ISP Gateway

Karel Řeřicha

Poslední revize: 13.9.2018

UNITEDNETWORKS

Co je ISP Gateway?

- software pro rozdělování konektivity mezi zákazníky
- kompletní řešení pro PoP

Co umí ISP Gateway?

- rozdělovat konektivitu :)
- monitorovat prvky sítě a sledovat síťový provoz
- chránit síť proti DoS a DDoS útokům
- Data Retention
- realtime napojení na existující CRM

UNITEDNETWORKS

Co řeší ISP v rámci provozování telekomunikační sítě:

I. Kvalita služby

- “rozumné” rozdělování konektivity zákazníkům
- prioritizace provozu
- ochrana proti zahlcení přípojek
- ochrana proti útokům

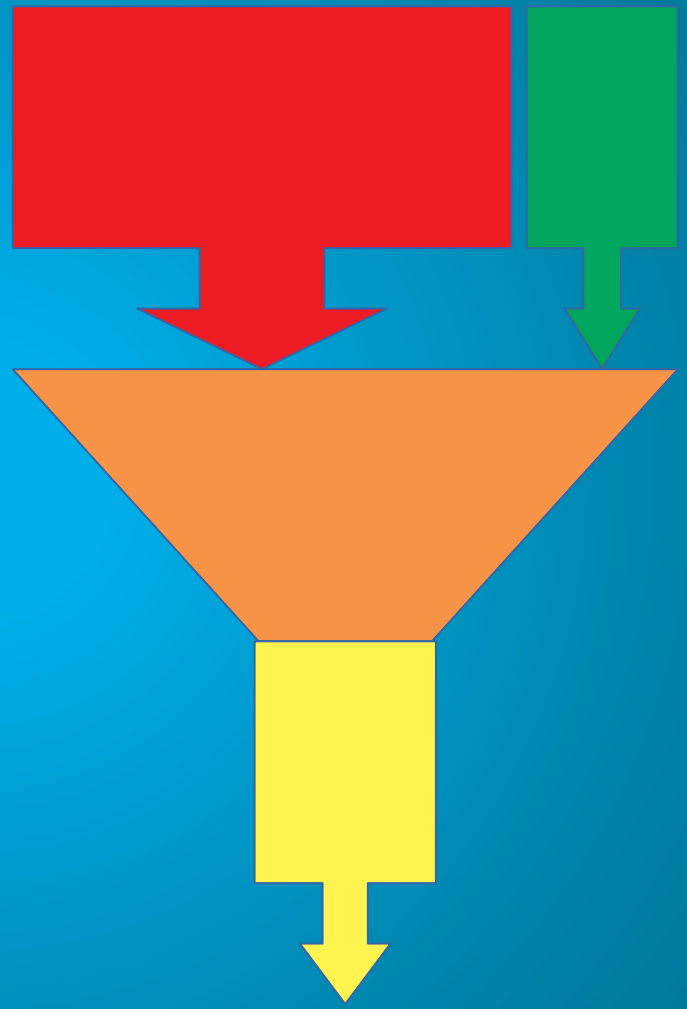
II. Monitoring sítě

- sledování latencí a jitteru
- accounting
- Data Retention

UNITEDNETWORKS

Rozdělování konektivity

co nejvyšší rychlosti
vs
úzká místa



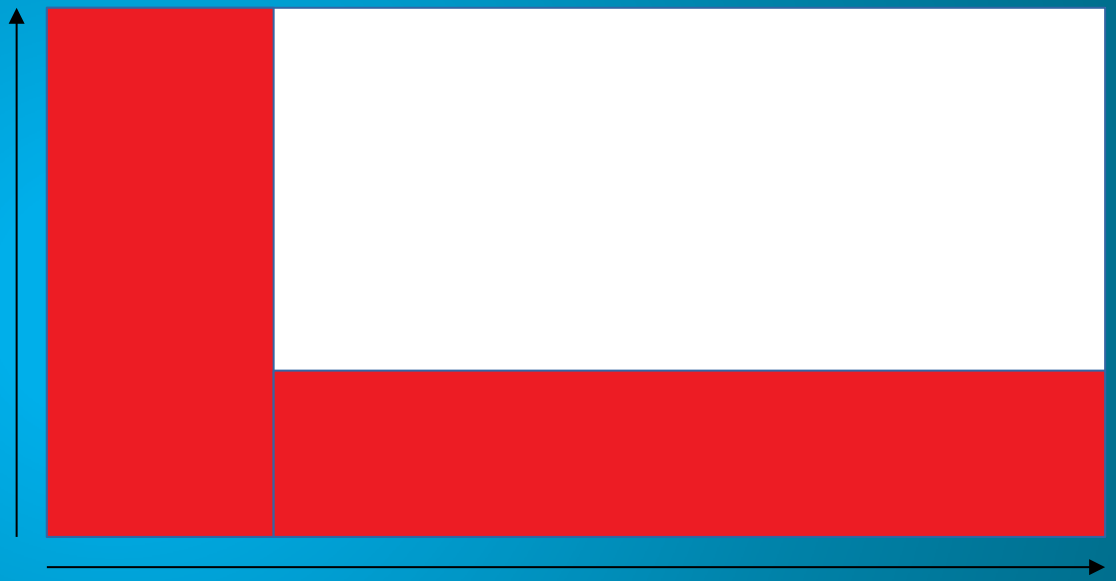
Jak řešit?

- omezit rychlosti - nechceme
- pracovat se šířkou pásma
  v závislosti na čerpání

