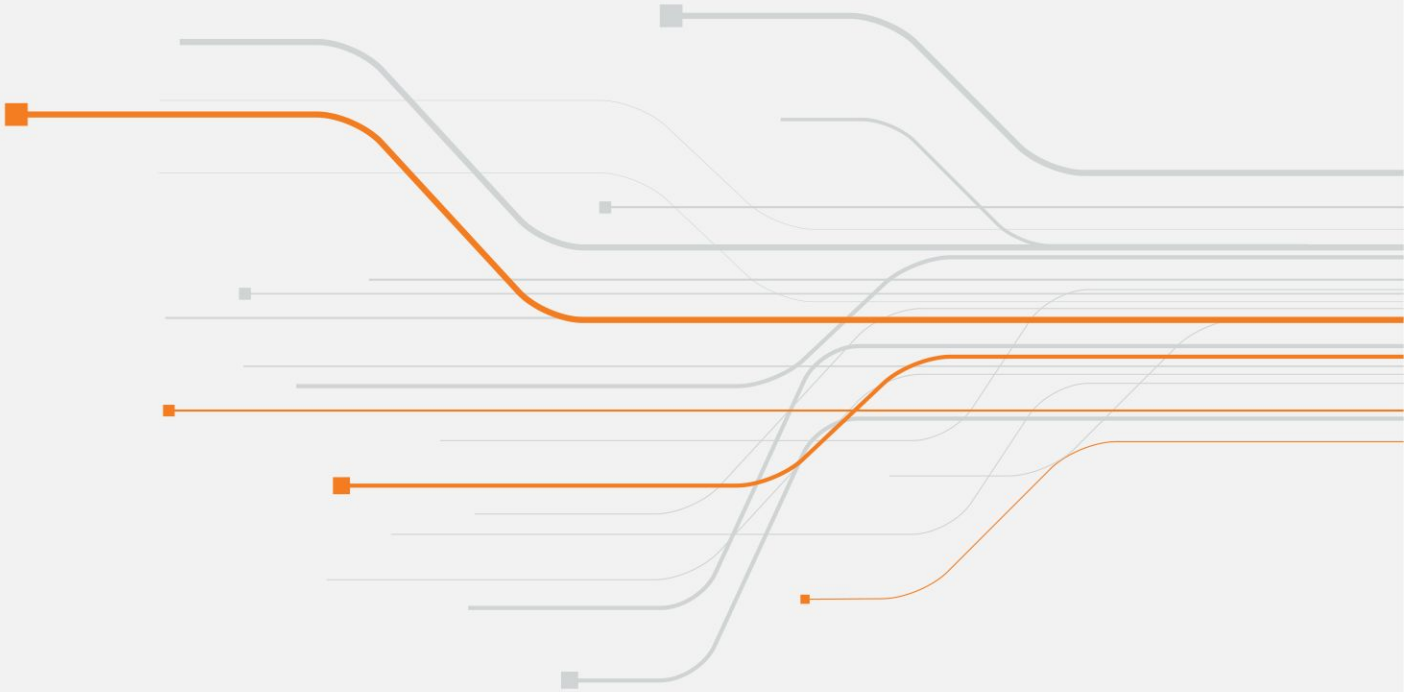
NOCTION
NETWORK INTELLIGENCE

BGP Network Traffic Geo-Blocking

Implementation Techniques and Best Practices

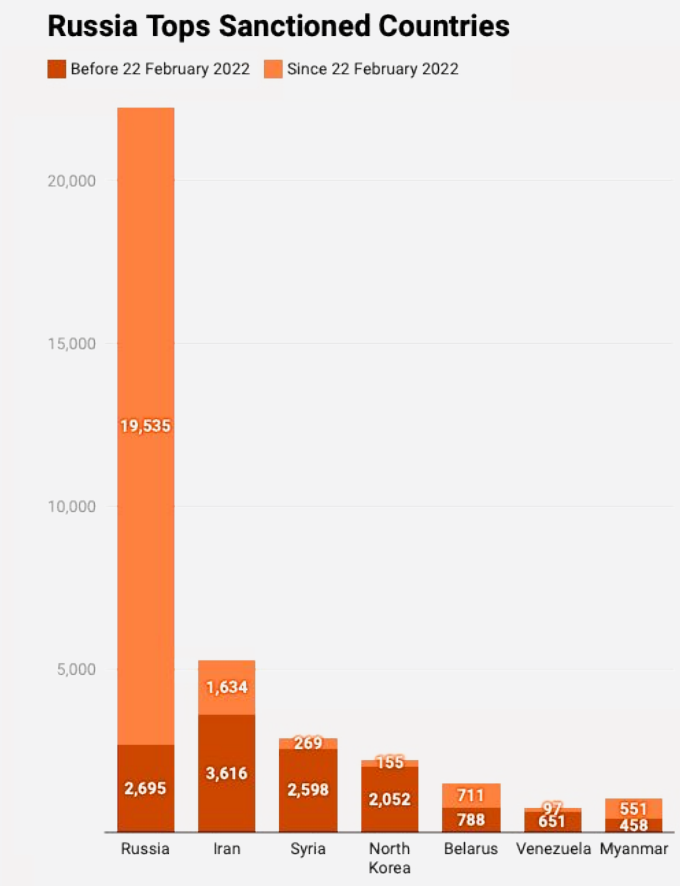


www.noction.com

Main Reasons for Geo-Blocking Implementation

- Compliance with imposed sanctions, laws and regulations
- Protecting network resources from security threats or excessive traffic
- Business objectives: content access control, pricing differentiation, etc.

Restrictive Sanctions:



Number of imposed sanctions per top countries (https://www.castellum.ai/russia-sanctions-dashboard)

Laws & Regulations:

71%

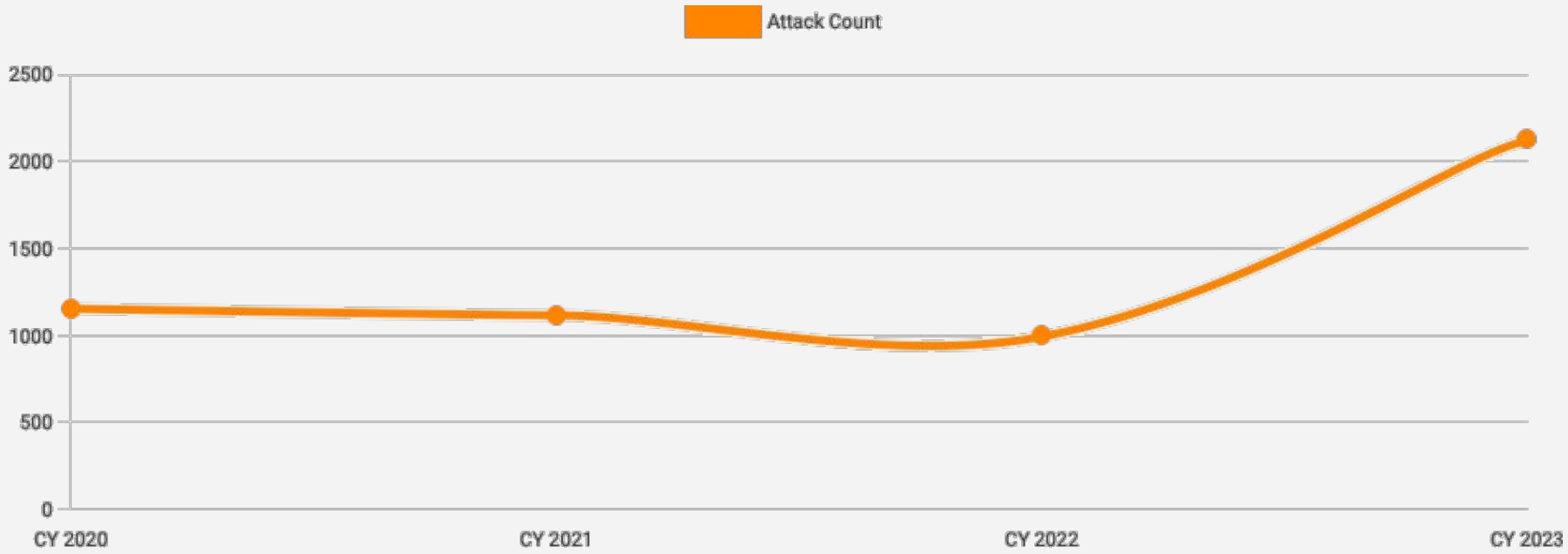
COUNTRIES WITH **CURRENT** LEGISLATION SIMILAR to GDPR

9%

COUNTRIES WITH **DRAFT** LEGISLATION SIMILAR to GDPR

