cesnet

INTEGRACE DDOS PROTECTORU V PROSTŘEDÍ PROPOJOVACÍHO UZLU NIX.CZ

Tomáš Podermański
CESNET

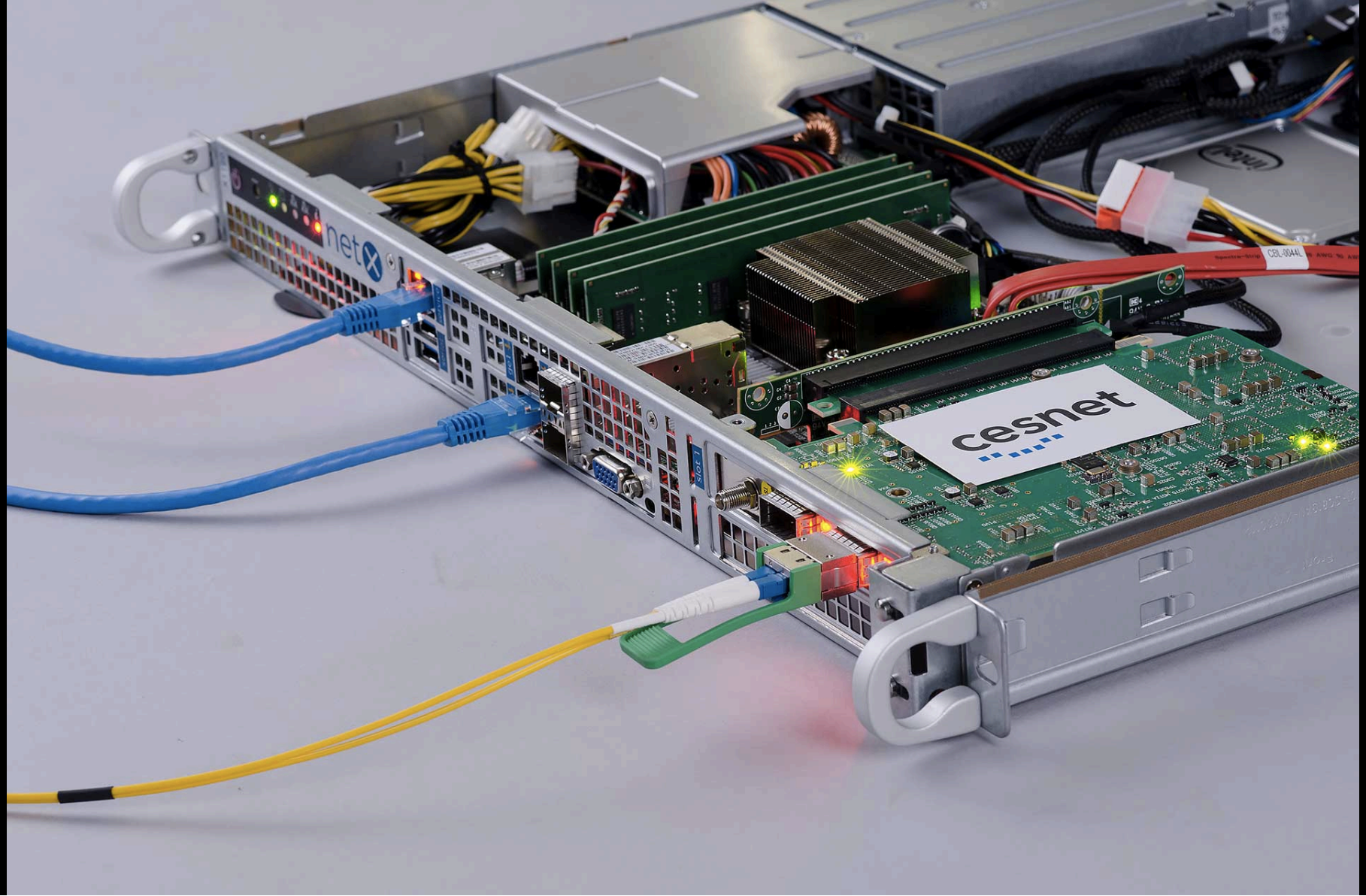
CSNOG 2019
Brno

cesnet

DDOS PROTECTOR

- HW akcelerované zařízení s programovatelnými FPGA poli.
- Specializované řešení vyvinuté pro síť CESNET2
- Obsahuje několik mitigačních algoritmů pro DDoS útoky.
- Podrobněji viz loňská přednáška Martina Žádnika

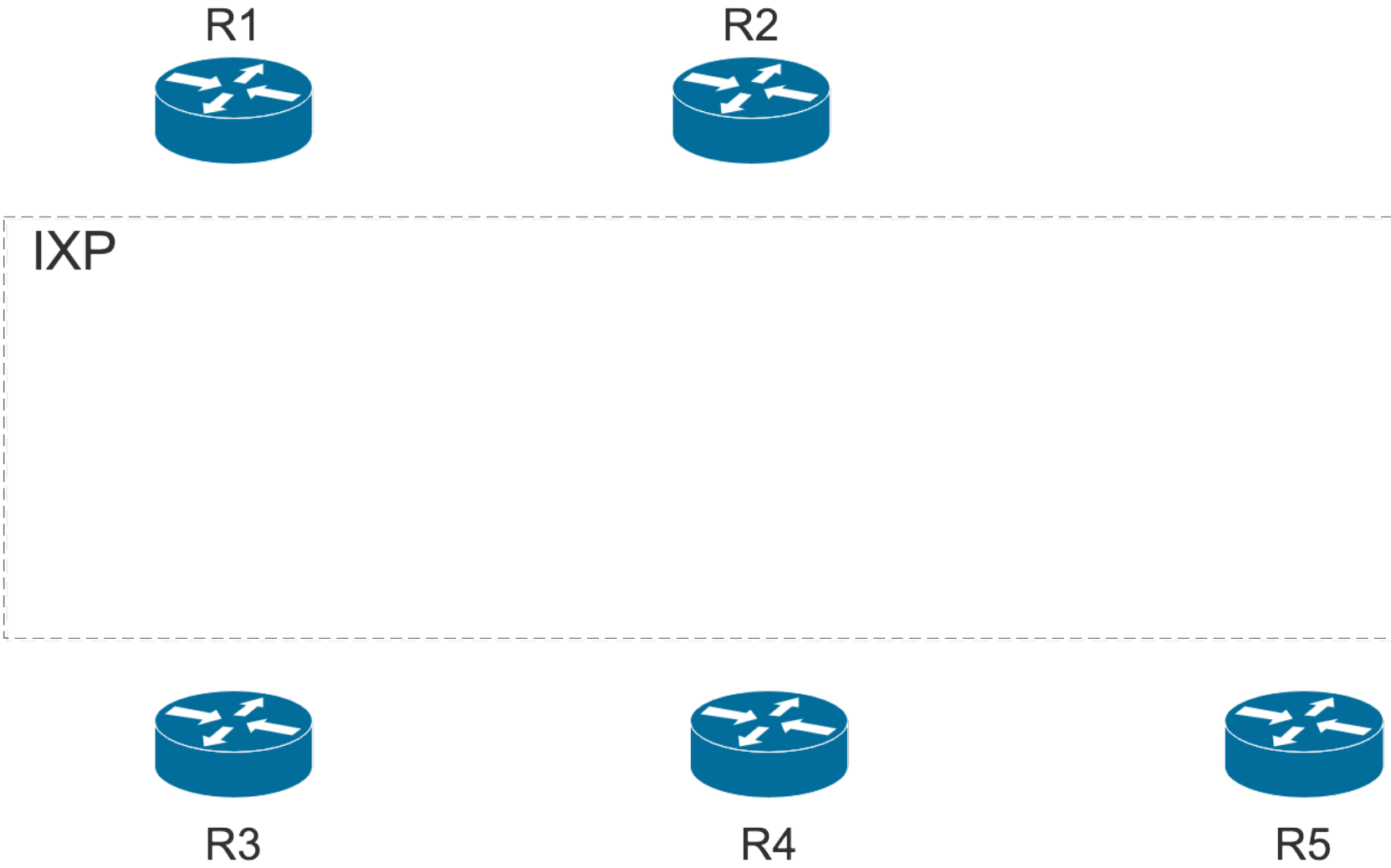
  https://indico.csnog.eu/event/1/contributions/11/