UNITEDNETWORKS

A. Snížení rychlosti při vysokém čerpání

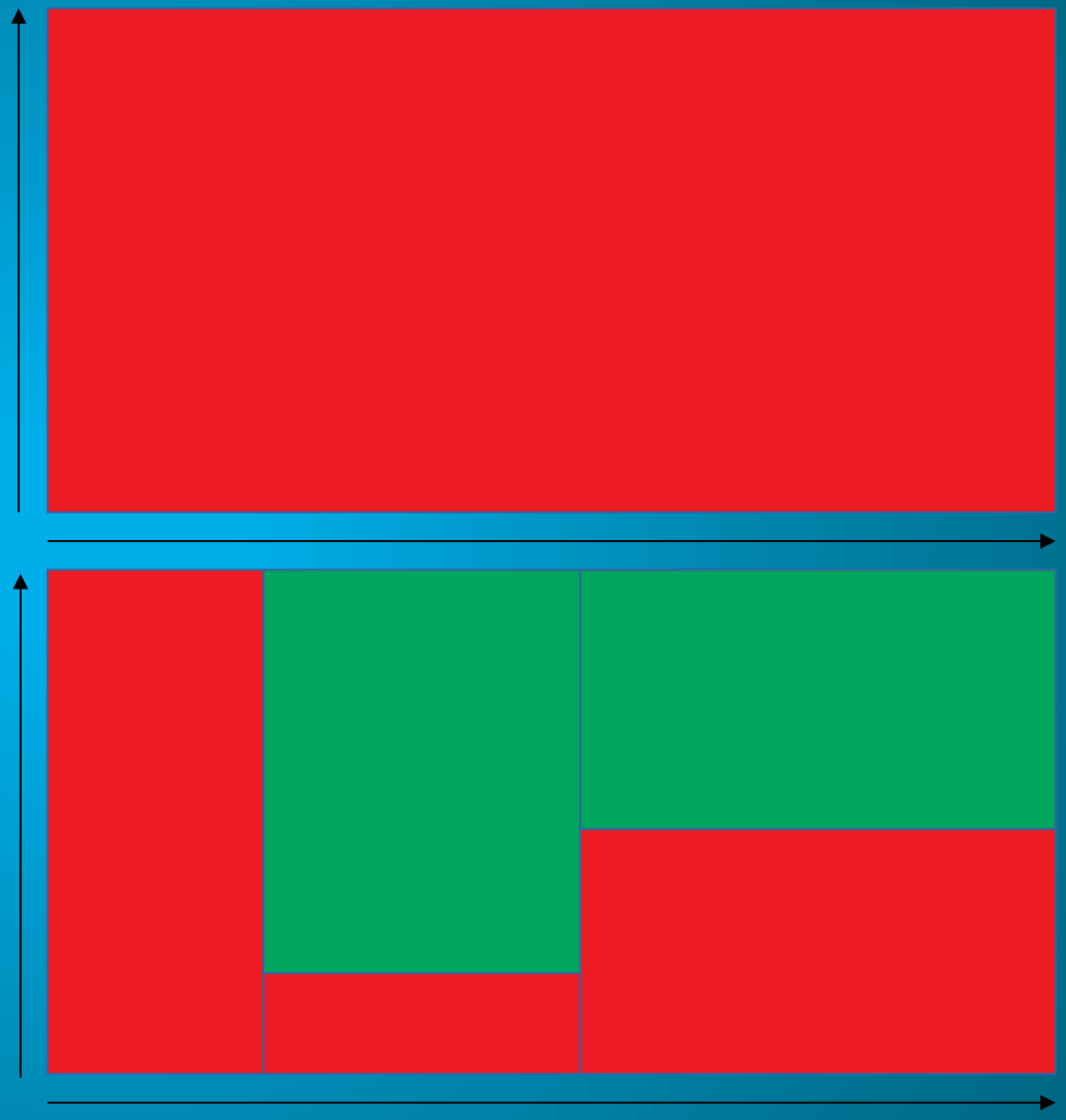
- při nevyužité lince zbytečné



UNITEDNETWORKS

B. Snížení priority při vysokém čerpání

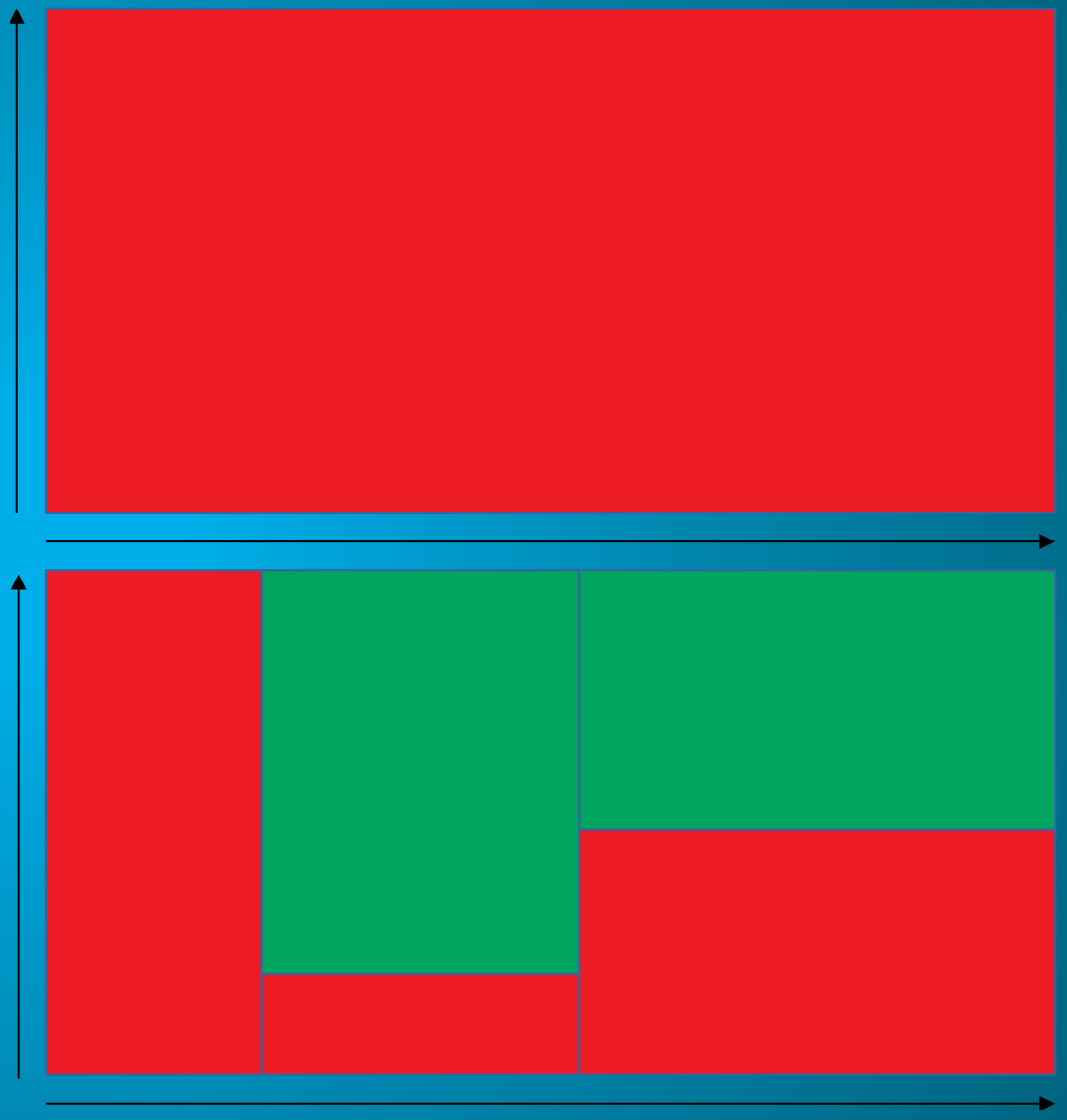
- celková kapacita je neustále využita
- zákazník vždy dostane na začátku čerpání výrazně vyšší podíl na kapacitě linky



UNITEDNETWORKS

B. Snížení priority při vysokém čerpání

- celková kapacita je neustále využita
- zákazník vždy dostane na začátku čerpání výrazně vyšší podíl na kapacitě linky
- nutno mezit kapacitou přípojného bodu



Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

STROM SLUŽEB

+ Přidat skupinu + Přidat službu

Vyhledávání

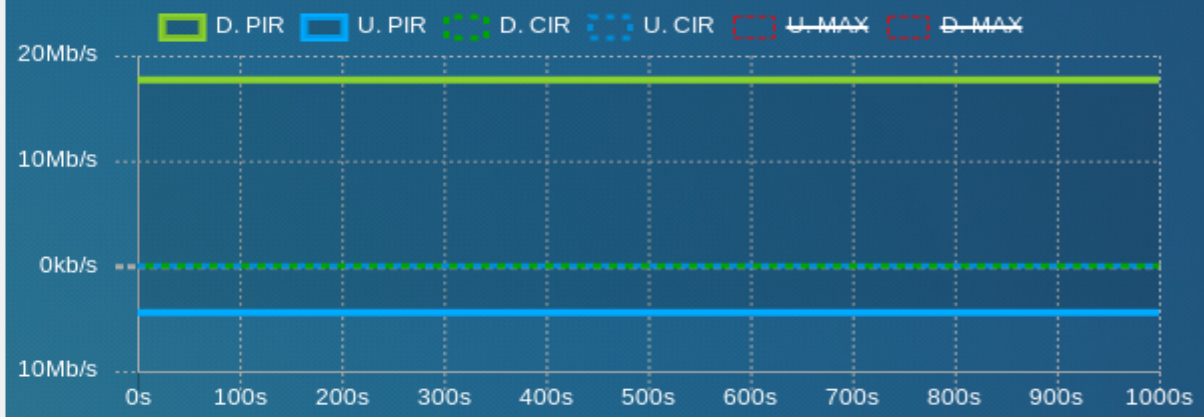
- 5GCIMICEVOD_UN2AC (2)
- 5GCIMICEVOD_UN3AC (4)
- 5GCIMICE_UN1AC (2)
- 5GCINOV_MAXTEL1 (9)
- 5GDOBRSIN (5)
- 5GDOMARAZ1N (6)
- 5GDOMARAZ2N (24)
- 5GDOMORAZ1 (10)
- 5GDOMORAZ3N (20)
- 5GDRAZOVICE (1)
- 5GDRAZOVICEN (15)
- **5GDUCHODAK (10)**
- 5GDUCHODAK2 (6)
- 5GFRVES_UN1N (8)
- 5GHARTMANICE (16)
- 5GHARTMANICE138_UN_1AC (0)
- 5GHARTMANICE138_UN_2AC (0)
- 5GHARTMANICE1AC (11)
- 5GHARTMANICE2 (7)
- 5GHARTMANICE3 (10)
- 5GHARTMANICE5 (14)
- 5GHARTMANICE_MAXTEL1D (16)
- 5GHARTMANICE_MAXTEL1N (13)
- 5GHARTMANICE_MAXTEL2D (11)
- 5GHDGARAZ2 (3)
- 5GHMB (20)
- 5GHMB1 (4)

