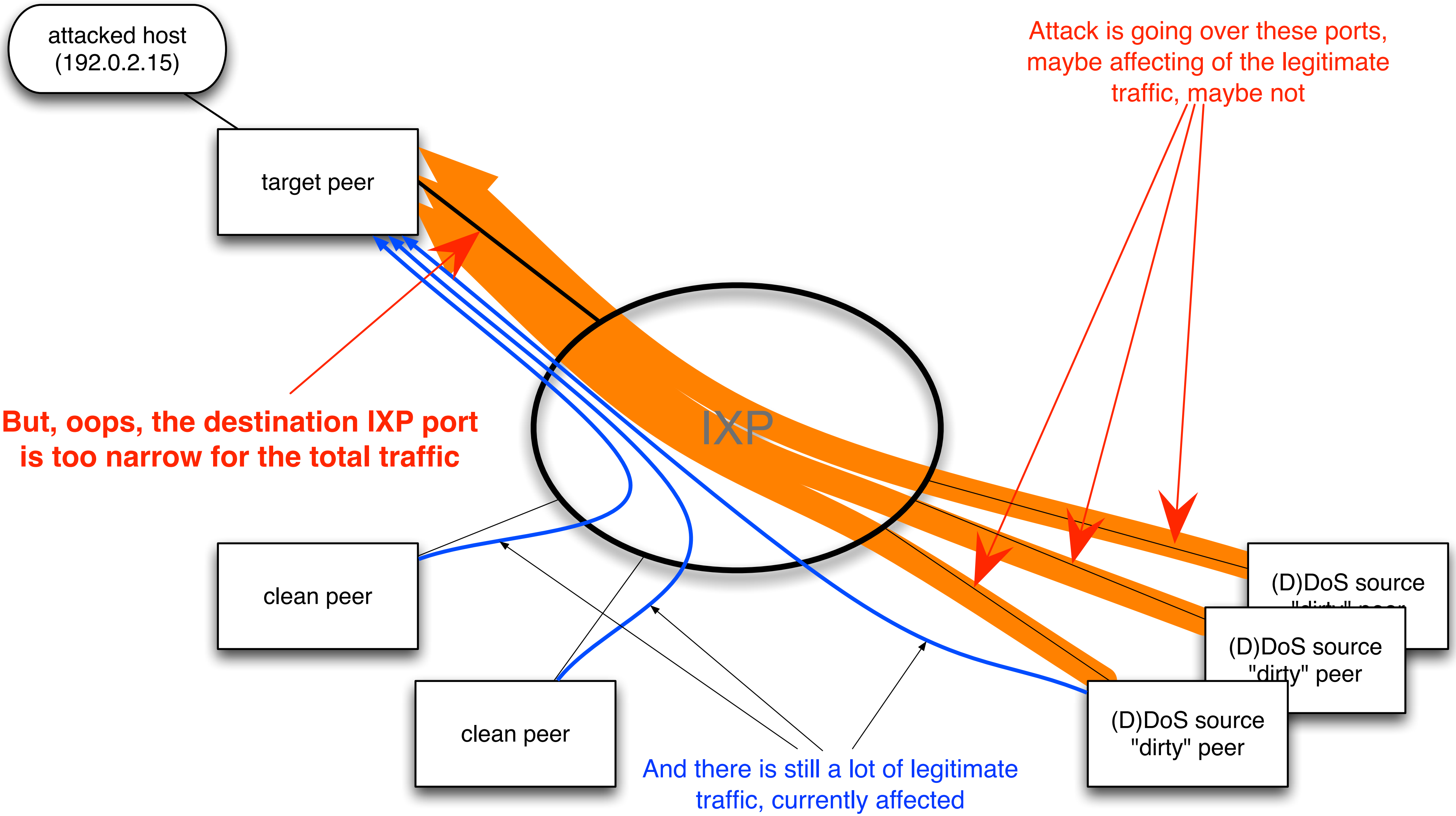
New generation of DDoS mitigation in NIX.CZ

Zbyněk Pospíchal
RIPE74, Budapest
10.5.2017

DDoS mitigation in an IXP: Why?