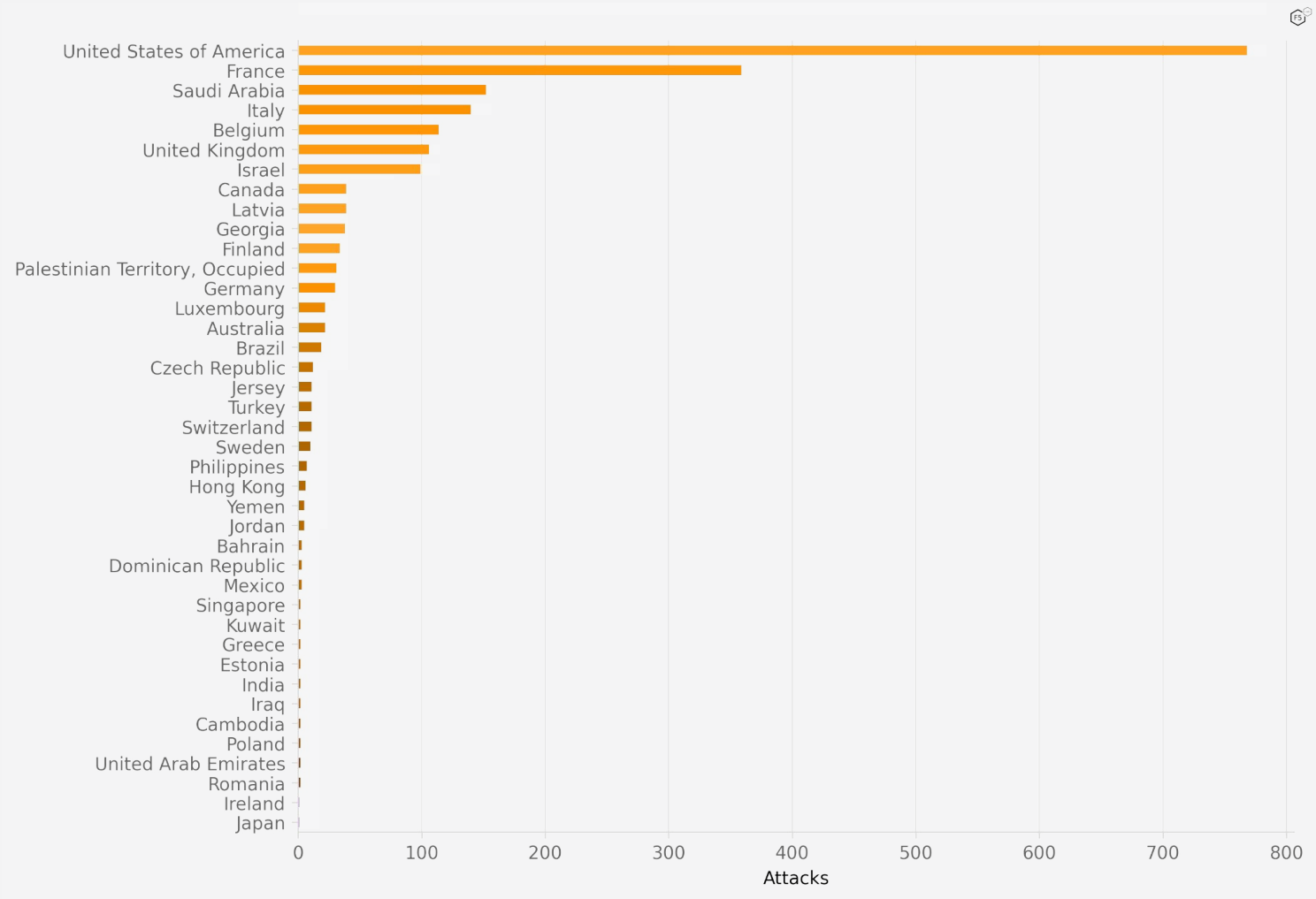
UN Trade and Development Commission Data (https://unctad.org/page/data-protection-and-privacy-legislation-worldwide)

