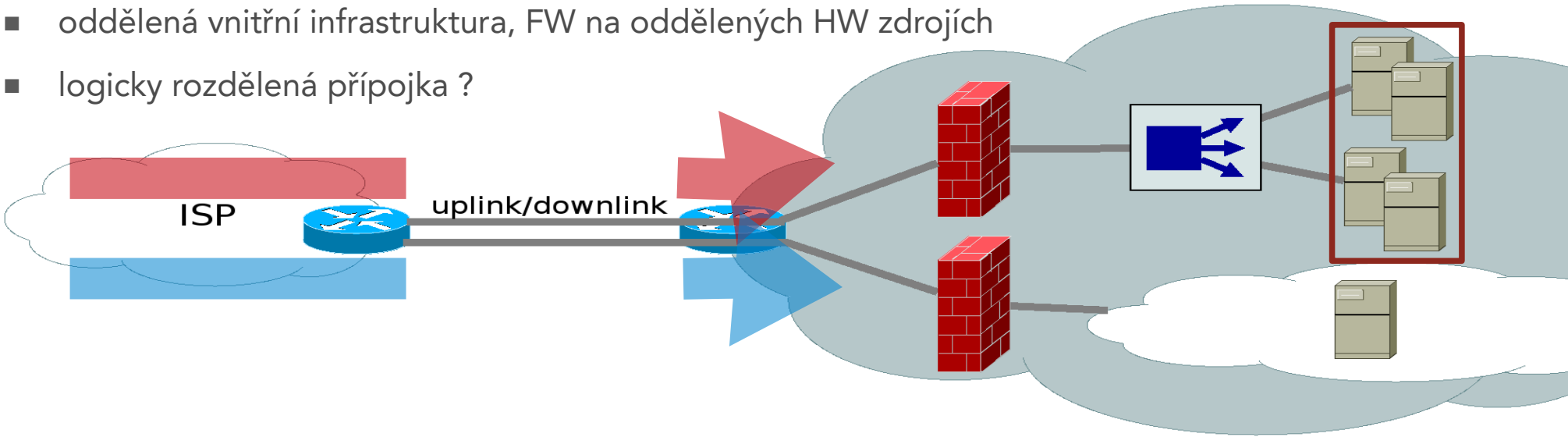
Síťová architektura připojení kritické služby

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



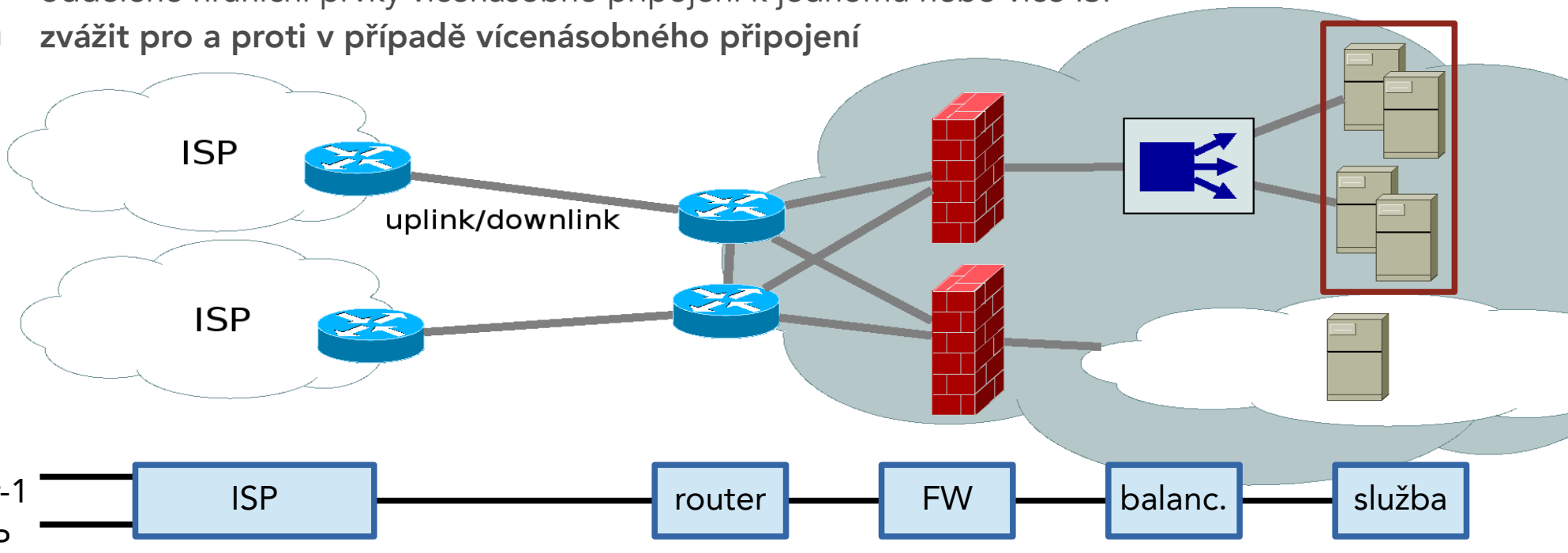
Síťová architektura připojení kritické služby