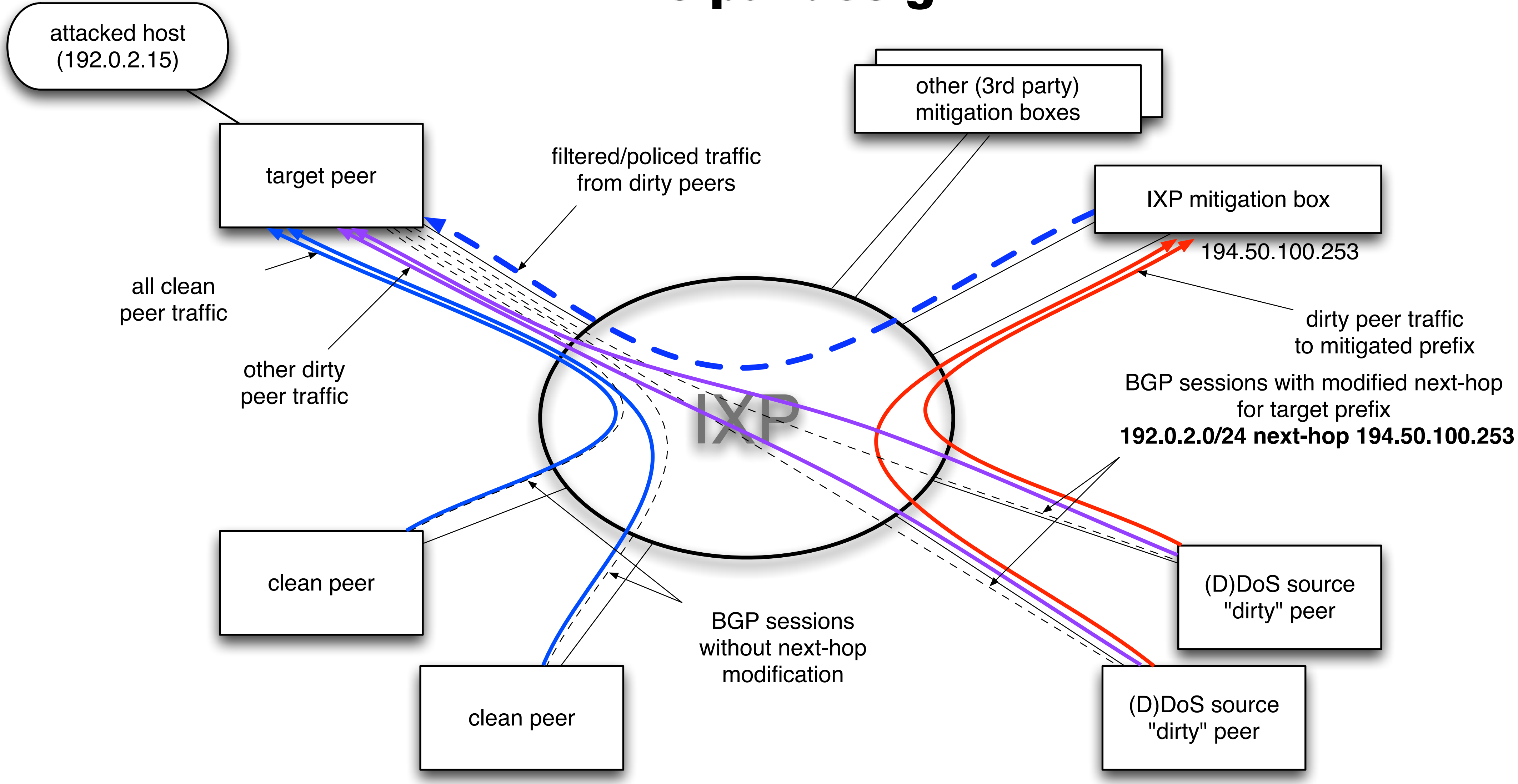


Attack is going over these ports, maybe affecting of the legitimate traffic, maybe not