DDoS attacks by numbers:



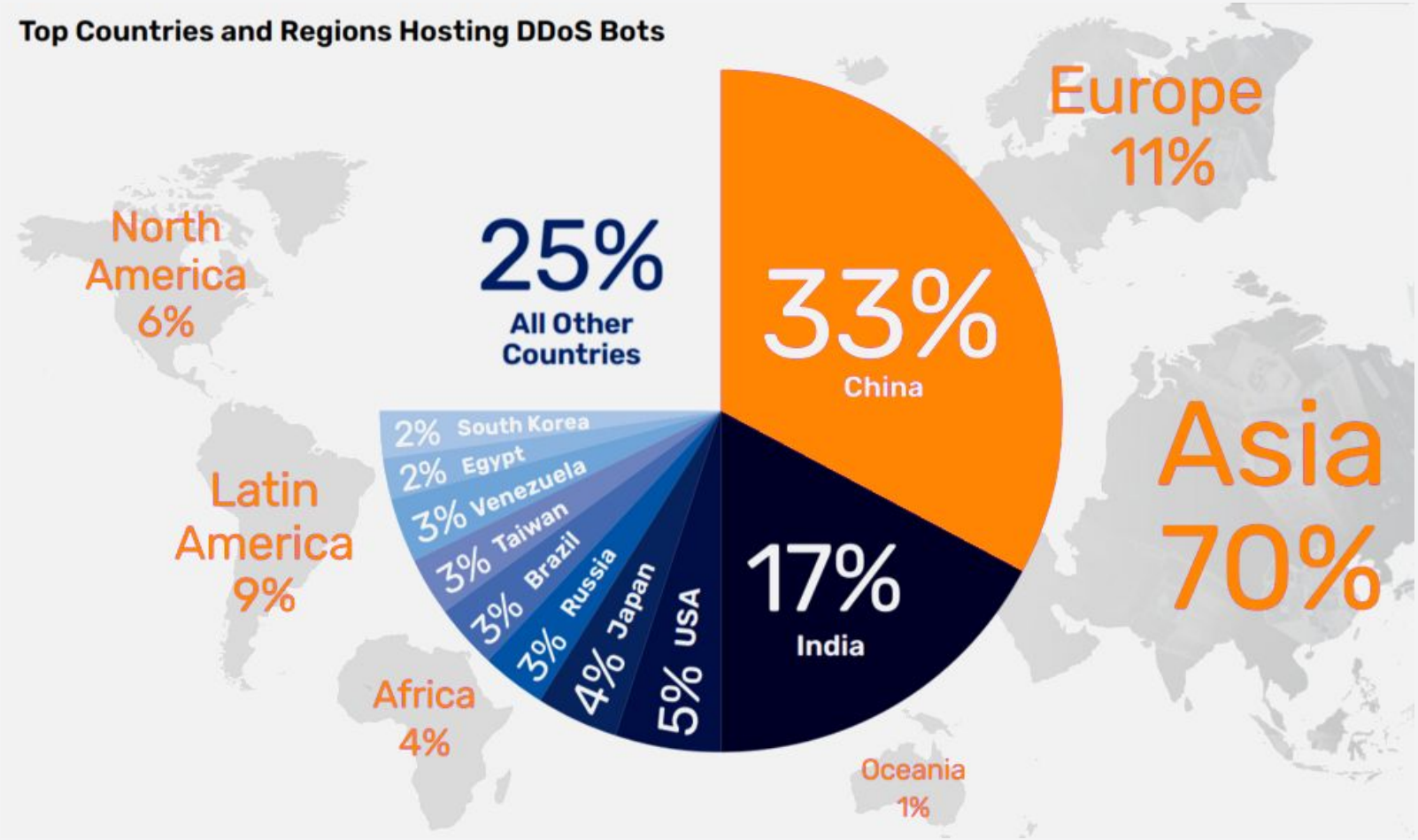
Count of DoS attacks by year (https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends)