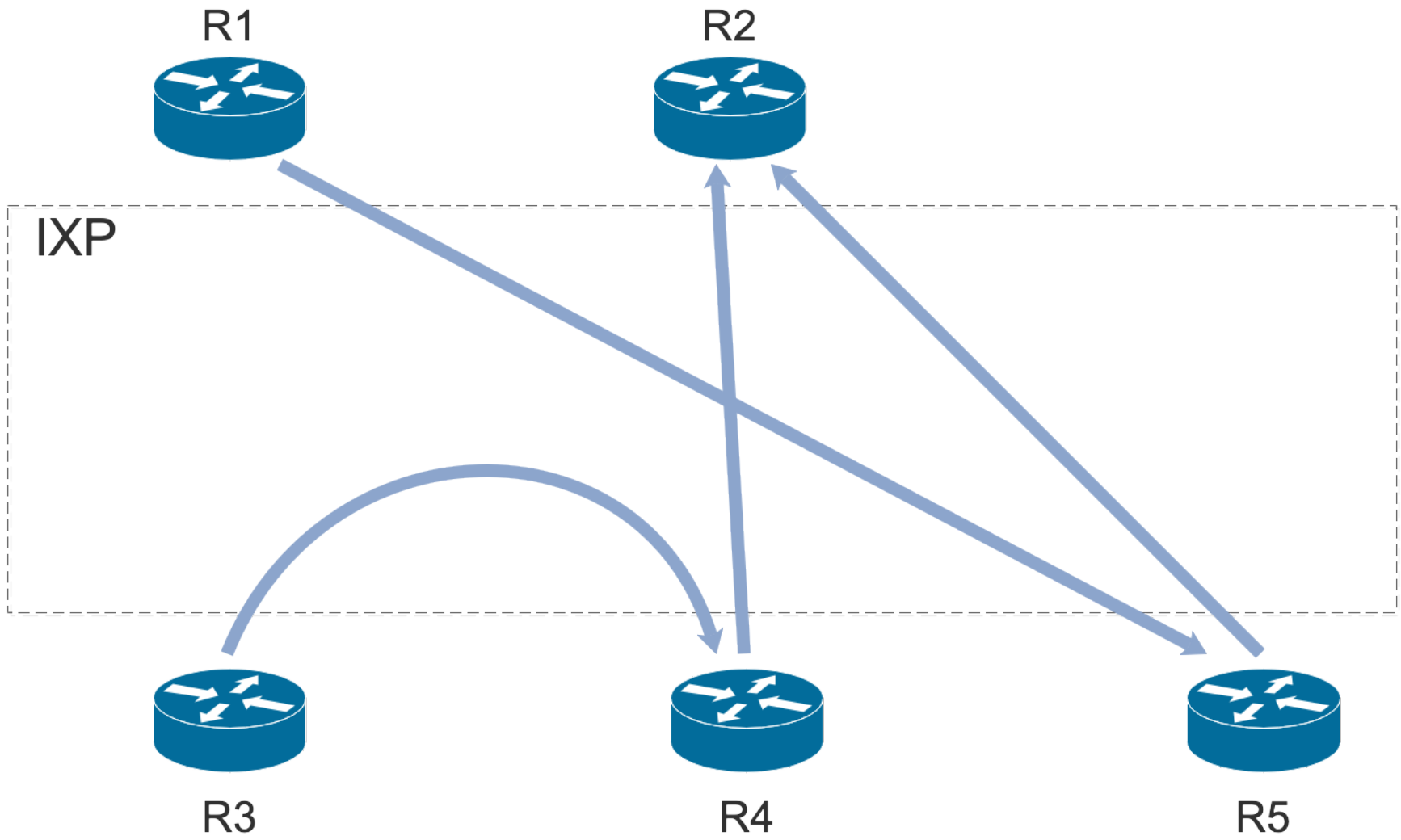

cesnet

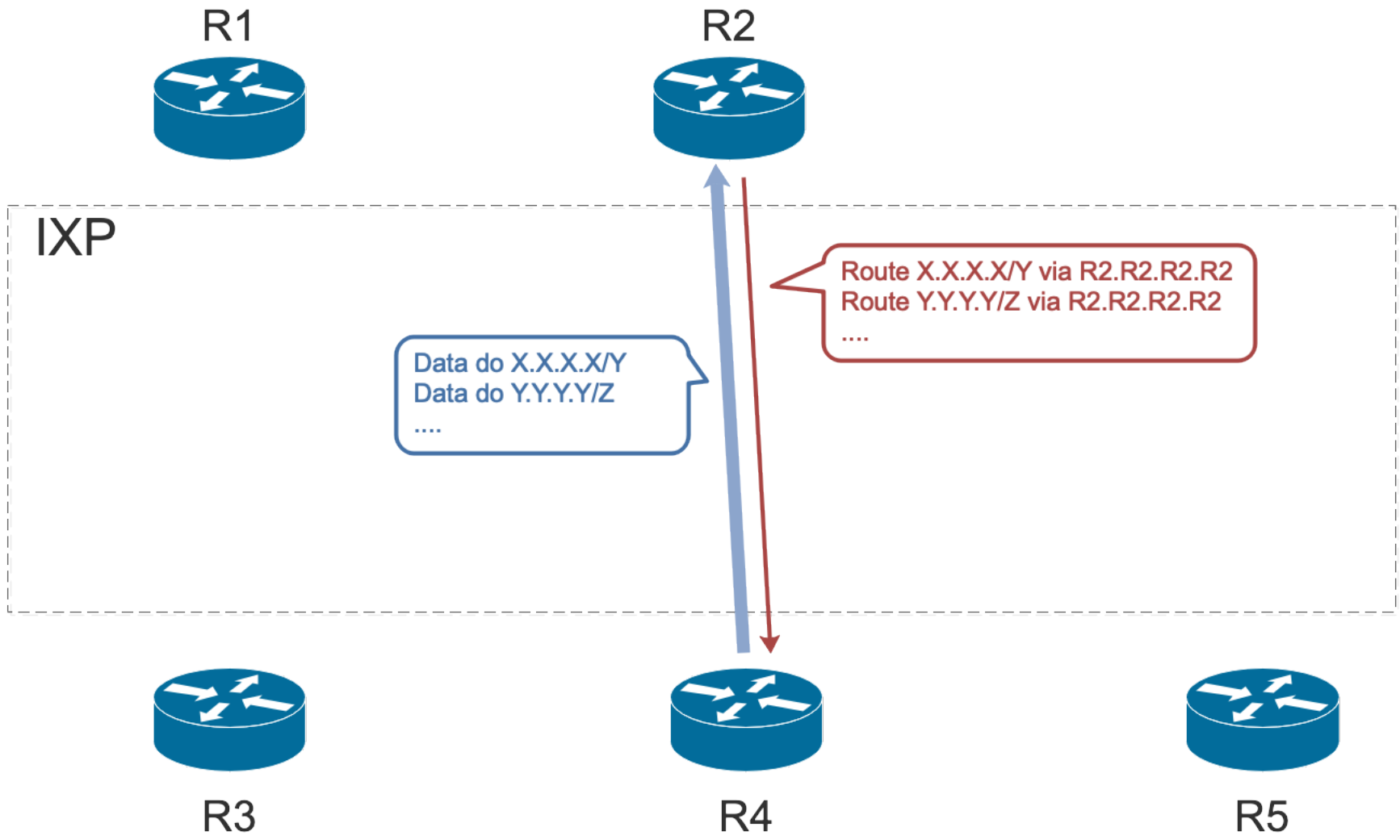
cesnet

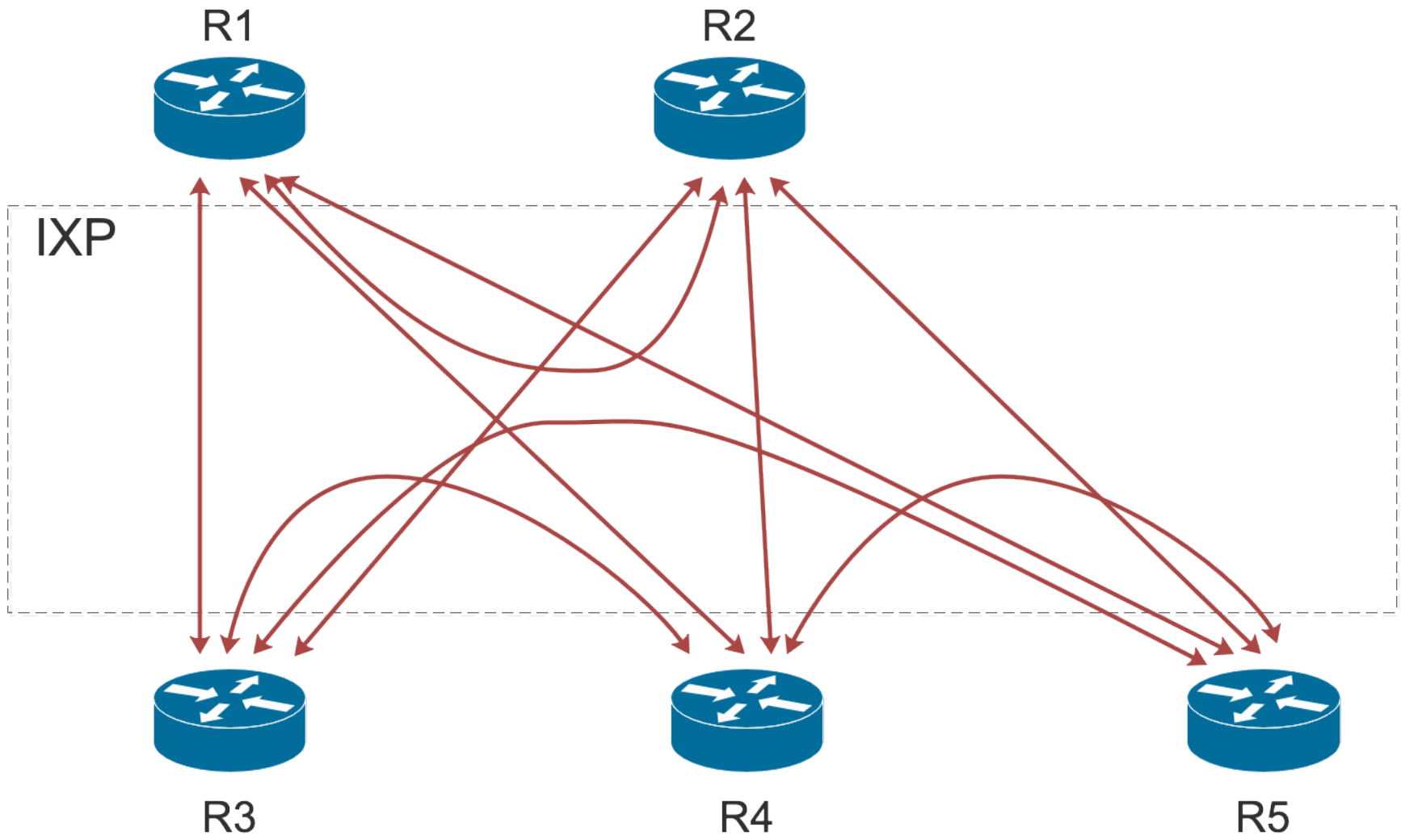
POŽADAVKY NA IMPLEMENTACI

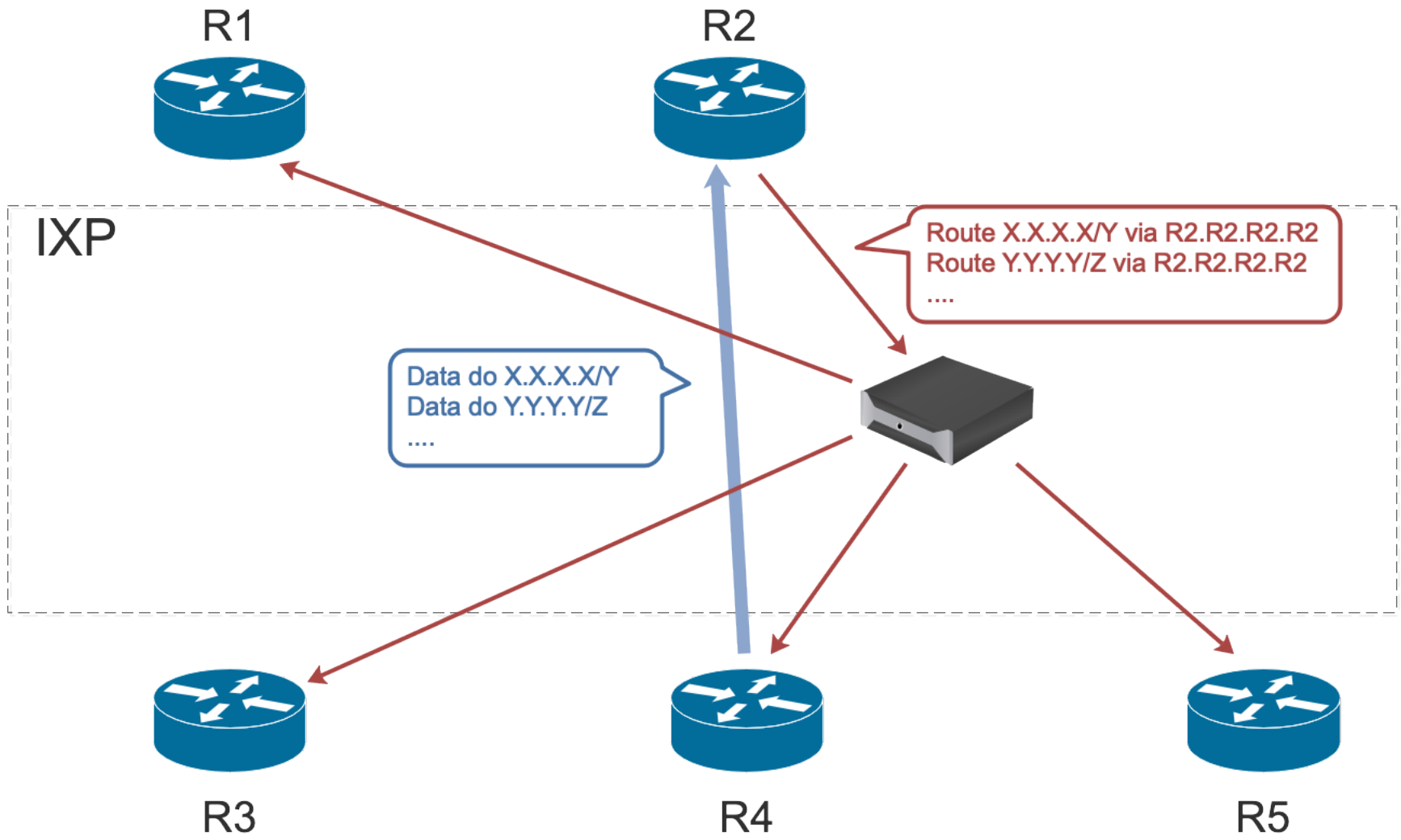
- Hrubá filtrace s vysokým výkonem.
- Minimalizace zásahu do infrastruktury IXP.
- Řízení průběhu mitigace plně ze strany člena/zákazníka.
- Řízení oprávnění.
- Zpětná vazba o průběhu mitigace.
- Vše bez “lidské“ interakce ze strany NIX.
- Plnohodnotná podpora IPv4 + IPv6.