But, oops, the destination IXP port is too narrow for the total traffic

And there is still a lot of legitimate traffic, currently affected

DDoS mitigation in IXP
Principal design



DDoS mitigation in IXP

Choosing the hardware and capacity

Only a portion of traffic reaches the mitigation device

Only a portion of such portion leaves the mitigation device

Existing junk routers/L3 switches versus specialized hardware

DDoS mitigation in IXP
NIX.CZ implementation

Based on Catalyst 6509E

currently used:

40Gbps in, 40 Gbps out

platform limits:

240 Gbps in, 80 Gbps out

DDoS mitigation in IXP
NIX.CZ implementation

Based on Catalyst 6509E

input interfaces in VRF(s)
output in GRT

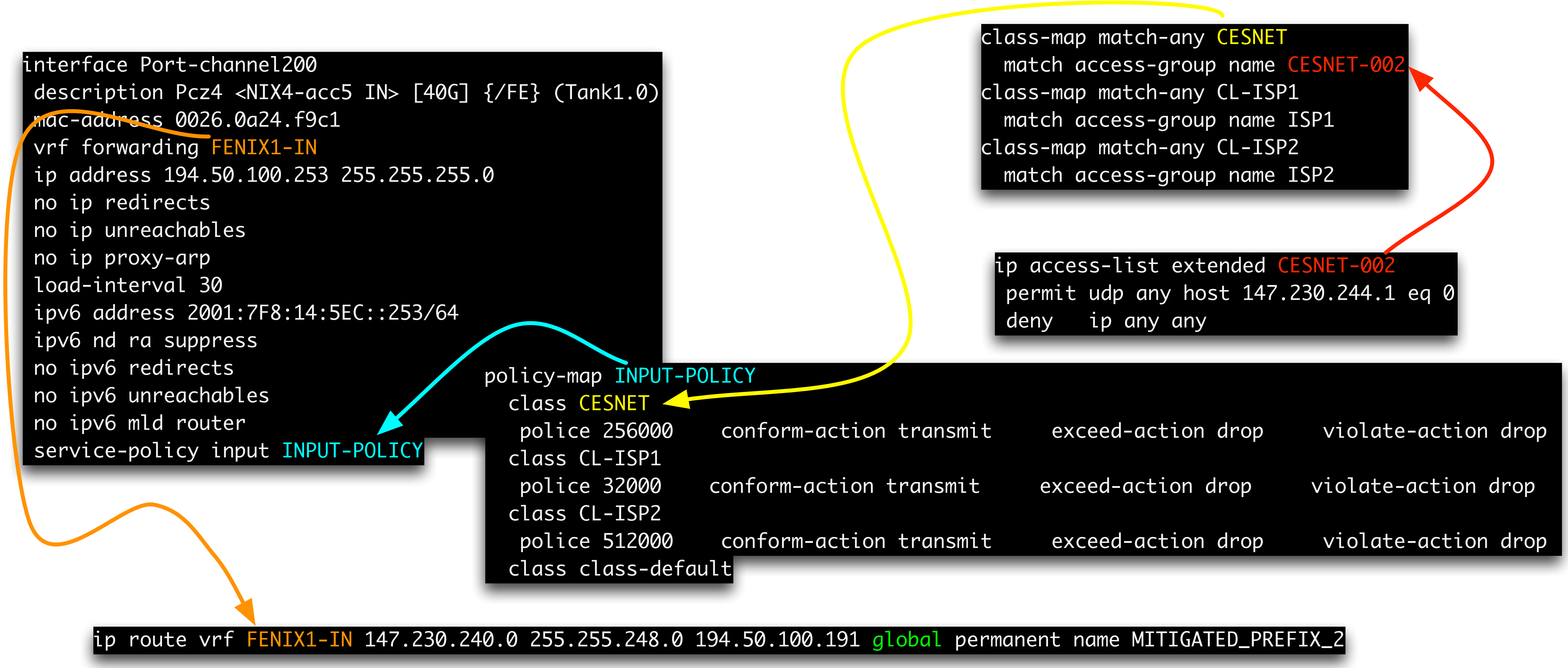
ACL -> class-map -> service-policy

ACL & class map for each participant

static route(s) to GRT for each mitigated pfx

ACL statistics, service-policy statistics

DDoS mitigation in IXP
UDP fragment attack mitigation



```
interface Port-channel200
 description Pcz4 <NIX4-acc5 IN> [40G] {/FE} (Tank1.0)
 mac-address 0026.0a24.f9c1
 vrf forwarding FENIX1-IN