- **topologie**
  - zmenšení vlivu okolí a sdílení zdrojů
  - oddělená vnitřní infrastruktura, FW na oddělených HW zdrojích
  - logicky rozdělená přípojka ?



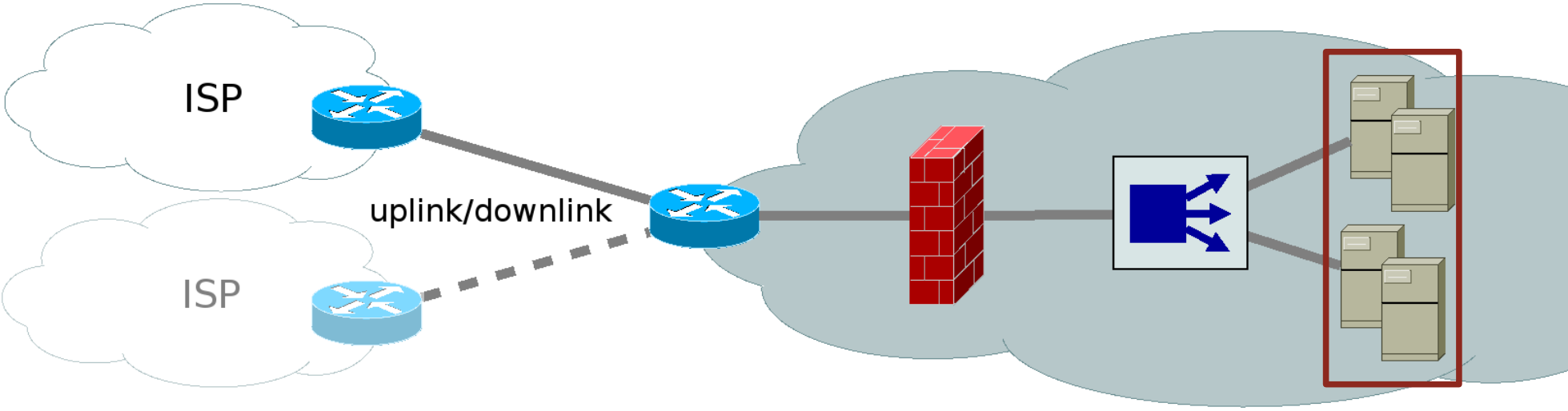
Síťová architektura připojení kritické služby

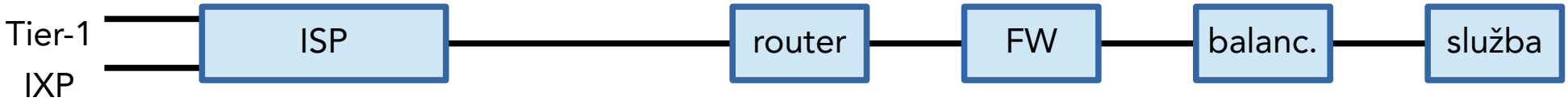
- **topologie**
  - zmenšení vlivu okolí a sdílení zdrojů
  - oddělené hraniční prvky vícenásobné připojení k jednomu nebo více ISP
  - **zvážit pro a proti v případě vícenásobného připojení**