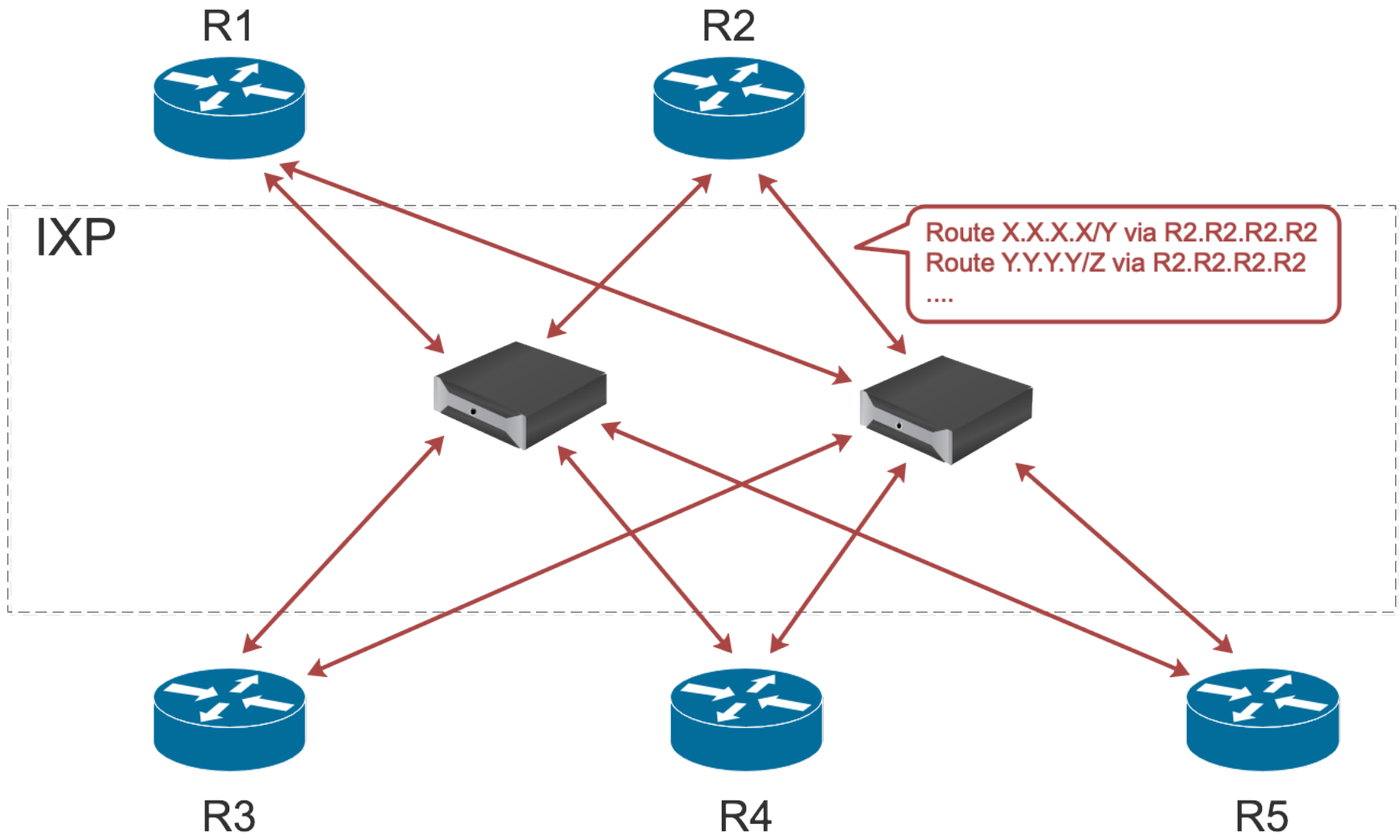

R1
R2
IXP
R3
R4
R5

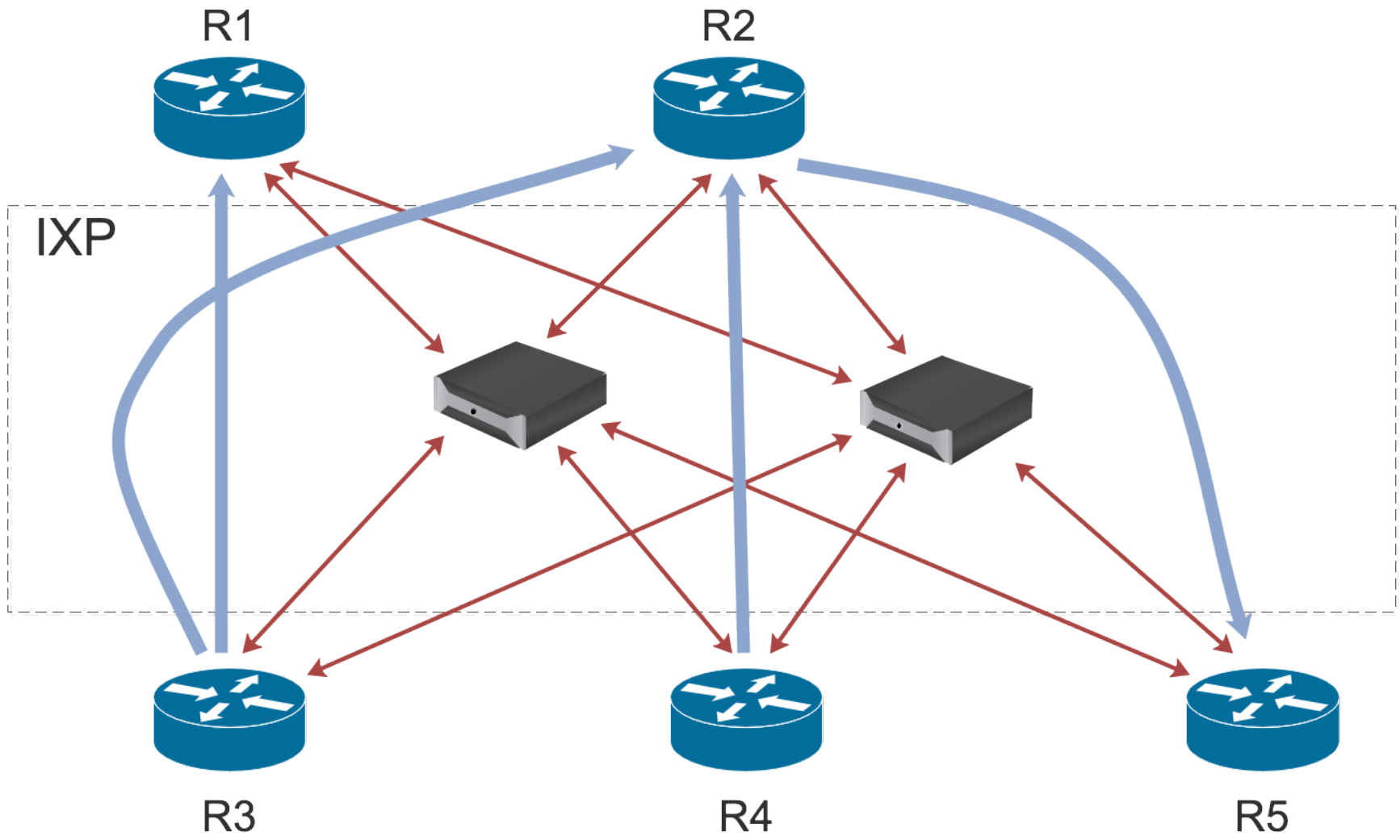

R1
R2
IXP
R3
R4
R5

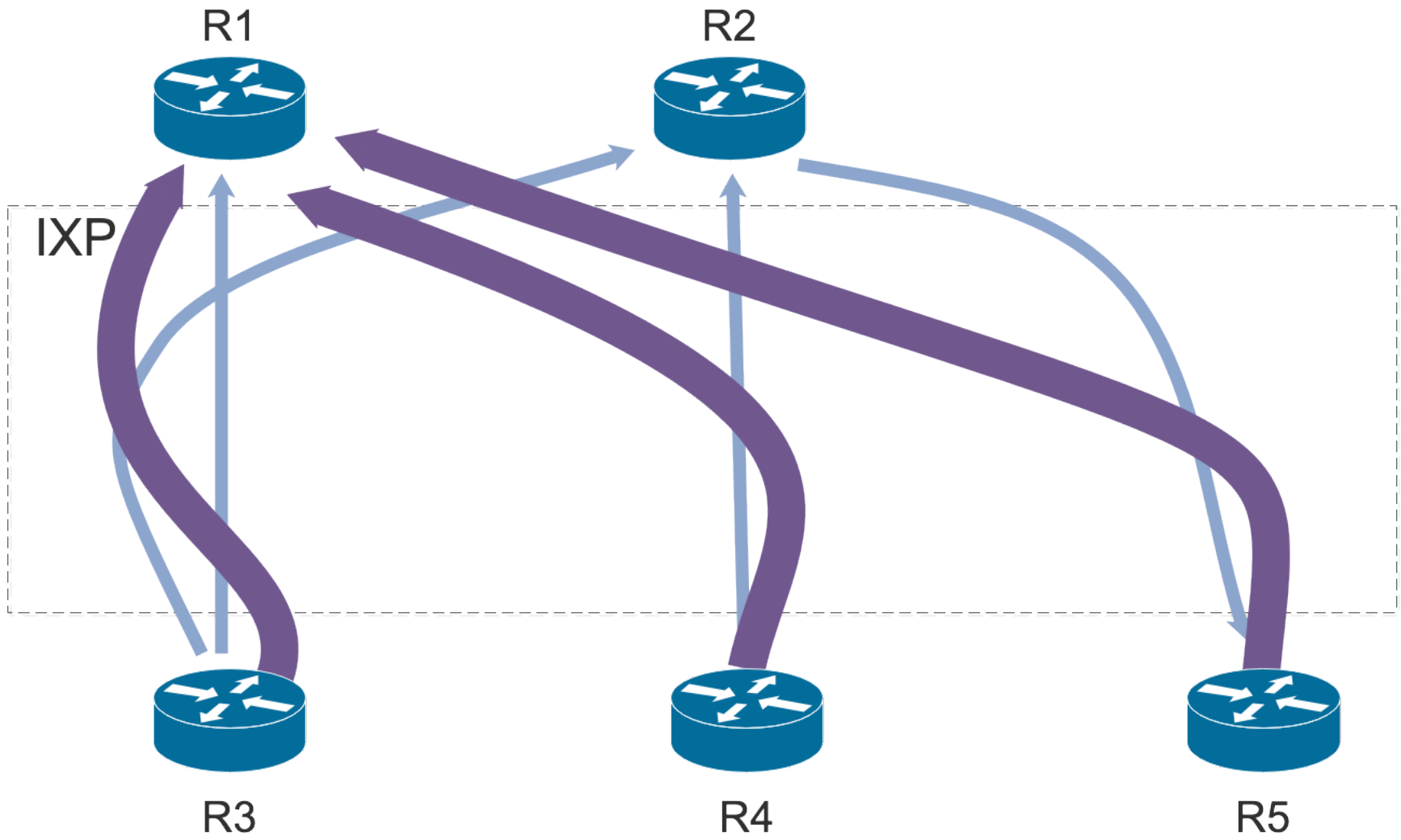

R1
R2
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
Route Y.Y.Y.Y/Z via R2.R2.R2.R2
....
Data do X.X.X.X/Y
Data do Y.Y.Y.Y/Z
....
R3
R4
R5