Název služby: 5GDUCHODAK

20Mb half duplex pro 802.11a a 802.11g v rate 36Mbit

Tarif: Speciální

ID služby:	100291	**Délka burstu:**	0s
Typ služby:	default	**Priorita při burstu:**	100%
Služba/Skupina:	false	**Priorita po burstu:**	100%



Příchozí provoz (kbps)	
Maximální propustnost při burstu	0
Vyhrazená propustnost při burstu	0
Propustnost	17694
Vyhrazená propustnost	0

Odchozí provoz (kbps)	
Maximální propustnost při burstu	0
Vyhrazená propustnost při burstu	0
Propustnost	4424
Vyhrazená propustnost	0

Upravit Smazat

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

Přehled / Strom služeb

STROM SLUŽEB

Home / 5GDUCHODAK / DivisovaPrikopy_

+ Přidat skupinu | + Přidat službu

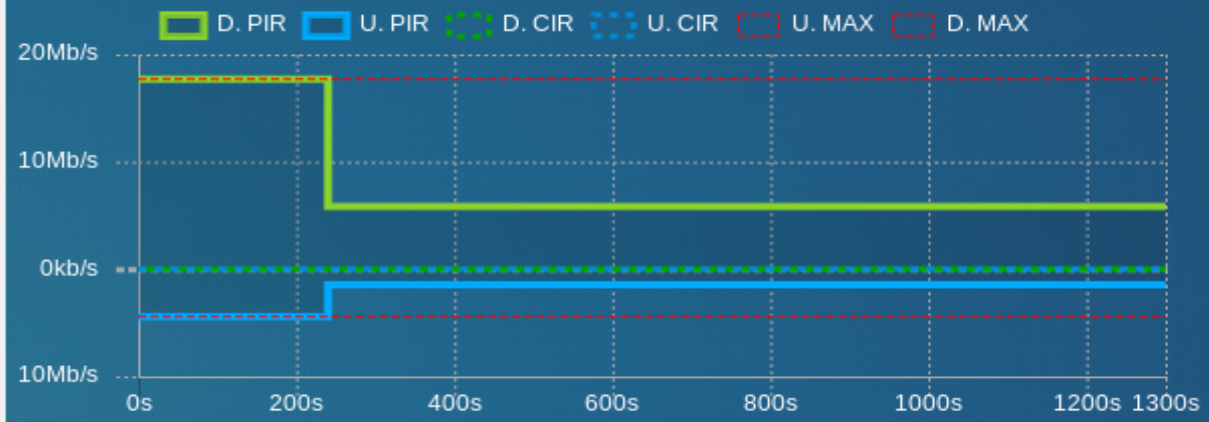
Vyhledávání

- 5GCIMICEVOD_UN2AC (2)
- 5GCIMICEVOD_UN3AC (4)
- 5GCIMICE_UN1AC (2)
- 5GCINOV_MAXTEL1 (9)
- 5GDOBRSIN (5)
- 5GDOMARAZ1N (6)
- 5GDOMARAZ2N (24)
- 5GDOMORAZ1 (10)
- 5GDOMORAZ3N (20)
- 5GDRAZOVICE (1)
- 5GDRAZOVICEN (15)
- 5GDUCHODAK (10)
  - **DivisovaPrikopy_**
  - pichlerovadlouhoveska_1
  - szvitkova_namsvobody_1
  - svrculaprikopy_2
  - jelinekfrantisek_1
  - krupar_1
  - kosmas_fialka_1
  - troblova_namsvobody50_1
  - almokhalalati_americkearmady86_1
- 5GDUCHODAK2 (6)
- 5GFRVES_UN1N (8)
- 5GHARTMANICE (16)
- 5GHARTMANICE138_UN_1AC (0)
- 5GHARTMANICE138_UN_2AC (0)

Název služby: DivisovaPrikopy_

Tarif: Speciální

ID služby:	2465	**Délka burstu:**	240s
Typ služby:	prio3	**Priorita při burstu:**	50%
Služba/Skupina:	false	**Priorita po burstu:**	25%



Příchozí provoz (kbps)	
Maximální propustnost při burstu	17694
Vyhrazená propustnost při burstu	0
Propustnost	5839
Vyhrazená propustnost	0

Odchozí provoz (kbps)	
Maximální propustnost při burstu	4424
Vyhrazená propustnost při burstu	0
Propustnost	1460
Vyhrazená propustnost	0

Upravit | Smazat

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

Přehled / Strom služeb

Služby jsou určené především ke specifikaci parametrů propustnosti připojení koncového zákazníka. Lze k nim přiřadit IP adresy, ale nemohou obsahovat další podřazené skupiny či služby.

UPRAVIT SLUŽBU

Název: DivisovaPrikopy_

Předdefinovaný tarif / Nový speciální tarif

-- vyberte tarif --

Typ prioritizace

Popis

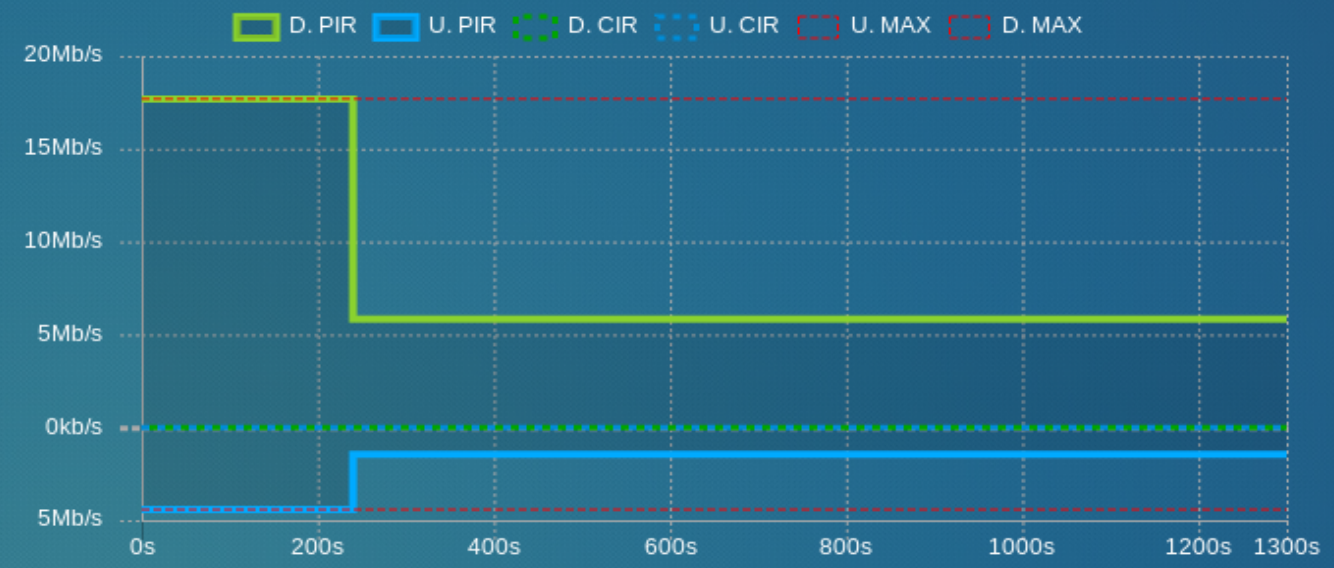
Maximální příchozí propustnost při burstu: 17694 kb/s