Síťová architektura připojení kritické služby

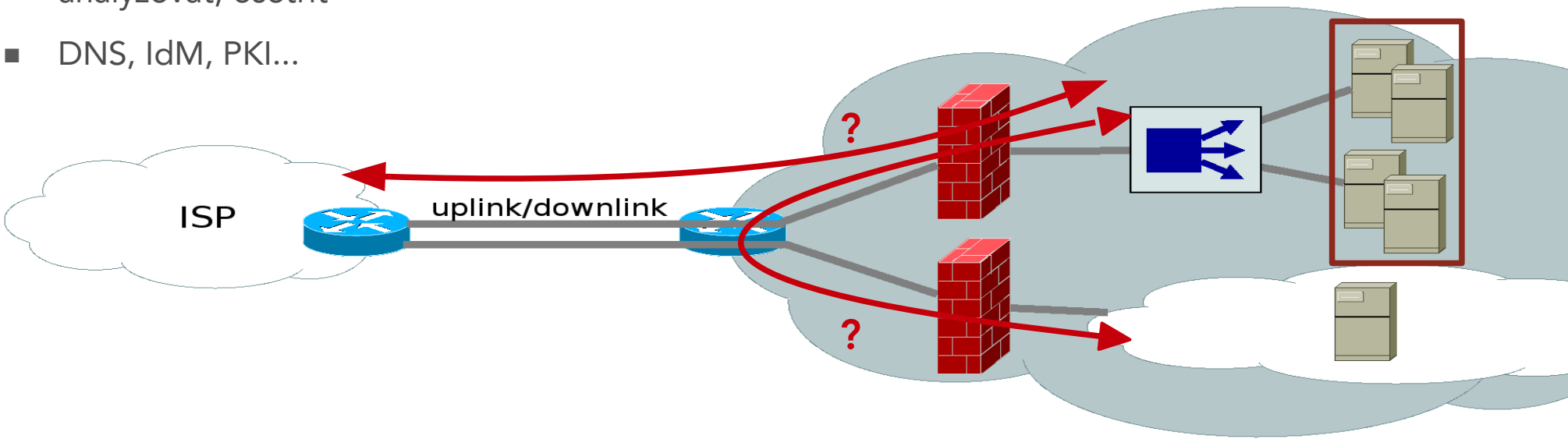
- **topologie**
  - samostatná síť pro službu

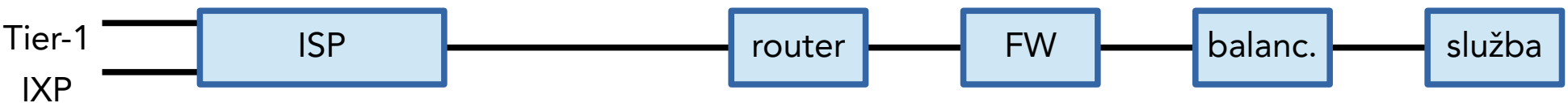




Síťová architektura připojení kritické služby

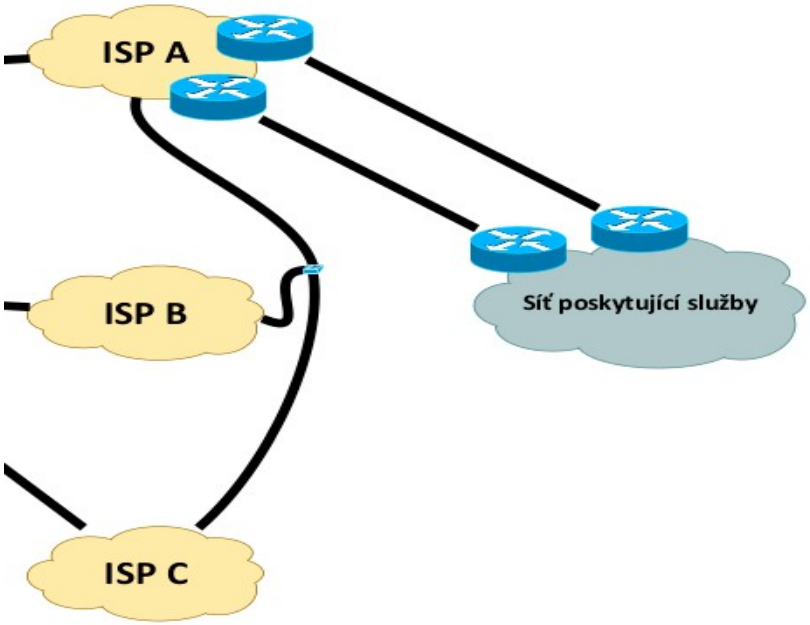
- **pozor na závislosti na dalších službách**
  - analyzovat, ošetřit
  - DNS, IdM, PKI...