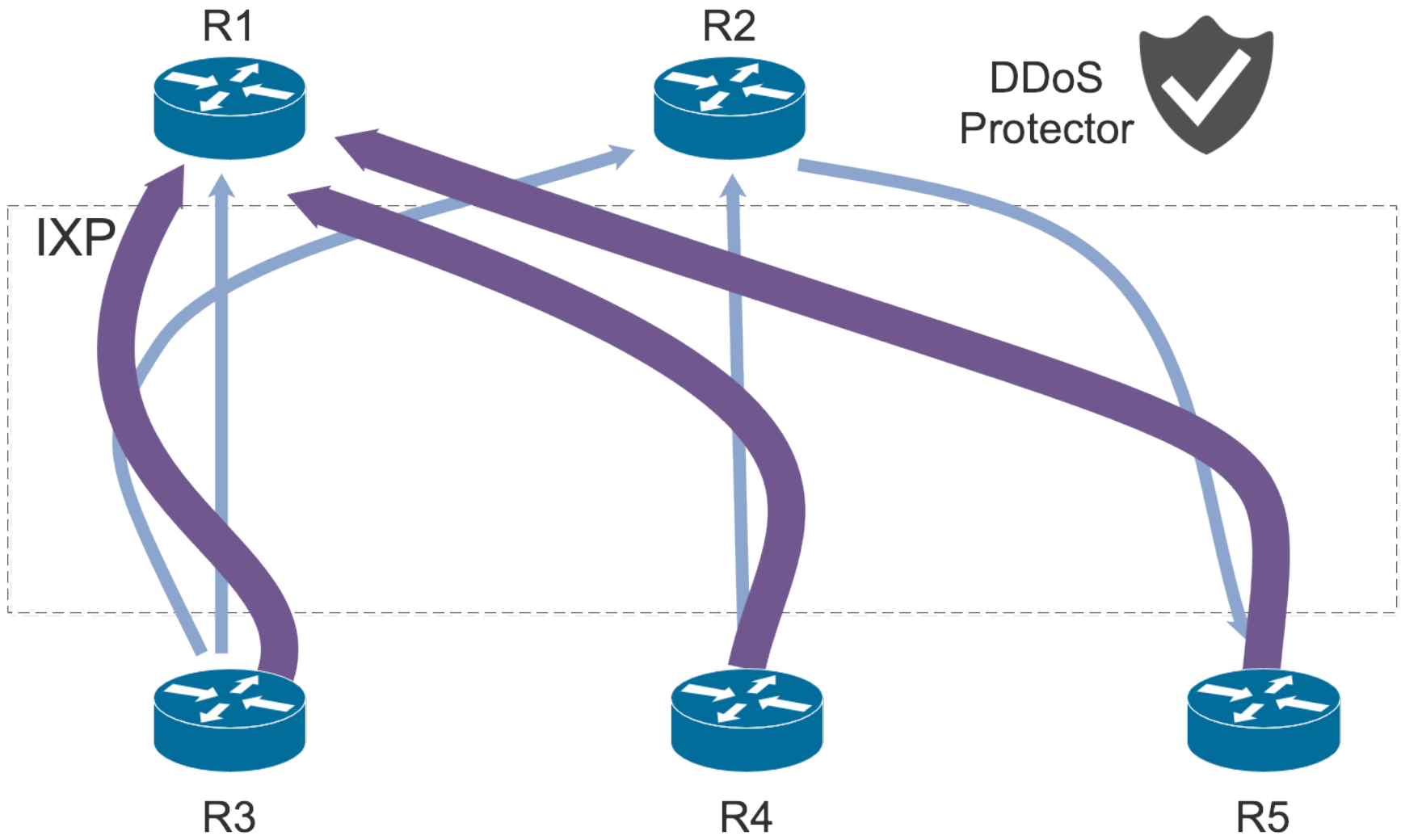

R1
R2
IXP
R3
R4
R5

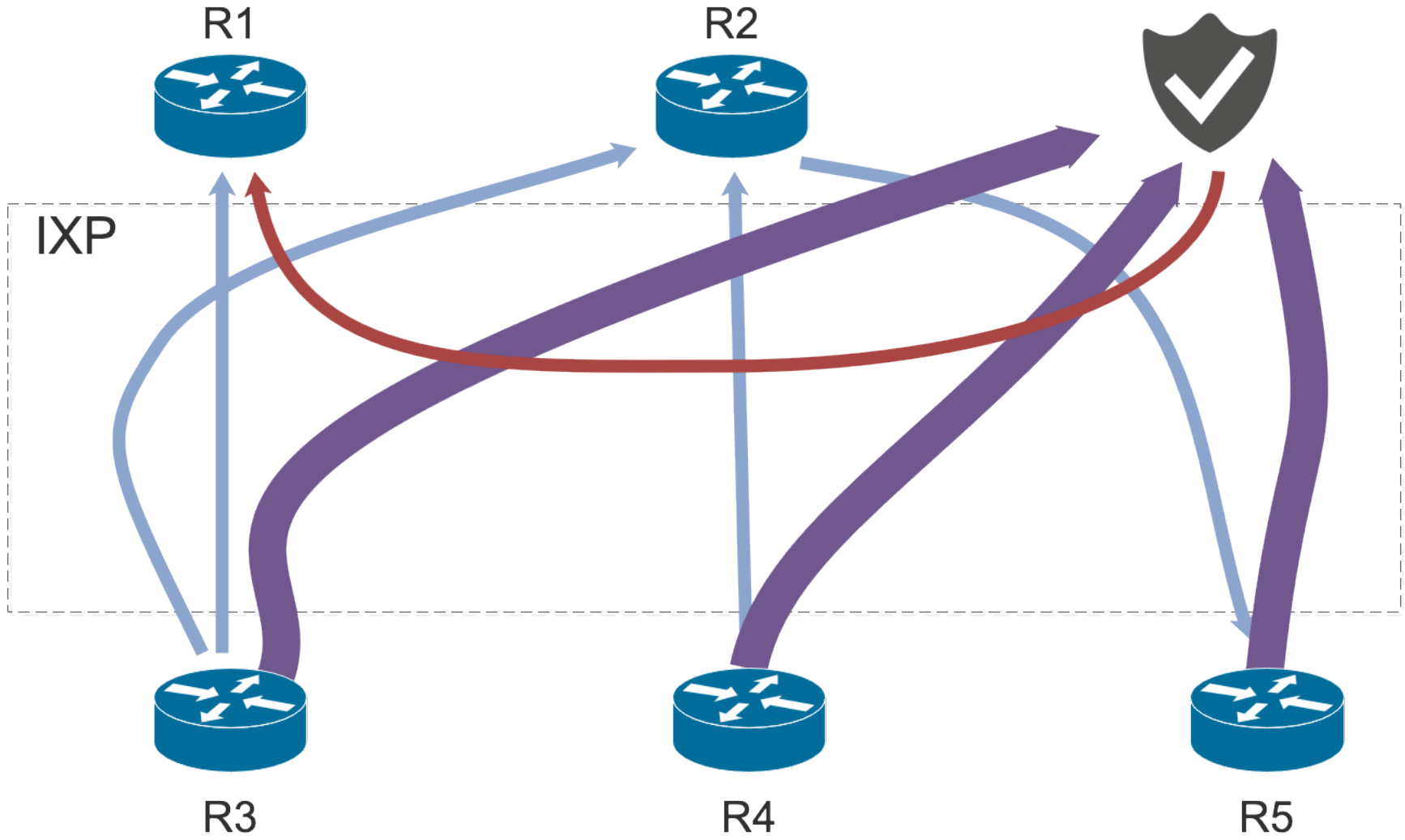

R1
R2
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
Route Y.Y.Y.Y/Z via R2.R2.R2.R2
....
Data do X.X.X.X/Y
Data do Y.Y.Y.Y/Z
....
R3
R4
R5