Vyhrazená příchozí propustnost při burstu: 0 kb/s

Priorita při burstu: 50%

Vyhrazená odchozí propustnost při burstu: 0 kb/s

Maximální odchozí propustnost při burstu: 4424 kb/s



Maximální příchozí propustnost: 5839 kb/s

Vyhrazená příchozí propustnost: 0 kb/s

Priorita po burstu: 25%

Vyhrazená odchozí propustnost: 0 kb/s

Maximální odchozí propustnost: 1460 kb/s

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

Přehled / Strom služeb

Služby jsou určené především ke specifikaci parametrů propustnosti připojení koncového zákazníka. Lze k nim přiřadit IP adresy, ale nemohou obsahovat další podřazené skupiny či služby.

UPRAVIT SLUŽBU

Název: DivisovaPrikopy_

Předdefinovaný tarif / Nový speciální tarif: -- vyberte tarif --

Typ prioritizace:

Popis:

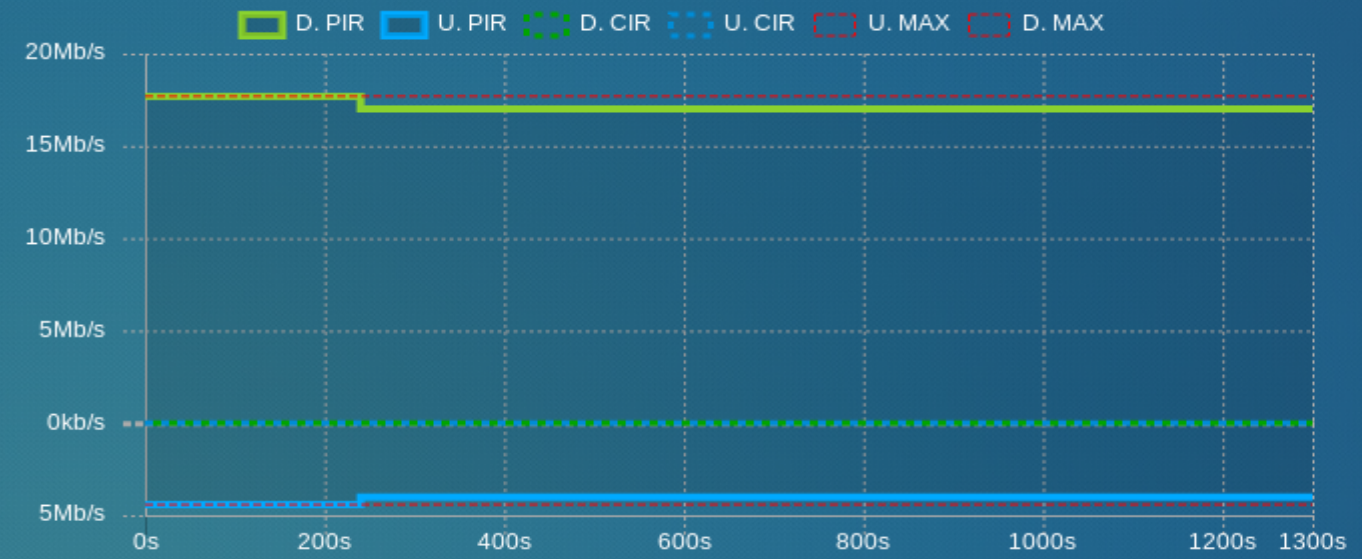
Maximální příchozí propustnost při burstu: 17694 kb/s

Vyhrazená příchozí propustnost při burstu: 0 kb/s

Priorita při burstu: 50%

Vyhrazená odchozí propustnost při burstu: 0 kb/s

Maximální odchozí propustnost při burstu: 4424 kb/s



Maximální příchozí propustnost: 17000 kb/s

Vyhrazená příchozí propustnost: 0 kb/s

Priorita po burstu: 25%

Vyhrazená odchozí propustnost: 0 kb/s

Maximální odchozí propustnost: 4000 kb/s

UNITEDNETWORKS

Prioritizace provozu

zákazník čerpá maximální přidělenou kapacitu

=

nárůst latencí, služby citlivé na latence přestávají fungovat

Jak řešit?

- prioritizovat provoz :)
- několik stupňů prioritizace

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Prioritizace paketů
Konfigurační soubory
Uživatelé
Systém

tcphighprio - Vysoká priorita dle cílového TCP portu
udphighprio - Vysoká priorita dle cílového UDP portu
tcpoverdefprio - Střední priorita dle cílového TCP portu
udpoverdefprio - Střední priorita dle cílového UDP portu
addrhighprio - Vysoká priorita dle cílové IP adresy
addroverdefprio - Střední priorita dle cílové IP adresy

PRIORITIZAČNÍ SETY

- **tcphighprio** 16
- udphighprio 13
- tcpoverdefprio 13
- udpoverdefprio 12
- addrhighprio 14
- addroverdefprio 0

TCPHIGHPRIO

Port ▲	Akce
	+ Přidat
161	
162	
2000	
2001	
2002	
22	
23	

UNITEDNETWORKS

Ochrana před zahlcením

- prioritizace nevyřeší všechno
- je třeba zahlcení aktivně předcházet

Jak řešit?

FQ_CoDel

- rozdělí heuristicky provoz do mnoha toků a v těch se snaží udržet maximální latenci 5 ms, tím radikálně snižuje vzájemné ovlivňování služeb
- pokud se blíží zahlcení v daném toku, nastaví ECN