DDoS attacks by number and geography:



Count of DoS attacks by target country (https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends)

DDoS attacks by number and geography:



Top Countries Hosting DDoS Bots (https://www.a10networks.com/wp-content/uploads/A10-EB-2024-DDoS-Weapons-Report.pdf)

Geo Blocking using BGP Communities:

North American country origins (2914:20–)	
2914:2000	us (United States)
2914:2001	ca (Canada)
European country origins (2914:22–)	
2914:2201	uk (United Kingdom)
2914:2202	de (Germany)
2914:2203	nl (Netherlands)
2914:2204	fr (France)
2914:2205	es (Spain)
2914:2207	pl (Poland)
2914:2208	bg (Bulgaria)
2914:2209	hu (Hungary)
2914:2210	ro (Romania)

Geo Blocking using FlowSpec:

- Traffic Filtering Based on IP Address Origin
- Dynamic and Flexible unlike traditional ACLs
- Easily applied at the scale of large networks

Geo Blocking using FlowSpec Policies:

Let’s make our hands dirty and add class-map/policy-map manually on Cisco ASR1K:

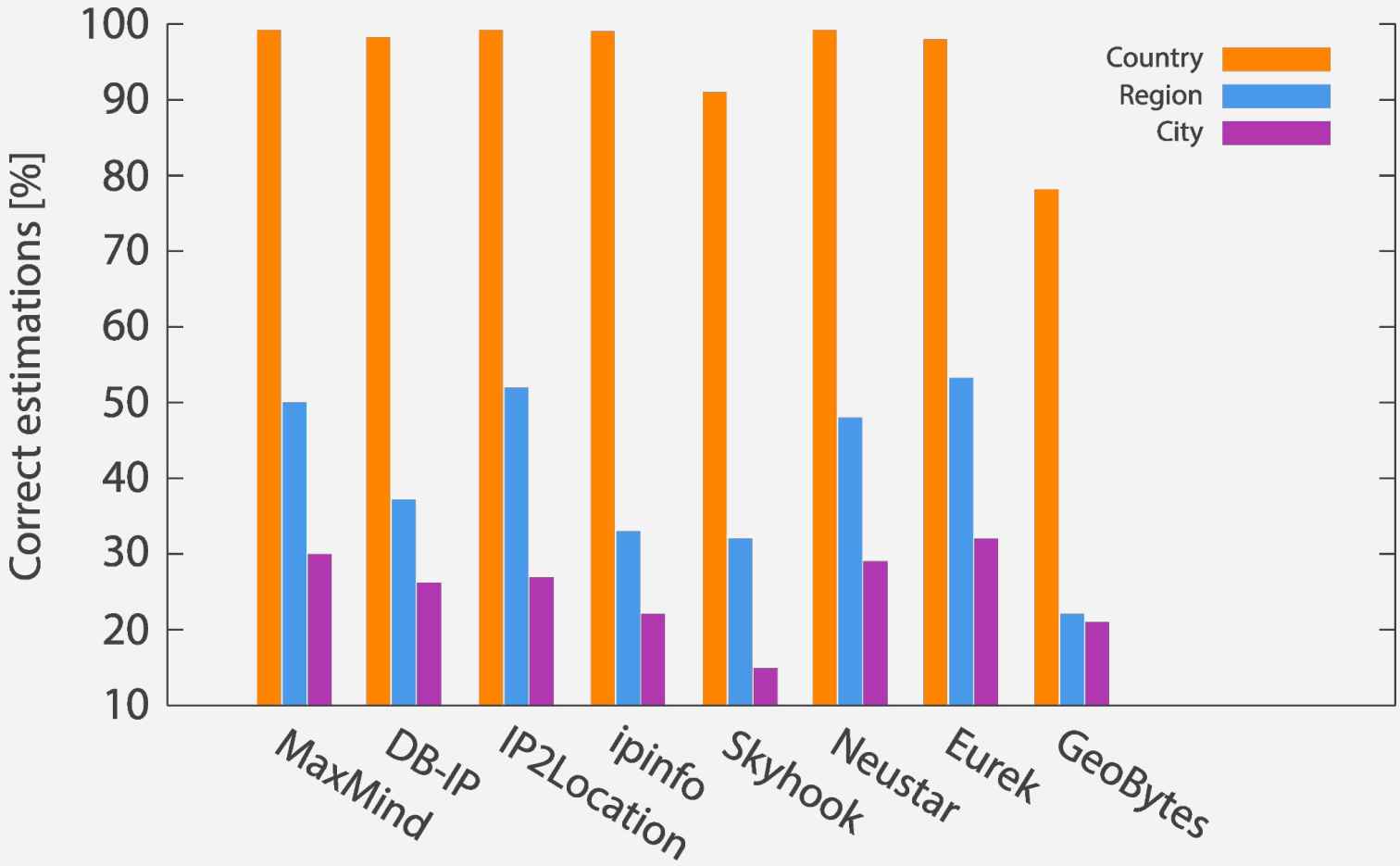
```
ip access-list standard BLOCK_BERMUDA
10 permit 44.164.140.0 0.0.3.255
11 permit 45.42.144.0 0.0.1.255
12 permit 63.85.42.0 0.0.1.255
13 permit 64.37.32.0 0.0.15.255
.....
77 permit 217.194.147.0 0.0.0.255

class-map type traffic match-all ICMP_IN
 match protocol icmp