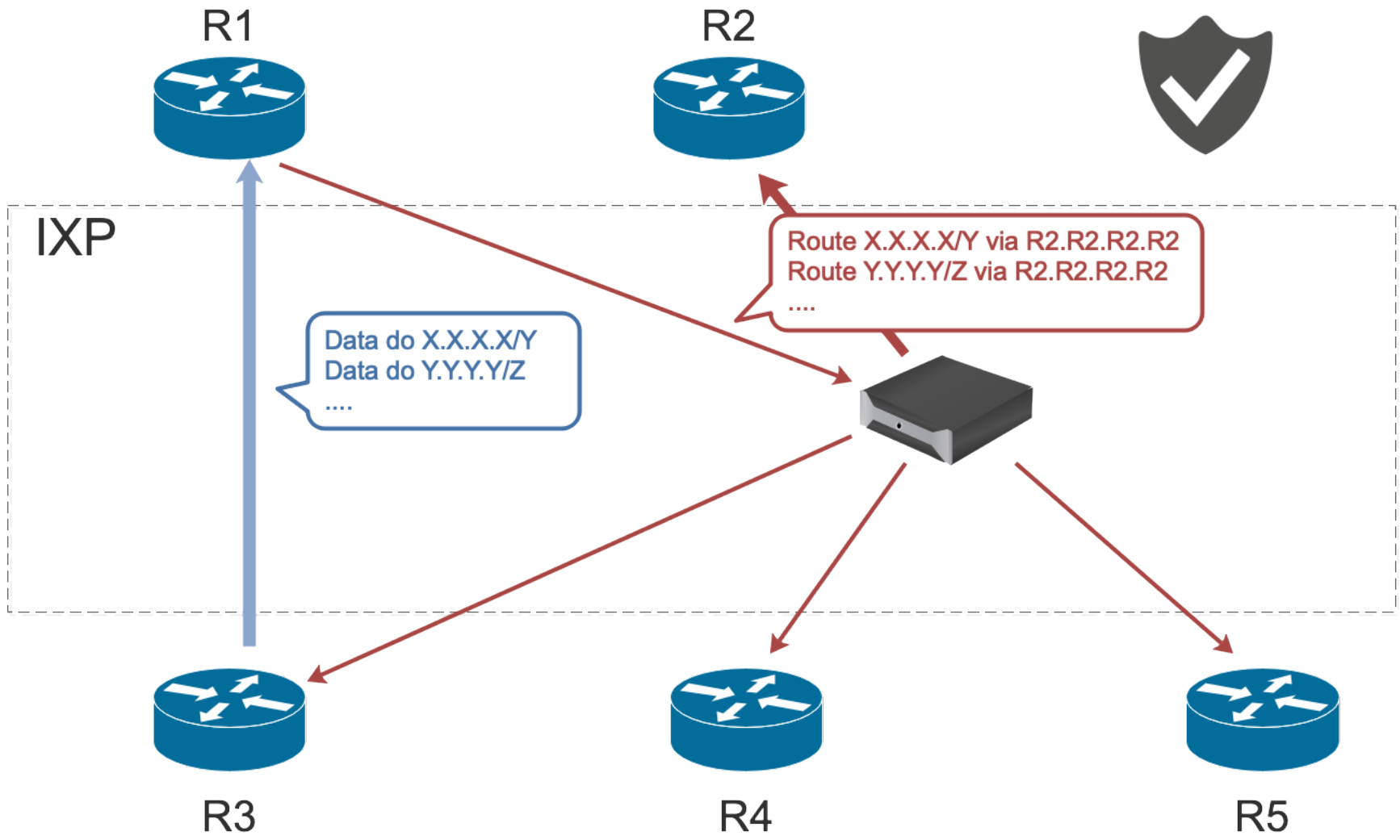

R1
R2
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
Route Y.Y.Y.Y/Z via R2.R2.R2.R2
....
R3
R4
R5

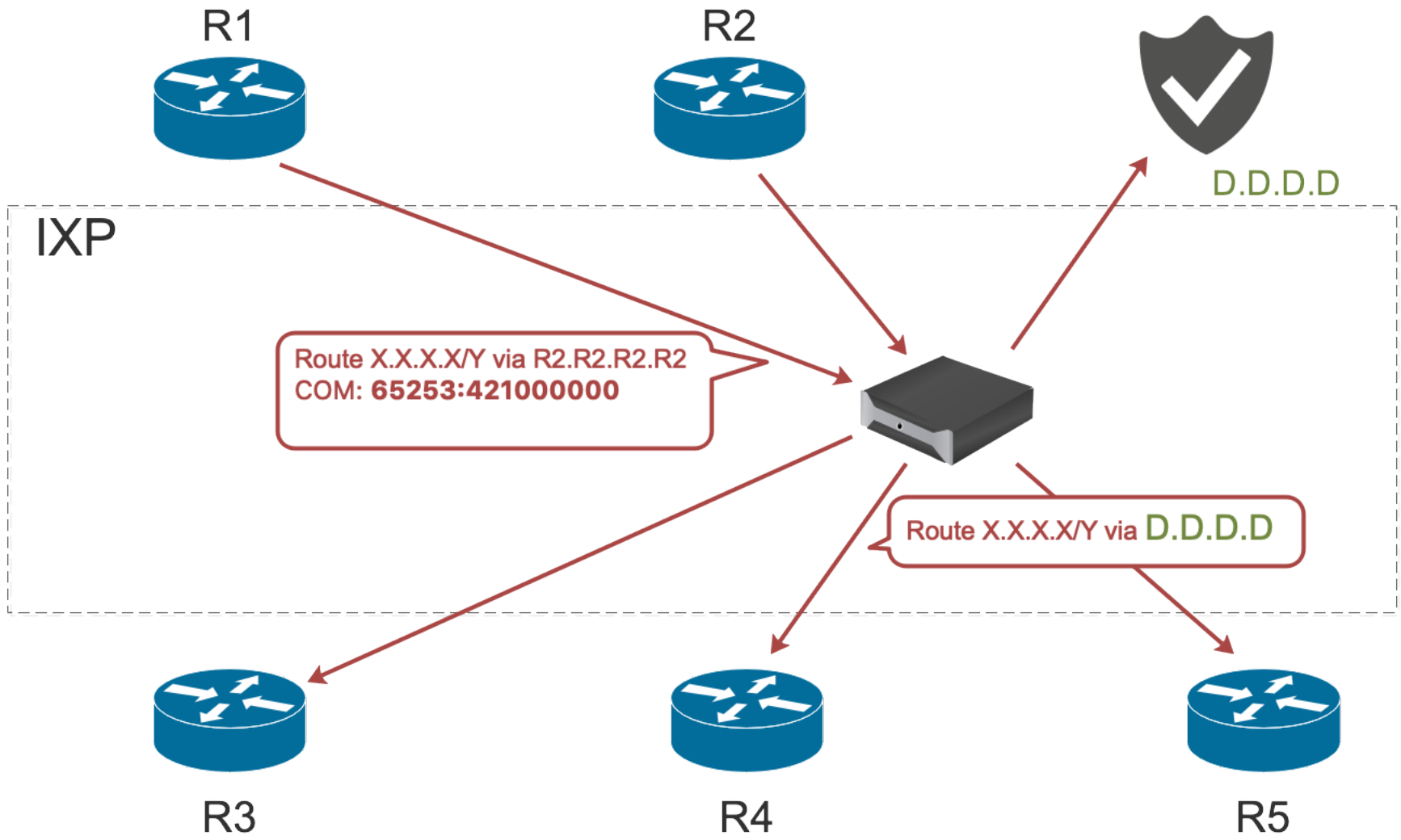

R1
R2
IXP
R3
R4
R5

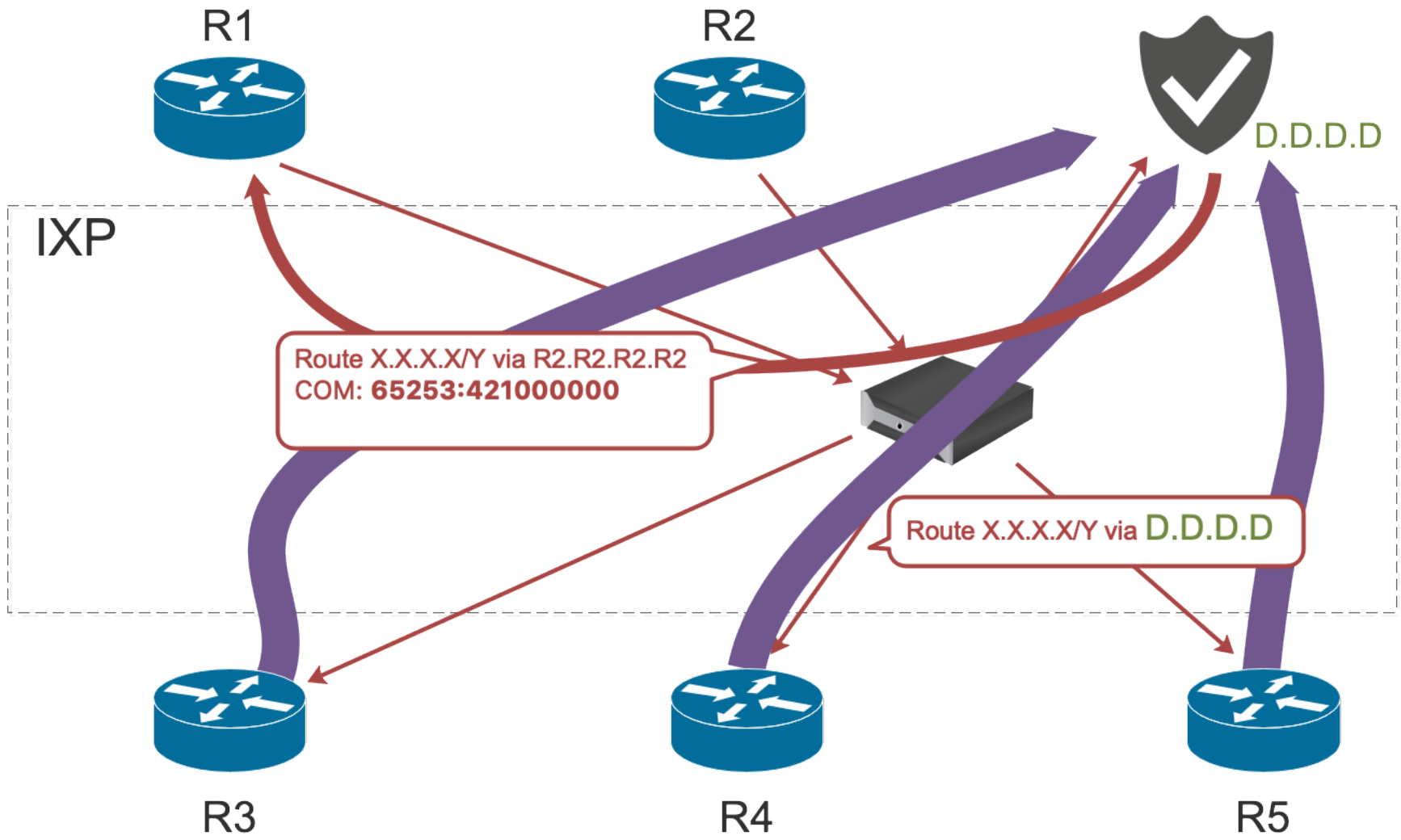

R1
R2
IXP
R3
R4
R5


R1
R2
DDoS
Protector
IXP
R3
R4
R5


R1
R2
IXP
R3
R4
R5


R1
R2
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
Route Y.Y.Y.Y/Z via R2.R2.R2.R2
....
Data do X.X.X.X/Y
Data do Y.Y.Y.Y/Z
....
R3
R4
R5