UNITEDNETWORKS

Monitoring sítě

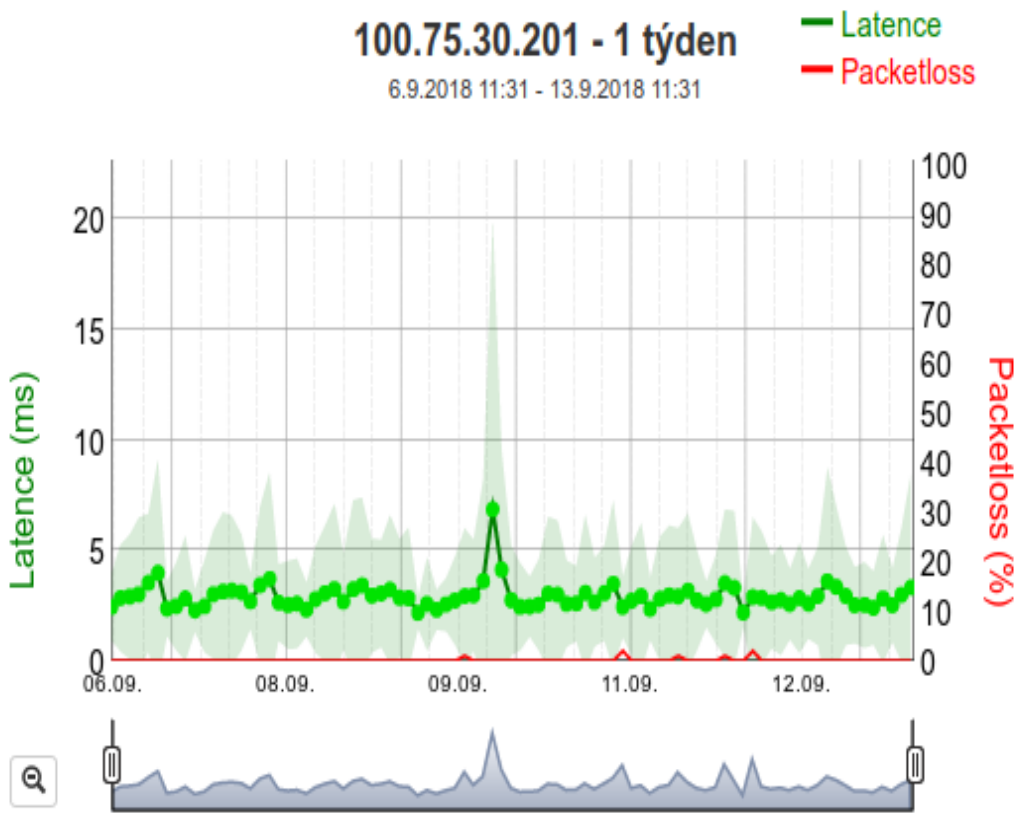
- předcházení problémů
- včasné řešení problémů
- analýza historických dat

Co monitorujeme?

- latence na všechny cíle
- alerty na nedostupnost, zvýšení latencí, změny jitteru
- provoz na všechny cíle

NMS Ping - 100.75.30.201

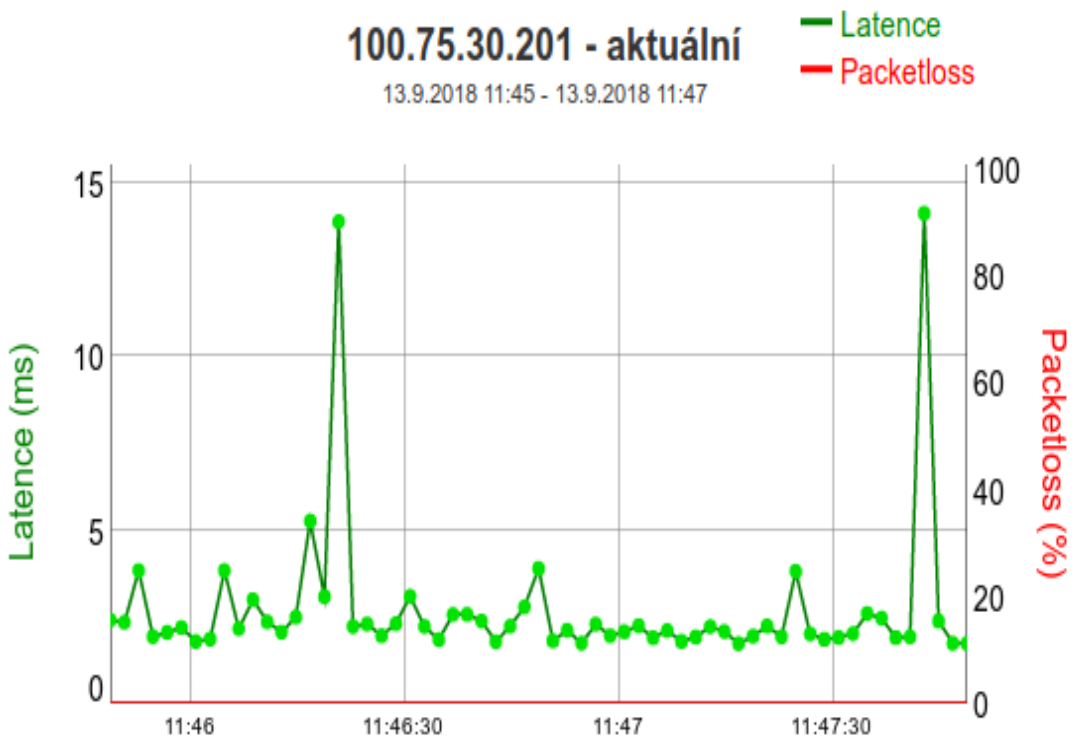
← Zpět | → Znovu | 1 den | 1 týden | 1 měsíc | 1 rok | ‹ Vlevo | › Vpravo



	avg	min	max
Latence:	2.916 ms	1.841 ms	18.283 ms
Packetloss:	0 %	0 %	20 %

Packetloss legend:
<3% | <10% | <30% | <40% | <50% | <90% | 90% - 100%

Interval: 2 s Timeout: 2 s Paketů: 1 ✔ Změnit



	avg	min	max
Latence:	2.601 ms	1.661 ms	28.870 ms
Packetloss:	0 %	0 %	100 %

Packetloss legend:
<3% | <10% | <30% | <40% | <50% | <90% | 90% - 100%

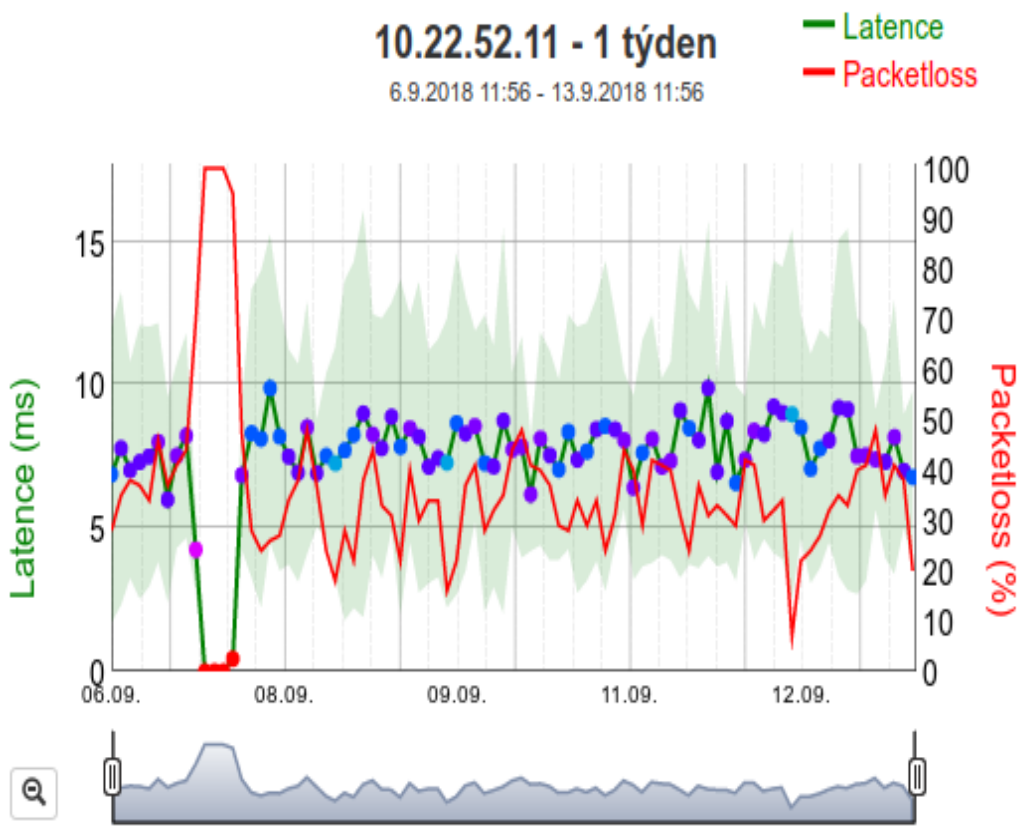
KABEL_ZALESI (1)