 ip address 194.50.100.253 255.255.255.0
 no ip redirects
 no ip unreachables
 no ip proxy-arp
 load-interval 30
 ipv6 address 2001:7F8:14:5EC::253/64
 ipv6 nd ra suppress
 no ipv6 redirects
 no ipv6 unreachables
 no ipv6 mld router
 service-policy input INPUT-POLICY
```

```
class-map match-any CESNET
  match access-group name CESNET-002
class-map match-any CL-ISP1
  match access-group name ISP1
class-map match-any CL-ISP2
  match access-group name ISP2
```

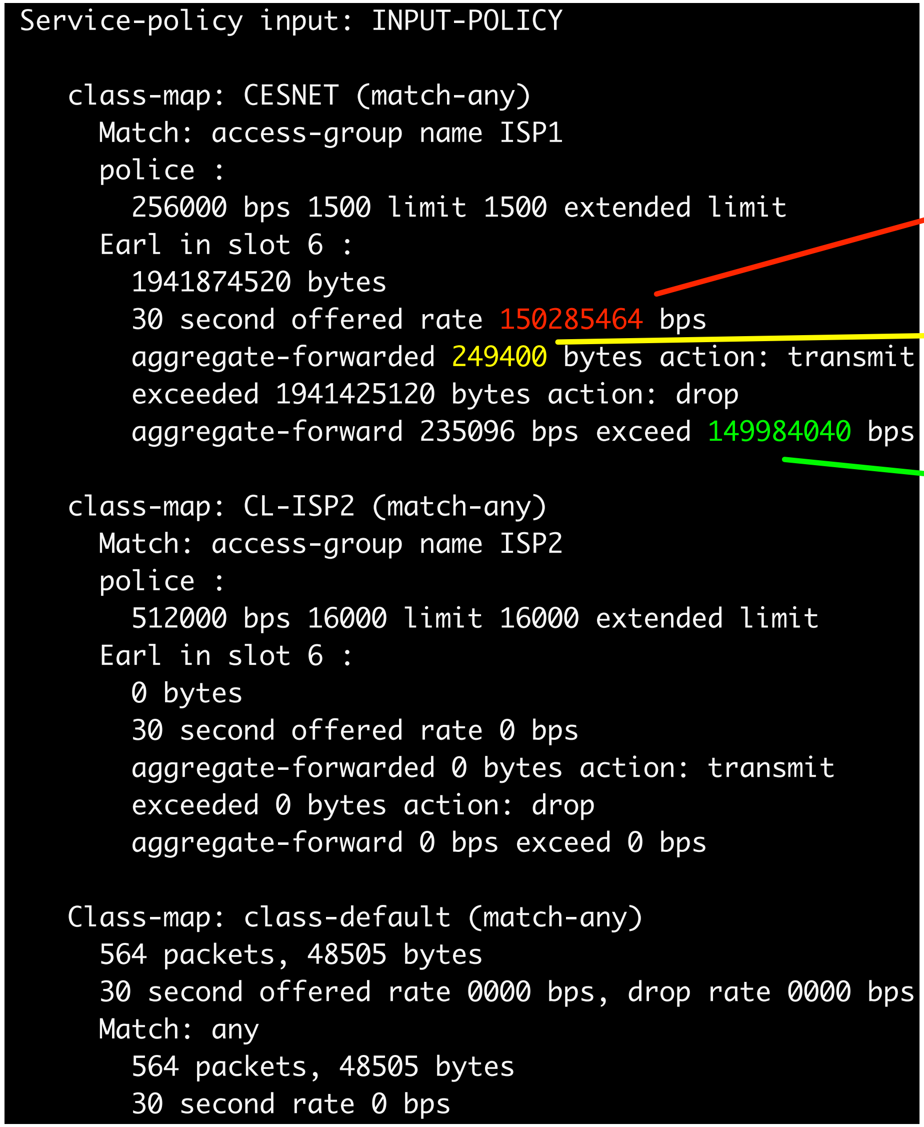
```
ip access-list extended CESNET-002
 permit udp any host 147.230.244.1 eq 0
 deny   ip any any
```

```
policy-map INPUT-POLICY
  class CESNET
   police 256000    conform-action transmit     exceed-action drop     violate-action drop
  class CL-ISP1
   police 32000    conform-action transmit     exceed-action drop     violate-action drop
  class CL-ISP2
   police 512000    conform-action transmit     exceed-action drop     violate-action drop
  class class-default
```

```
ip route vrf FENIX1-IN 147.230.240.0 255.255.248.0 194.50.100.191 global permanent name MITIGATED_PREFIX_2
```