R1
R2
D.D.D.D
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
COM: 65253:421000000
Route X.X.X.X/Y via D.D.D.D
R3
R4
R5


R1
R2
D.D.D.D
IXP
Route X.X.X.X/Y via R2.R2.R2.R2
COM: 65253:421000000
Route X.X.X.X/Y via D.D.D.D
R3
R4
R5

MITIGACE PŘÍJEMCEM - BIRD

```
...
if ( net ~ [ X.X.X.0/24 ] ) then {
      bgp_ext_community.add((rt, 65253, 421000000));
      bgp_ext_community.add((rt, 65253, 421010002));
      bgp_ext_community.add((rt, 65253, 421210240));
}
...
```

MITIGACE PŘÍJEMCEM - CISCO

```
...
access-list 1 permit x.x.x.0 0.0.0.255

route-map mitigation permit 10
 match ip address 1
 set extcommunity rt 65254:421000000 65254:421010002 \
             65254:421210240
...
```

POUŽITÍ KOMUNIT – VERZE 1

- Přesměrování do DDoS Protector
  - rt: 65253:421000000
- Parametry mitigace

  rt: 65253:421NNPPPP

  NN – typ mitigace
  PPPP – doplňkové parametry

Hodnota NN	Význam hodnoty PPPP	Popis/Poznámka
01	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP
02	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP pouze UDP
03	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP pouze TCP-SYN pakety
04	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP pouze UDP src port 123 (NTP)
05	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP pouze UDP src port 53 (DNS)
06	Hodnota ve stovkach Mb/s	Amplifikační omezení veškerý provoz na hodnotu PPPP pouze fragmentované pakety
21	Hodnota threshold počtu syn paketů v kp/s.	Syn drop na veškerý TCP provoz s parametry m=1k, n=10k

POUŽITÍ KOMUNIT – VERZE 2

- Přesměrování do DDoS Protector

  rt: 65253:00000000

- Parametry mitigace

  rt: 65253:NNPPPPPPP

  NN – typ mitigace
  PPPPPPP – doplňkové parametry

DDoS Protector Status - preview verze

Installed rules:

```
AS_PATH: 6881 6881 6881 6881 6881, NETX_HOP: 2001:7f8:14:5ec::2 fe80::aa0c:dff:fe8d:fa81
EXT_COMM: (rt, 65253, 421000000) (rt, 65253, 421010001)
DDP PARAMS: 01->0001
dst_net 2a02:38:bbbb::10/128 limit_bts 10000000 rule_id_amp 205 thres_bts 6000000
Matched: 794.0 pkts, 1079.2kB,   0.0 pkts/s,   0.0 b/s
Blocked:   0.0 pkts,   0.0 B,   0.0 pkts/s,   0.0 b/s


AS_PATH: 6881 6881 6881 6881 6881, NETX_HOP: 194.50.100.246
EXT_COMM: (rt, 65253, 421000000) (rt, 65253, 421010001)
DDP PARAMS: 01->0001
dst_net 93.190.130.10/32 limit_bts 10000000 rule_id_amp 206 thres_bts 6000000
Matched: 116.2Mpkts, 165.9GB, 472.7kpkts/s,   5.4Gb/s
Blocked: 113.7Mpkts, 162.4GB, 472.7kpkts/s,   5.4Gb/s
```

DDoS Protector Status - preview verze

Installed rules

UDP FLOOD ~ 3.1 Gb/s -> AS197451 -> AS2852 -> NIX OFFICE
UDP FLOOD ~ 2.3 Gb/s -> AS24971 -> NIX OFFICE

```
AS_PATH: 6881
EXT_COMM: (rt,
DDP PARAMS: 01->0001
dst_net 2a02:38:bbbb::10/128 limit_bts 10000000 rule_id_amp 205 thres_bts 6000000
Matched: 794.0 pkts, 1079.2kB,   0.0 pkts/s,   0.0 b/s
Blocked:   0.0 pkts,   0.0 B,   0.0 pkts/s,   0.0 b/s


AS_PATH: 6881 6881 6881 6881 6881, NETX_HOP: 194.50.100.246
EXT_COMM: (rt, 65253, 421000000) (rt, 65253, 421010001)
DDP PARAMS: 01->0001
dst_net 93.190.130.10/32 limit_bts 10000000 rule_id_amp 206 thres_bts 6000000
Matched: 116.2Mpkts, 165.9GB, 472.7kpkts/s,   5.4Gb/s
Blocked: 113.7Mpkts, 162.4GB, 472.7kpkts/s,   5.4Gb/s
```

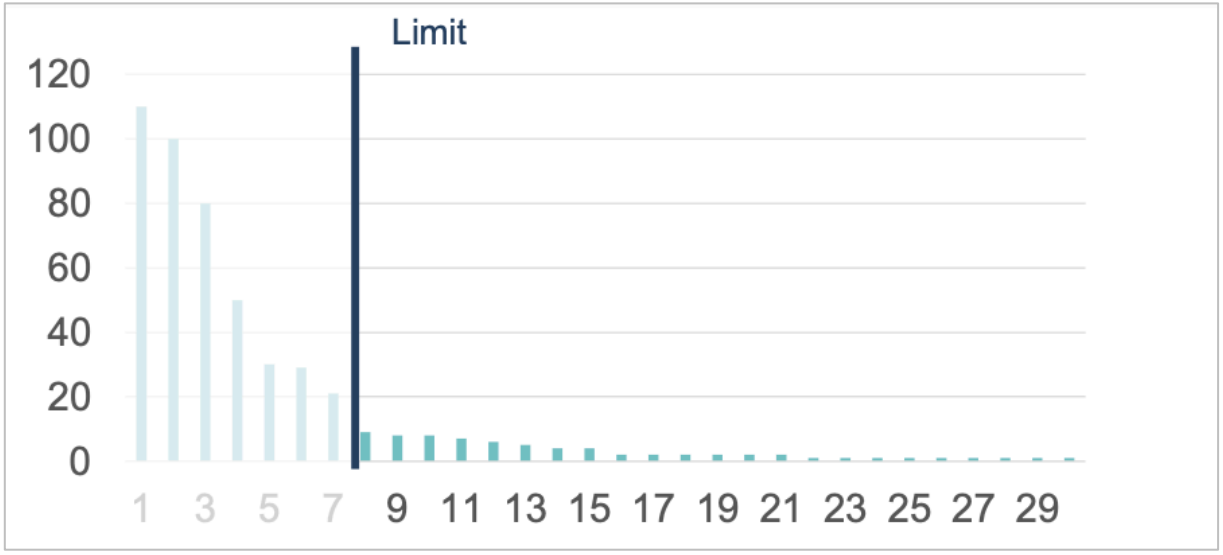
cesnet

ZÁKLADNÍ TYPY MITIGACE

- Amplifikační modul
- Syn drop modul

Amplifikační modul

- Fáze 1: dosažení hodnoty threshold na cílový prefix,
- Fáze 2: prořezávaní zdrojů s největším příspěvkem až dojde k poklesu na hodnotu limit.