Příchozí provoz (kbps)

Odchozí provoz (kbps)

NMS Ping - 10.22.52.11

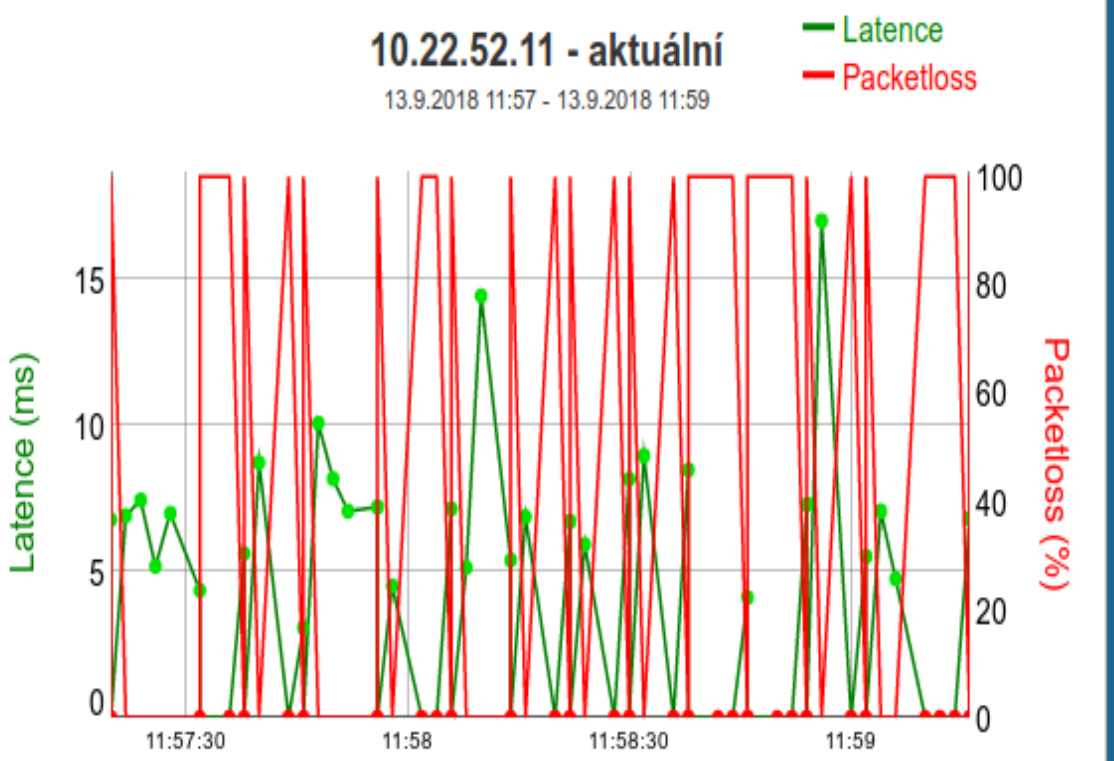
Zpět | Znovu | 1 den | 1 týden | 1 měsíc | 1 rok | Vlevo | Vpravo



	avg	min	max
Latence:	7.934 ms	2.032 ms	21.725 ms
Packetloss:	33 %	0 %	80 %

Packetloss legend:
<3% | <10% | <30% | <40% | <50% | <90% | 90% - 100%

Interval: 2 s Timeout: 2 s Paketů: 1 Změnit

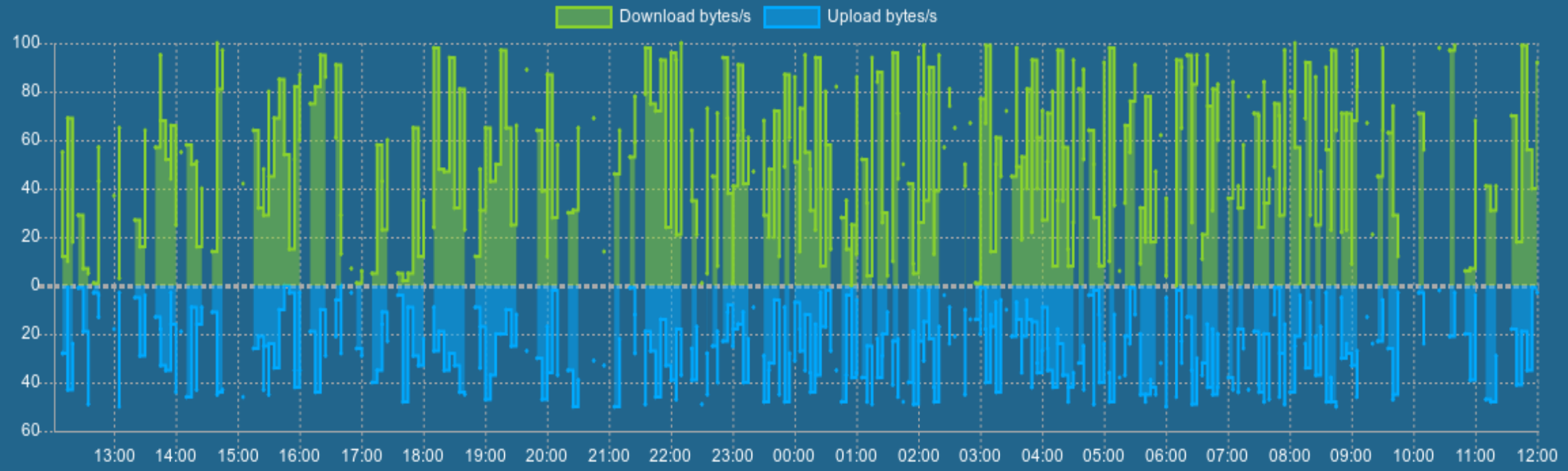


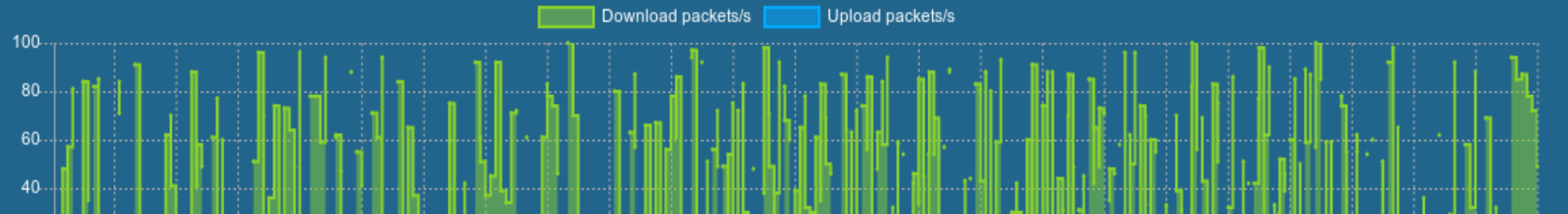
	avg	min	max
Latence:	4.009 ms	0.000 ms	16.982 ms
Packetloss:	45 %	100 %	100 %

Packetloss legend:
<3% | <10% | <30% | <40% | <50% | <90% | 90% - 100%

IP Accounting - 10.22.52.11

Den | Týden | Měsíc | Rok





UNITEDNETWORKS

Ochrana proti DoS a DDoS útokům

RTBH (Remotely Triggered Black Hole)
vs
blokování specifického provozu

Jak funguje blokování specifického provozu?