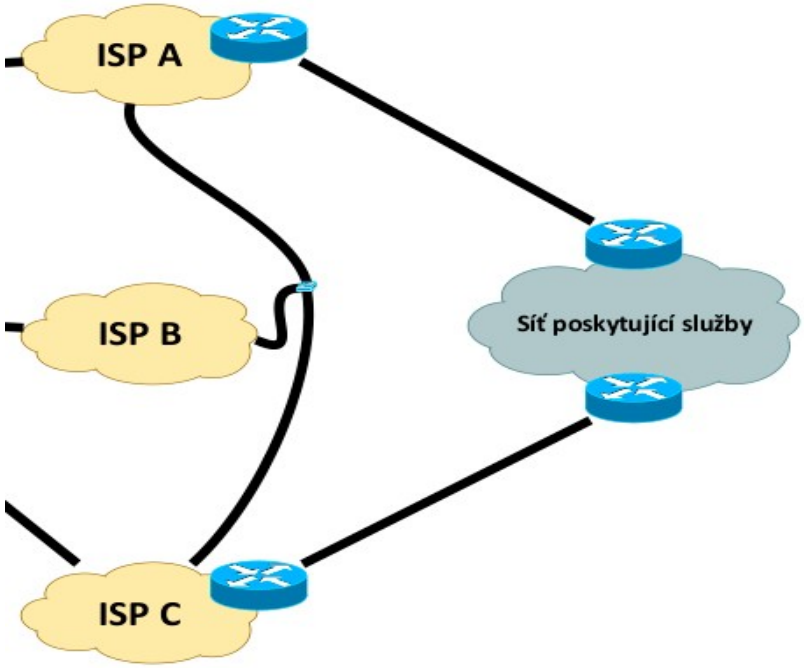




Vícenásobné připojení koncové sítě

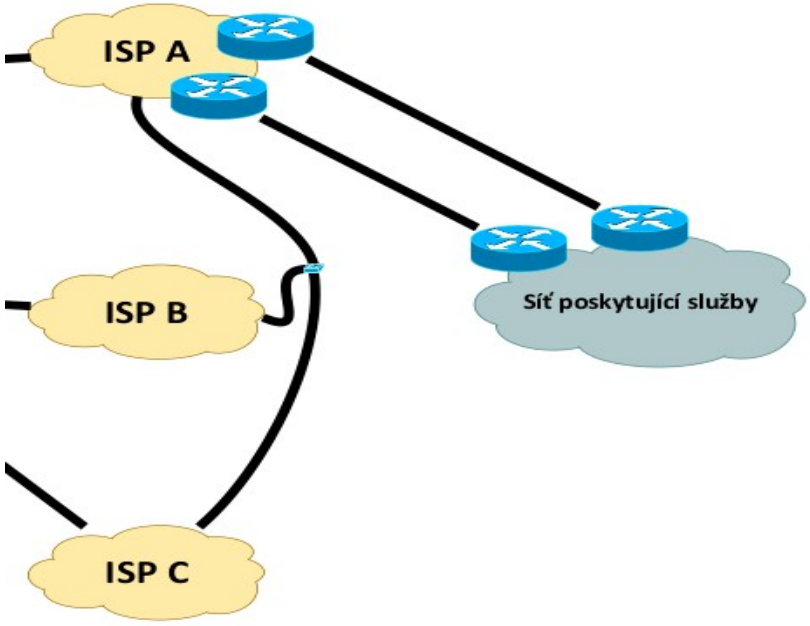
- **vícenásobné připojení**
  - zvýšení dostupnosti, při jednoduché chybě bez výpadku, možnost přesměrování při plánovaných odstávkách
    - k jednomu vs. více poskytovatelům