 match access-group input name BLOCK_BERMUDA
 end-class-map

class-map type traffic match-all UDP_IN
 match protocol udp
 match access-group input name BLOCK_BERMUDA
 end-class-map

class-map type traffic match-all TCP_IN
 match protocol tcp
 match access-group input name BLOCK_BERMUDA
 end-class-map

policy-map type pbr BLOCK_ICMP_UDP_TCP_IN_BERMUDA
 class type traffic ICMP_IN
  drop
 class type traffic UDP_IN
  drop
 class type traffic TCP_IN
  drop
 class type traffic class-default

end-policy-map
```

```
class-map type traffic match-all ICMP_IN
 match protocol icmp
 match access-group output name BLOCK_BERMUDA
 end-class-map

class-map type traffic match-all UDP_IN
 match protocol udp
 match access-group output name BLOCK_BERMUDA
 end-class-map

class-map type traffic match-all TCP_IN
 match protocol tcp
 match access-group output name BLOCK_BERMUDA
 end-class-map


policy-map type pbr
BLOCK_ICMP_UDP_TCP_OUT_BERMUDA
 class type traffic ICMP_OUT
  drop
 class type traffic UDP_OUT
  drop
 class type traffic TCP_OUT
  drop
 class type traffic class-default

end-policy-map


 flowspec
  address-family ipv4
   service-policy type pbr
  BLOCK_ICMP_UDP_TCP_IN_BERMUDA
   service-policy type pbr
  BLOCK_ICMP_UDP_TCP_OUT_BERMUDA
```

show flowspec afi-all detail
Output:

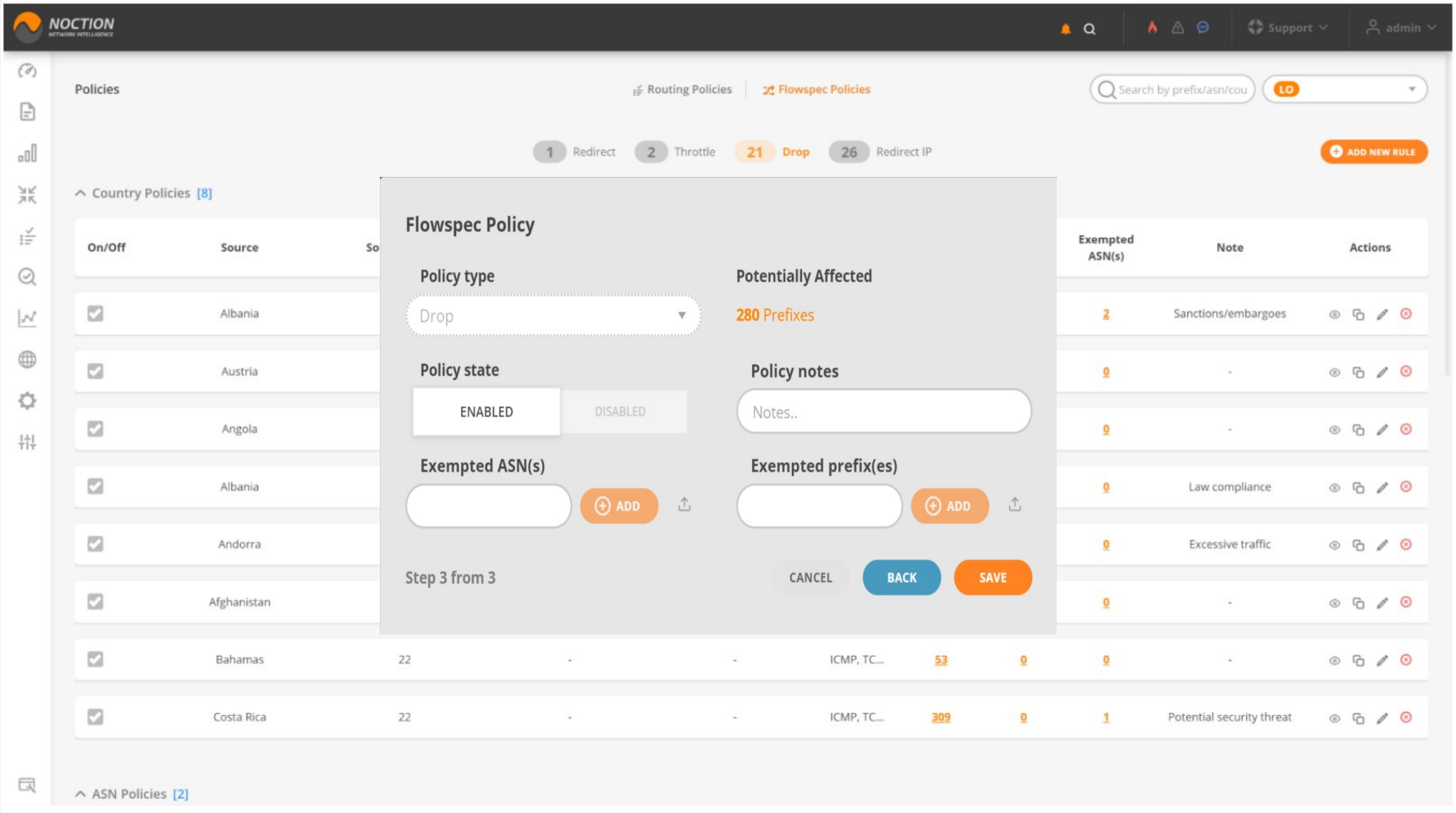
```
  Flow           :Source:44.164.140.0/22,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:45.42.144.0/22,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:63.85.42.0/23,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:64.37.32.0/20,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:64.147.80.0/20,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:65.171.98.0/24,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
  Flow           :Source:66.55.112.0/20,Proto:=1|=6|=17
    Actions      :Traffic-rate: 0 bps  (bgp.1)
    Statistics                        (packets/bytes)
      Matched             :                   0/0
      Dropped             :                   0/0
```

IP Geolocation Databases and their Accuracy:

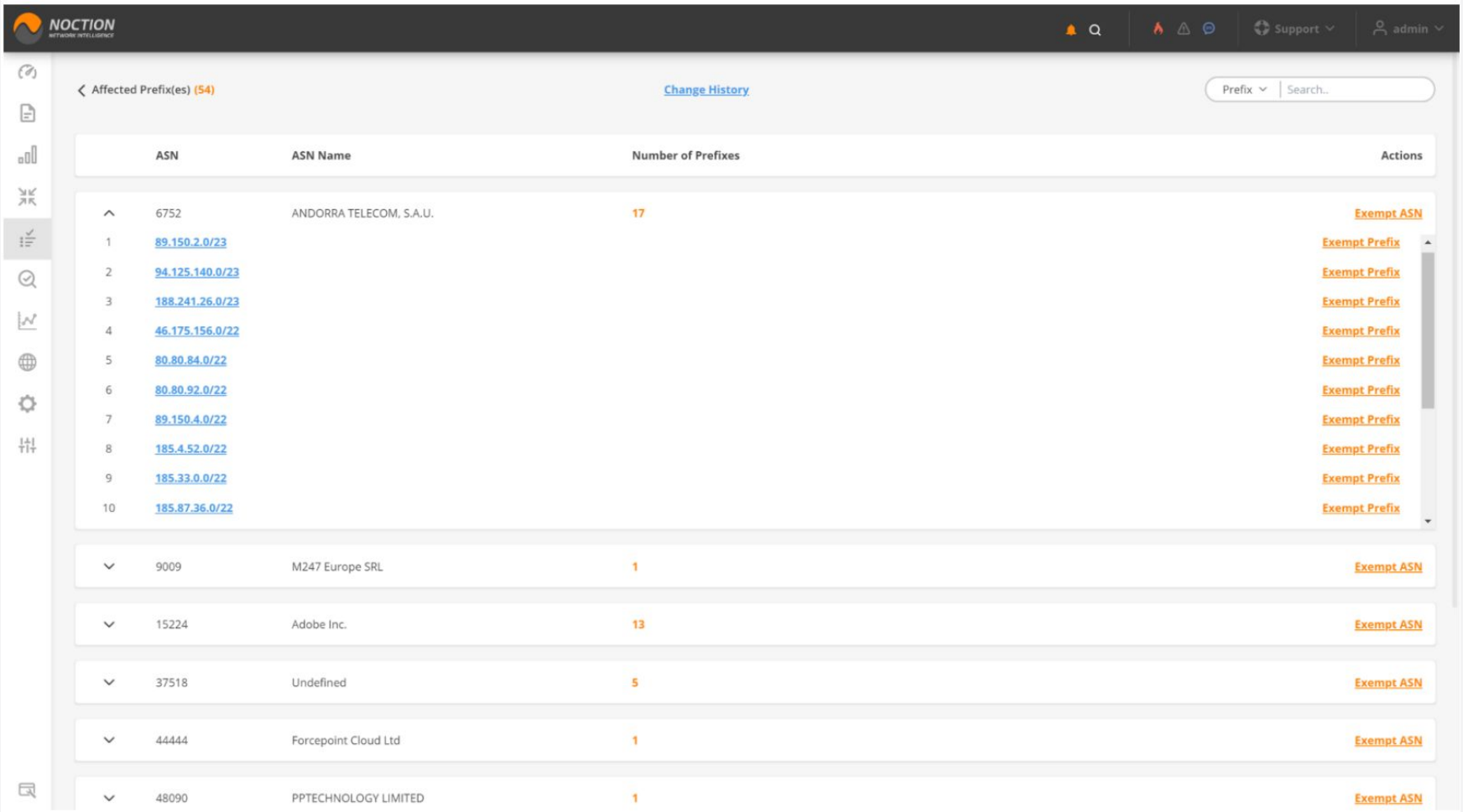


IP Geolocation Databases Accuracy % (https://itc.ktu.lt/index.php/ITC/article/view/14451)

Policies by Country in IRP:



Affected Prefixes in Policies by Country:



THANK YOU

Have questions?

info@noction.com | www.noction.com

omaculetchi@noction.com