- analýza veškerého provozu na předdefinované znaky
- různé druhy akcí (alertů) dle úrovně výskytu znaku
- automatické i manuální blokování a odblokování

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Vyhledávání toků
DoS a DDoS útoky
Blokování útoků
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

POSLEDNÍ DETEKOVANÉ ÚTOKY

Datum a čas	Útok	Popis	Provedené akce	Limit detekce	Časový limit (s)
13.09.2018 11:08:25	tcp: 10.64.68.10:? -> ?.?.?.?:7078	TCP SYN DOS attacks from source IP address to destination port	log, block, event	500/0.1s (500.6)	1h0s
13.09.2018 11:08:25	tcp: ?.?.?.?:? -> 43.227.183.70:7078	TCP SYN DDOS attacks to destination IP address and port	log, block, event	500/0.1s (500.6)	1h0s
13.09.2018 11:07:39	tcp: 10.64.68.10:? -> ?.?.?.?:7078	TCP SYN DOS attacks from source IP address to destination port	log, block, event	500/0.1s (500.75)	1h0s
13.09.2018 11:07:39	tcp: ?.?.?.?:? -> 43.227.183.70:7078	TCP SYN DDOS attacks to destination IP address and port	log, block, event	500/0.1s (500.75)	1h0s
13.09.2018 11:07:11	tcp: 10.64.68.10:? -> ?.?.?.?:7078	TCP SYN DOS attacks from source IP address to destination port	log, block, event	500/0.1s (500.42)	1h0s
13.09.2018	tcp: ?.?.?.?:? -> 43.227.183.70:7078	TCP SYN DDOS attacks to destination IP address and	log, block, event	500/0.1s	1h0s

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Vyhledávání toků
DoS a DDoS útoky
Blokování útoků
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

ddostcpsport - DDoS útok přes TCP protokol z portu na IP adresu
ddostcpdport - DDoS útok přes TCP protokol na port a IP adresu
ddosudpsport - DDoS útok přes UDP protokol z portu na IP adresu
ddosudpdport - DDoS útok přes UDP protokol na port a IP adresu
ddosprotocol - DDoS útok přes protokol (ICMP, GRE, IGMP, OSPF, IPIP, SCTP) na IP adresu

dostcpsport - DoS útok přes TCP protokol z IP adresy a portu
dostcpdport - DoS útok přes TCP protokol za IP adresy na port
dosudpsport - DoS útok přes UDP protokol z IP adresy a portu
dosudpdport - DoS útok přes UDP protokol za IP adresy na port
dosprotocol - DoS útok přes protokol (ICMP, GRE, IGMP, OSPF, IPIP, SCTP) z IP adresy

TYPY BLOKOVÁNÍ

- **ddostcpdport** 1
- ddostcpsport 0
- ddosudpdport 0
- ddosudpsport 0
- ddosprotocol 0
- dostcpdport 1
- dostcpsport 0
- dosudpdport 0
- dosudpsport 0
- dosprotocol 0

DDOSTCPDPORT

IP adresa	Port ▲	Timeout (s)	Akce
			+ Přidat
43.227.183.70	7078	16m37s880ms/1h	

ISP Gateway

- Přehled
- Strom služeb
- Tarify
- Mapování a sety
- Neznámé IP adresy
- Statistika paketů
- Správa provozu
- Tabulka konexí
- Log
- Dokumentace
- Nastavení
- Systém

Přehled / Strom služeb

STROM SLUŽEB

+ Přidat skupinu | + Přidat službu

Vyhledávání

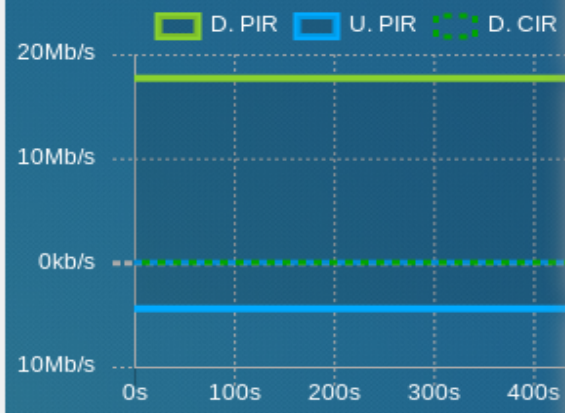
- 5GCIMICEVOD_UN2AC (2)
- 5GCIMICEVOD_UN3AC (4)
- 5GCIMICE_UN1AC (2)
- 5GCINOV_MAXTEL1 (9)
- 5GDOBRSIN (5)
- 5GDOMARAZ1N (6)
- 5GDOMARAZ2N (24)
- 5GDOMORAZ1 (10)
- 5GDOMORAZ3N (20)
- 5GDRAZOVICE (1)
- 5GDRAZOVICEN (15)
- **5GDUCHODAK (10)**
- 5GDUCHODAK2 (6)
- 5GFRVES_UN1N (8)
- 5GHARTMANICE (16)
- 5GHARTMANICE138_UN_1AC (0)
- 5GHARTMANICE138_UN_2AC (0)
- 5GHARTMANICE1AC (11)
- 5GHARTMANICE2 (7)
- 5GHARTMANICE3 (10)
- 5GHARTMANICE5 (14)
- 5GHARTMANICE_MAXTEL1D (16)
- 5GHARTMANICE_MAXTEL1N (13)
- 5GHARTMANICE_MAXTEL2D (11)
- 5GHDGARAZ2 (3)
- 5GHMB (20)
- 5GHMB1 (4)

Název služby:

20Mb half duplex pro 802.11a a 802.11g v ra

Tarif: S

ID služby:	100291
Typ služby:	default
Služba/Skupina:	false



Příchozí provoz (kbps)	
Maximální propustnost při burstu	0
Vyhrazená propustnost při burstu	0
Propustnost	17694
Vyhrazená propustnost	0

Vyhrazená propustnost při burstu	0
Propustnost	4424
Vyhrazená propustnost	0

Upravit | Smazat

Netflow - útok
TCP SYN DOS attacks from source IP address to destination port
tcp: 10.64.68.10:? -> ?.?.?.?:8040

Netflow - útok
TCP SYN DDOS attacks to destination IP address and port
tcp: ?.?.?.?:? -> 183.131.200.196:8040

Netflow - útok
TCP SYN DOS attacks from source IP address to destination port
tcp: 10.64.68.10:? -> ?.?.?.?:8040

Netflow - útok
TCP SYN DDOS attacks to destination IP address and port
tcp: ?.?.?.?:? -> 183.131.200.196:8040

Netflow - útok
TCP SYN DOS attacks from source IP address to destination port
tcp: 10.64.68.10:? -> ?.?.?.?:8040

UNITEDNETWORKS

Data Retention

- zákon vyžaduje ukládat údaje o provozu po dobu půl roku
- vhodné nejen z hlediska splnění zákonné povinnosti, ale při řešení případných problémů

NAT – ukládání údajů o všech konexích

- data přímo z Netfiltru, není blackbox
- vyhledávání dle různých parametrů

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

KONEXE - VÝPIS

Počet: 72144

Hledat... Ok

IPv	Prot.	TTL	A	B	C	D	E	F	G	H	I	J
ipv4 (2)	tcp (6)	7216	ESTABLISHED	src 100.82.86.4	dst 172.217.23.194	sport 56187	dport 443	src 172.217.23.194	dst 46.23.50.4	sport 443	dport 56187	[A
ipv4 (2)	tcp (6)	22	TIME_WAIT	src 46.23.51.28	dst 195.122.177.168	sport 53904	dport 443	src 195.122.177.168	dst 46.23.51.28	sport 443	dport 53904	[A
ipv4 (2)	tcp (6)	7416	ESTABLISHED	src 10.51.64.31	dst 31.13.84.8	sport 52634	dport 443	src 31.13.84.8	dst 46.23.50.31	sport 443	dport 52634	[A
ipv4 (2)	tcp (6)	291	ESTABLISHED	src 10.67.63.15	dst 95.168.214.209	sport 59009	dport 80	src 95.168.214.209	dst 46.23.50.15	sport 80	dport 59009	[A
ipv4 (2)	tcp (6)	7427	ESTABLISHED	src 10.67.63.9	dst 212.162.49.208	sport 52397	dport 443	src 212.162.49.208	dst 46.23.50.9	sport 443	dport 52397	[A
ipv4 (2)	tcp (6)	7436	ESTABLISHED	src 46.23.59.38	dst 74.125.133.188	sport 5592	dport 5228	src 74.125.133.188	dst 46.23.59.38	sport 5228	dport 5592	[A
ipv4 (2)	tcp (6)	100	TIME_WAIT	src 100.75.239.180	dst 93.91.151.75	sport 50526	dport 80	src 93.91.151.75	dst 46.23.50.180	sport 80	dport 50526	[A
ipv4 (2)	tcp (6)	98	TIME_WAIT	src 46.23.57.107	dst 92.123.36.12	sport 56036	dport 443	src 92.123.36.12	dst 46.23.57.107	sport 443	dport 56036	[A