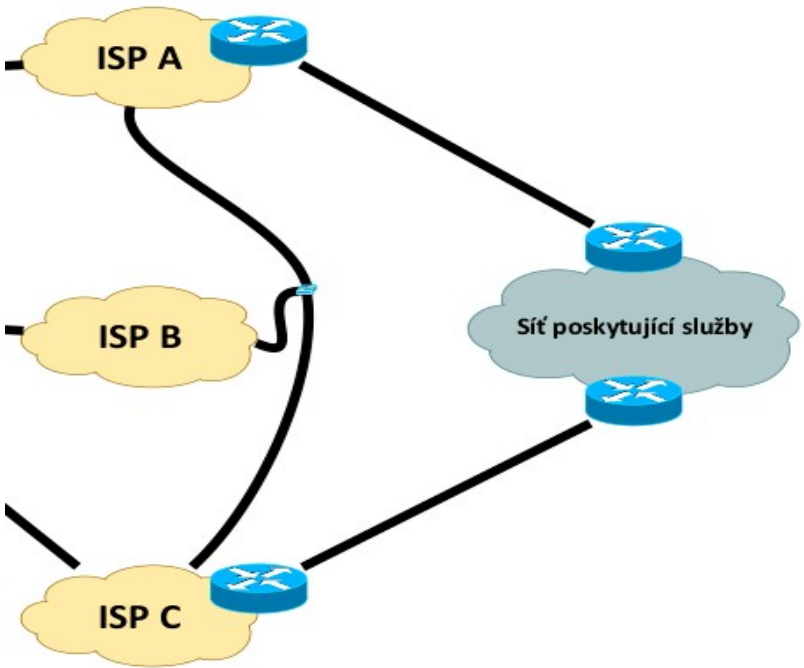
Vícenásobné připojení koncové sítě

- **vícenásobné připojení k jednomu poskytovateli**
- výhody
  - komunikace pouze s jedním partnerem
  - není nutné mít vlastní IP adresy
  - směrovací protokol nemusí být BGP (byť je nejvýhodnější)
  - snadné dosažení symetrie provozu
  - možnost domluvy s poskytovatelem na odstranění nežádoucího provozu
- nevýhody
  - v případě problémů v síti poskytovatele není alternativa – nutno počkat na jejich vyřešení



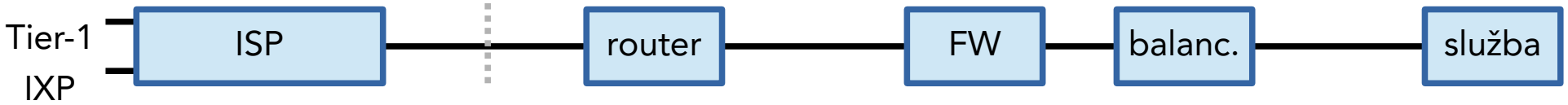
Vícenásobné připojení koncové sítě

- **vícenásobné připojení k více poskytovatelům**
- výhody
  - v případě problémů v síti jednoho poskytovatele je možné přelít provoz jinudy
- nevýhody
  - zvýšení administrativy - RIPE a další poskytovatel
  - je nutné získat vlastní IP adresy
  - směrovací protokol pouze BGP
  - potenciální asymetrie provozu – obtížná regulace dráhy příchozího provozu
  - zvýšení nákladů
    - RIPE (registrace + roční poplatek ~ € 2k + € 1,4K)



Architektura připojení pro kritické služby a sítě

- **možná opatření**



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

- *filtrace provozu*
- *rate limit policy*
  - *zahození/označení*
- *čištění provozu*
- *RTBH*
- *obecné – transportní síť*

- *filtrace provozu*
- *rate limit policy*
- *znalost cílové infrastrukury*

- *filtrace provozu*
  - *+detail, stav ?*
- *vyvážení provozu ke službě*
- *znalost cílového prostředí/služby*

- *on-host FW*
- *response-rate limiter*
- *...*
- *znalost cílové aplikace*

Shrnutí

- **1. proaktivně - optimalizace nastavení/konfigurace**
  - komplexní pohled → rozdělení na komponenty → konkrétní opatření respektující souvislosti
  - podmínky pro samostatné ošetření jednotlivých služeb
  - znalost služby + analýza provozu → stanovení priorit provozu + rozložení úkolů mezi články soustavy → implementace + ověření funkce (testy) => **nové nastavení/konfigurace**
  - strategie pro extrémní případ → „řízené ztráty“
- **2. reaktivně - v případě útoků**
  - východiskem je odzkoušené funkční nastavení dle 1.
  - kontrola/řízení nastavených funkcí dle strategie
  - aktivně (kreativně) se věnujeme tomu, co jsme nedokázali predikovat
  - po skončení útoku vyhodnotíme efektivitu implementované strategie → zpět na začátek ;-)
- **periodicky**
  - revize, optimalizace nastavení/konfigurace ~ 1.

Strategické úvahy

- **vše předchozí směřovalo ke zvýšení odolnosti infrastruktury**
  - *...a bylo zaměřené především na technickou stránku věci*
  - *..nejen technologická infrastruktura..*
  - před-nastavení celého organismu + akceschopnost v případě mimořádné situace
  - zabezpečení dat ~ strategie a způsob zálohování (off-line)
  - komunikační nástroje ~ primární, záložní *(nezávislé na vlastní infrastruktuře)*
  - procesy/rozdělení práce ~ organizovaná činnost vs. všichni všechno → nikdo nic *..cvičme..testujme se..*
  - **<u>lidské zdroje, lidské zdroje, lidské zdroje</u>**
    - máme je vůbec / jsme schopni je získat / zaplatit ? a jaké ? kvalita/kvantita ? osobnostní mix ?
    - efektivita využití ?
    - expertiza/know-how, zástupnost ?
    - krizový tým ?
  - spolupráce s ISP
  - ...a spousta dalších...

cesnet

Děkuji za pozornost...