more VRFs -> one such route in each VRF

DDoS mitigation in IXP
UDP fragment attack mitigation



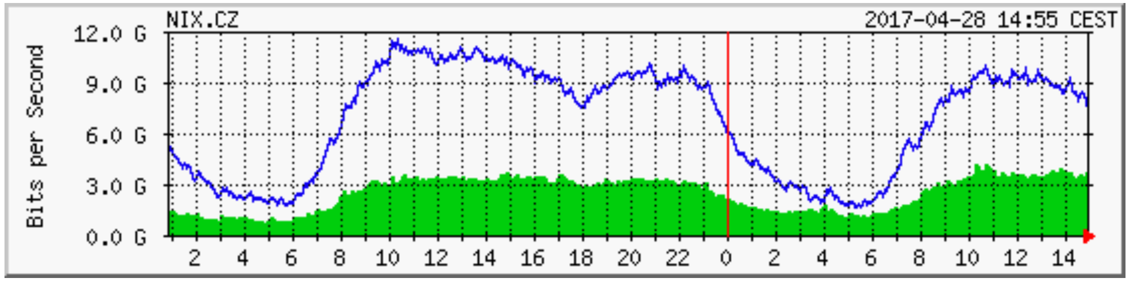
```
Service-policy input: INPUT-POLICY

   class-map: CESNET (match-any)
     Match: access-group name ISP1
     police :
       256000 bps 1500 limit 1500 extended limit
     Earl in slot 6 :
       1941874520 bytes
       30 second offered rate 150285464 bps
       aggregate-forwarded 249400 bytes action: transmit
       exceeded 1941425120 bytes action: drop
       aggregate-forward 235096 bps exceed 149984040 bps

   class-map: CL-ISP2 (match-any)
     Match: access-group name ISP2
     police :
       512000 bps 16000 limit 16000 extended limit
     Earl in slot 6 :
       0 bytes
       30 second offered rate 0 bps
       aggregate-forwarded 0 bytes action: transmit
       exceeded 0 bytes action: drop
       aggregate-forward 0 bps exceed 0 bps

   Class-map: class-default (match-any)
     564 packets, 48505 bytes
     30 second offered rate 0000 bps, drop rate 0000 bps
     Match: any
       564 packets, 48505 bytes
       30 second rate 0 bps
```

~150.2 Mbps of attack traffic

~250 kbps forwarded

the rest (~149.9 Mbps) is dropped

Total IXP traffic of the target network:



DDoS mitigation in IXP

NIX.CZ implementation

It works!

Even with junk hardware...

...with incredible possible capacity

Though, there is still a lot of disadvantages

DDoS mitigation in IXP
NIX.CZ implementation

Questions?