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Vyhledávání toků
DoS a DDoS útoky
Blokování útoků
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

VYHLEDÁVÁNÍ TOKŮ

Všechny datové toky procházející ISP Gateway se ukládají do databáze definovaný počet dnů zpětně, standardně 183 dnů. V této databázi je možné vyhledávat jednak podle času a časového rozpětí, případně lze pomocí rozšířeného vyhledávání zadat zdrojovou IP adresu (veřejnou po případném NATu), cílovou IP adresu, zdrojový port (opět po případném NATu), cílový port a protokol.
POZOR! Tato data podléhají nařízení GDPR a může k nim mít přístup pouze oprávněná osoba a o každém konkrétním vyhledávání musí být pořízen záznam.

VYHLEDÁVÁNÍ

Datum a čas: 13.09.2018 12:02:07

Rozmezí +- sekund: 10

+ Rozšířené vyhledávaní

Vyhledat

Export CSV

vytvořeno	naposledy modifikováno	protokol	zdrojová IP adresa	zdrojový port	zdrojová IP adresa po NATu	zdrojový port po NATu	cílová IP adresa	cílový port
13.09.2018 12:01:41	13.09.2018 12:01:57	tcp	100.75.100.170	56374	46.23.50.170	56374	121.40.125.12	8000
13.09.2018 12:01:52	13.09.2018 12:01:57	udp	93.153.6.24	49455	93.153.6.24	49455	46.23.48.83	29810
13.09.2018 12:01:51	13.09.2018 12:01:57	tcp	100.75.202.5	46871	46.23.50.5	46871	120.25.151.121	8000

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Vyhledávání toků
DoS a DDoS útoky
Blokování útoků
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

VYHLEDÁVÁNÍ TOKŮ

Všechny datové toky procházející ISP Gateway se ukládají do databáze definovaný počet dnů zpětně, standardně 183 dnů. V této databázi je možné vyhledávat jednak podle času a časového rozpětí, případně lze pomocí rozšířeného vyhledávání zadat zdrojovou IP adresu (veřejnou po případném NATu), cílovou IP adresu, zdrojový port (opět po případném NATu), cílový port a protokol.
POZOR! Tato data podléhají nařízení GDPR a může k nim mít přístup pouze oprávněná osoba a o každém konkrétním vyhledávání musí být pořízen záznam.

VYHLEDÁVÁNÍ

Datum a čas: 13.09.2018 12:01:41

Rozmezí +- sekund: 10

Zdrojová IP adresa: 46.23.50.170

Cílová IP adresa: 121.40.125.12

Zdrojový port: 56374

Cílový port: 8000

Protokol: tcp

Vyhledat

Export CSV

vytvořeno	naposledy modifikováno	protokol	zdrojová IP adresa	zdrojový port	zdrojová IP adresa po NATu	zdrojový port po NATu	cílová IP adresa	cílový port
13.09.2018 12:01:41	13.09.2018 12:01:57	tcp	100.75.100.170	56374	46.23.50.170	56374	121.40.125.12	8000

UNITEDNETWORKS

WAMP protokol

- nadstavba WebSocketu, obousměrná realtime komunikace
- pro komunikaci s CRM a dalšími systémy
- u rozsáhlejších systémů je web rozhraní nepraktické – duplikace dat
- přes WAMP je dostupných mnohem více funkcí
- RPC pro volání funkcí a PUB/SUB pro alerty

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

OBSAH

INTRODUCTION

ISP Gateway

ISP Gateway is software system for managing and monitoring internet connectivity for large number of services (large number of ISP customers). It supports tens of thousands services and up to ten gigabits per seconds traffic on relatively cheap hardware (several times cheaper than proprietary hardware).

It is based on new Linux kernel network core nftables, uses HFSC work non-conserving discipline to distribute internet connectivity to services, has FQ_CoDel as work conserving queue for each service (configurable), stores data in NoSQL OrientDB database and uses WAMP protocol for communication between modules or with existing CRM and other software.

It can be managed with built-in web interface or preferably connected to existing CRM by WAMP protocol using RPC and PUB/SUB messages.

Basic functions

- supports hierarchical service trees, burst, priorities, FUP, access points congestion protection etc.
- logging internet traffic for each service, analysis and DoS, DDoS protection
- monitoring of all network L3 elements, historical latency and traffic graphs
- managed using simple web interface or by existing CRMs through WAMP RPCs and PUB/SUBs

Modules

popd

Manages network traffic for services using multilevel QoS tree (typically dedicated line -> access points -> services). Supports both link sharing and realtime HFSC curves optionally with both curve parts (burst, backlogged) and priorities. Included are manually or automatically updated blacklists for network protection from bogus IP addresses.

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

OBSAH

WAMP API

WAMP API Overview

WAMP (Web Application Messaging Protocol, http://wamp-proto.org/), is WebSocket based subprotocol which provides RPC and PUB/SUB messages in one uniform protocol.

Most of ISP Gateway system modules utilize WAMP protocol for internal or inter-module communication, for communication with web interface and for providing management API. Autobahn library (https://crossbar.io/autobahn/) is used as an implementation of WAMP and Crossbar.io router (https://crossbar.io) based on Twisted network engine (https://twistedmatrix.com/) is used for routing RPCs and PUB/SUBs.

Basics

Synchronization mechanism

ISP Gateway has simple synchronization mechanism for synchronizing internal database state with external software (CRMs etc.). It is based on counter named 'ageid', which has starting value 0 (when database is empty) and is increased by one with every RPC, which changes database state. All such RPCs are required to have ageid as first parameter and its value must match internal value of ageid. RPCs, which only read some data, dont have such requirement.

External CRM should log all RPCs into some kind of buffer and when disconnection occures, it can still accept commands, which otherwise would require firing RPCs to change ISP Gateway status. And after both systems are reconnected again, it just have to read ISP Gateway internal ageid and then replay RPCs from buffer from this ageid.

QOS

Defining bandwidth

- RPCs which accepts bandwidth as parameter require its format to be as following:

Přehled
Strom služeb
Tarify
Mapování a sety
Neznámé IP adresy
Statistika paketů
Správa provozu
Tabulka konexí
Log
Dokumentace
Nastavení
Systém

OBSAH

POPDRPC.PY

```
#!/usr/bin/python
#
# popd project
#
# run rpc from command line
#
# syntax is: popdrpc.py [-s address] [-p port] rpcname [param ...]
#
# Karel Rericha
#
# Created: 11.12.2016
# Last modified: 23.3.2018
#

import time
import argparse
import ast
import sys

from twisted.internet.defer import inlineCallbacks

sys.path.append("..")
from lib.libtools import run_worker, run_rpc, listen_pubsubs  # noqa


# IP address and port of host to connect
```

ISP Gateway

Děkuji za pozornost

www.ispgateway.cz