Syn drop modul

- **Fáze 1: dosažení hodnoty threshold na cílový prefix**
- **Fáze 2: počítání statistik SYN a ACK pro každý zdroj:**
  - Čítač SYN > m && Čítač ACK 0: DROP – spoofnutá IP (generuje SYNy, jinak nekomunikuje)
  - Čítač SYN > n: DROP – útok z jedné IP (příliš agresivní)
  - Čítač ACK > 0: ALLOW – validní provoz (IP komunikuje)
  - Čítač SYN 1: DROP – první SYN (čekám retransmit)
  - Čítač SYN > 1: ALLOW – další SYNy (v mezích [2,m])

Ack spoofing, RST Cookies moduly

- Problematické použití v prostředí IXP
- vyžaduji “zpětný kanál”

ČASOVÝ HARMONOGRAM

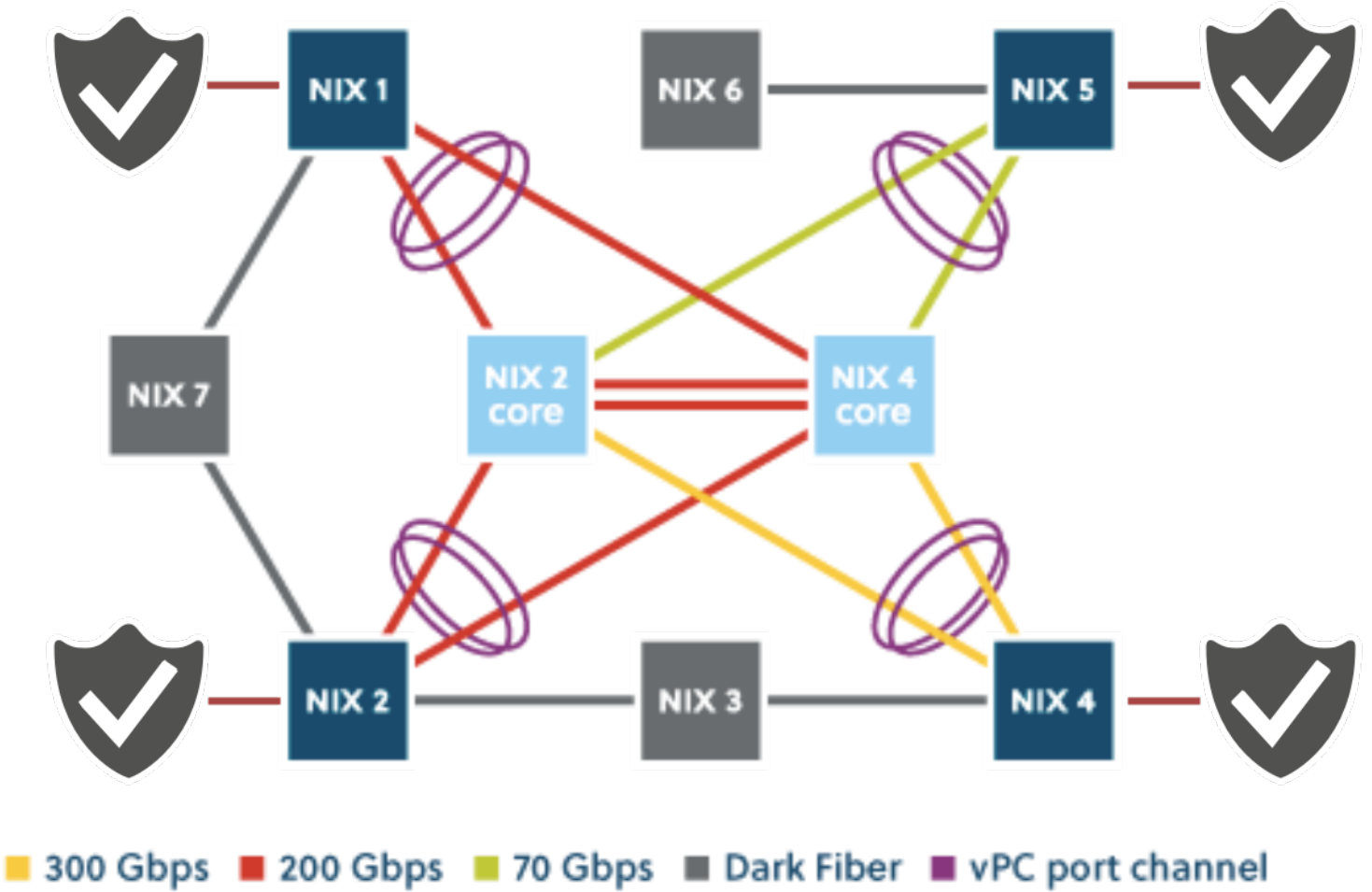
- Q1-4/2018 Příprava na straně DDoS Protectoru.
- Q1-2/2019 Implementace v projektu FENIX
- Q3-4/2019
  - Přesun do produkční VLAN.
  - Integrace RPKI.
  - Povelování V2.
  - Testování.
- Vyhodnocení podnětů, další kroky

jakékoliv podněty vítány

cesnet

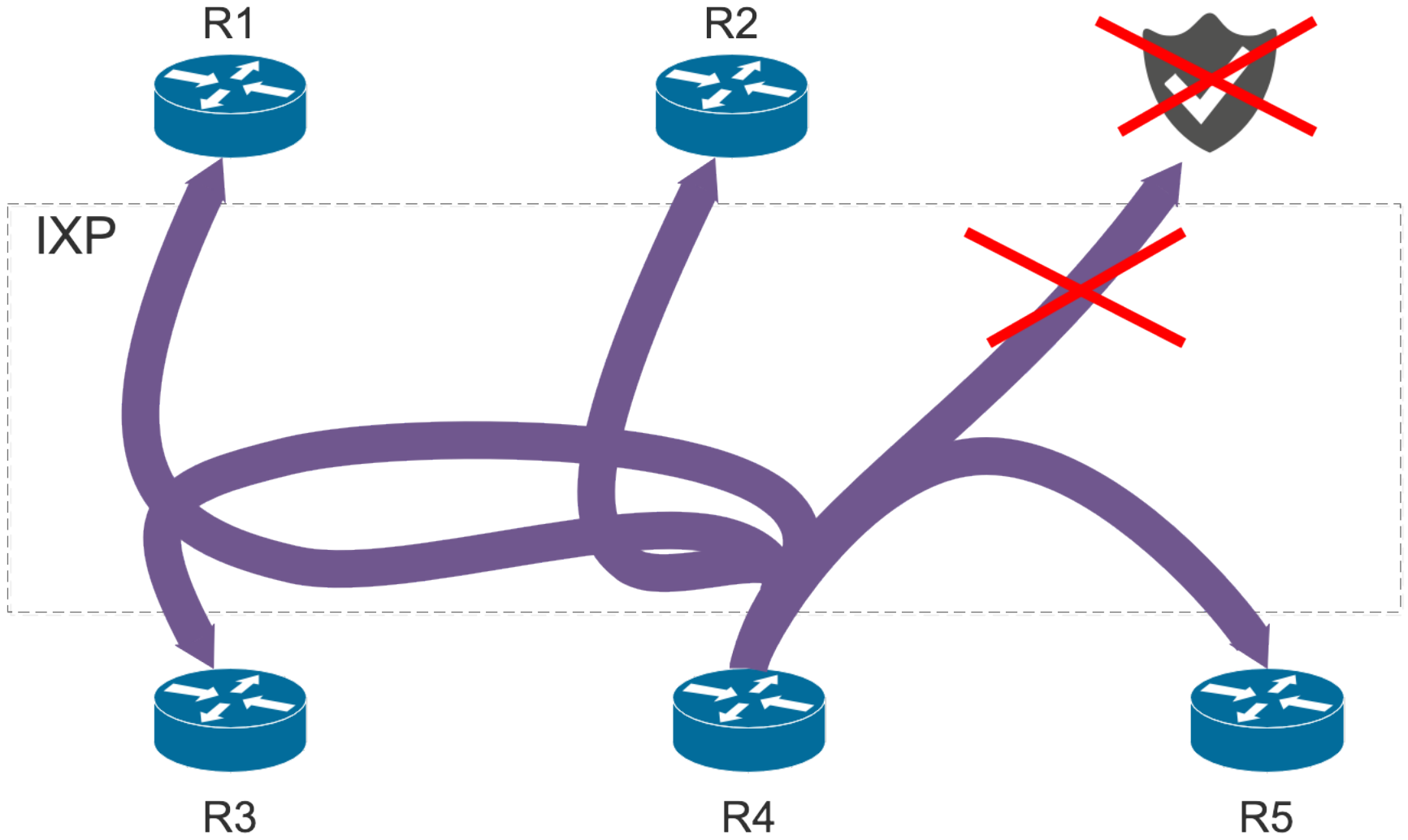
JAK S NAVYŠOVANÍM KAPACITY ?

- **Aktuální filtrační kapacita 100Gb/s box.**
- **Vývoj 400Gb/s.**
- **Přidávání dalších instancí DDoS Protectoru**
  - Load balancing na L3.
  - Ethernet anycast.


NIX 1
NIX 6
NIX 5
NIX 7
NIX 2
core
NIX 4
core
NIX 2
NIX 3
NIX 4
300 Gbps
200 Gbps
70 Gbps
Dark Fiber
vPC port channel

ZÁVĚREČNÝ KVÍZ

- Co se stane když “podvádím“ při routingu ?
- Co se stane když switch neví na který port má poslat paket ?


R1
R2
IXP
R3
R4
R5

- Co se stane když “podvádím“ při routingu ?
- Co se stane když switch neví na který port má poslat paket ?

```
interface Ten-GigabitEthernet1/0/29
        mac-address static 0011-1700-0017 vlan 1700
```

cesnet

DĚKUJI ZA POZORNOST