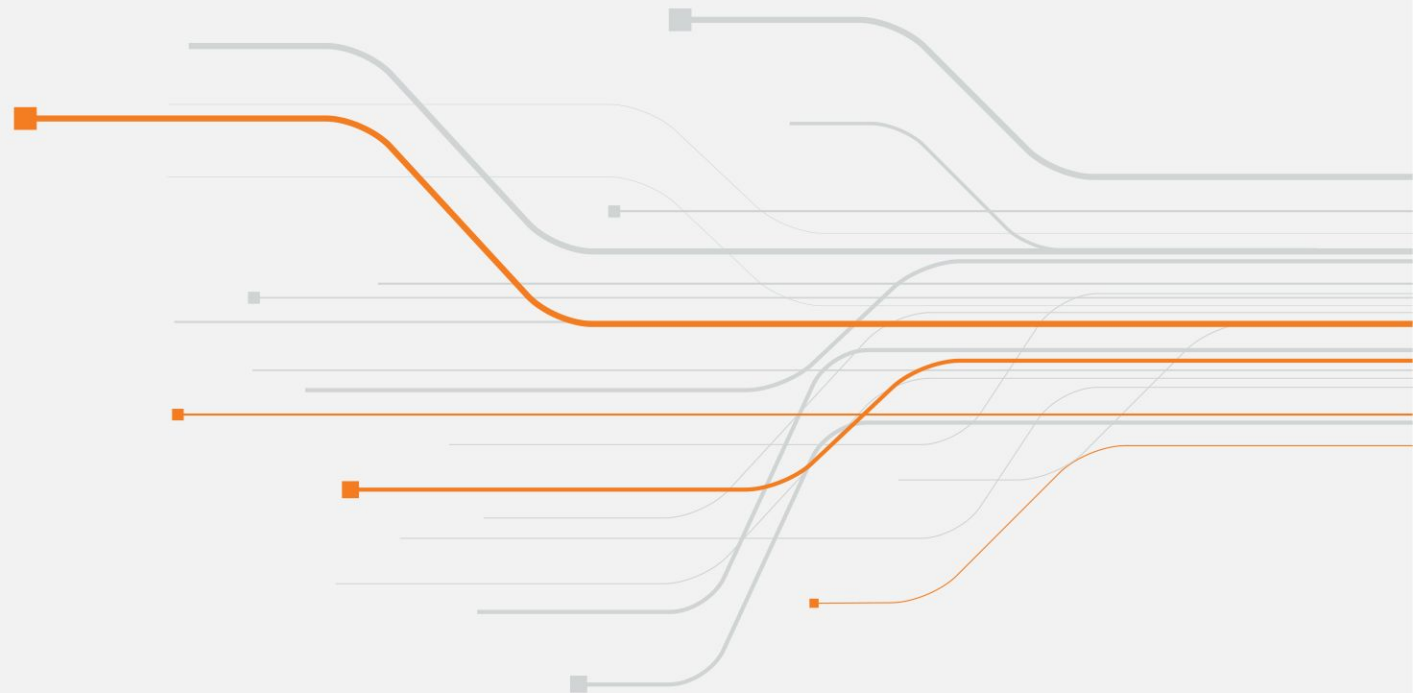




BGP Network Traffic Geo-Blocking

Implementation Techniques and Best Practices



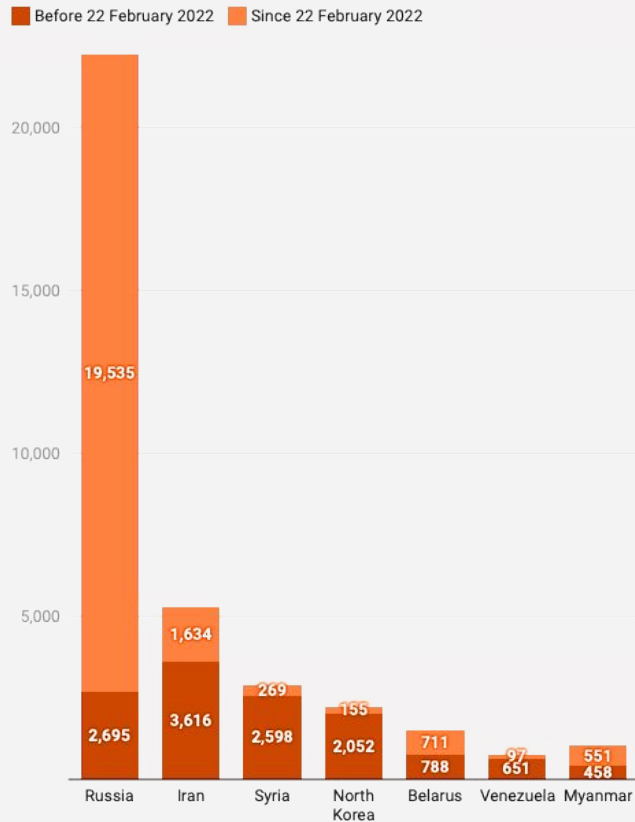
Main Reasons for Geo-Blocking Implementation

- ➔ 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:

Russia Tops Sanctioned Countries



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

Laws & Regulations:

71%

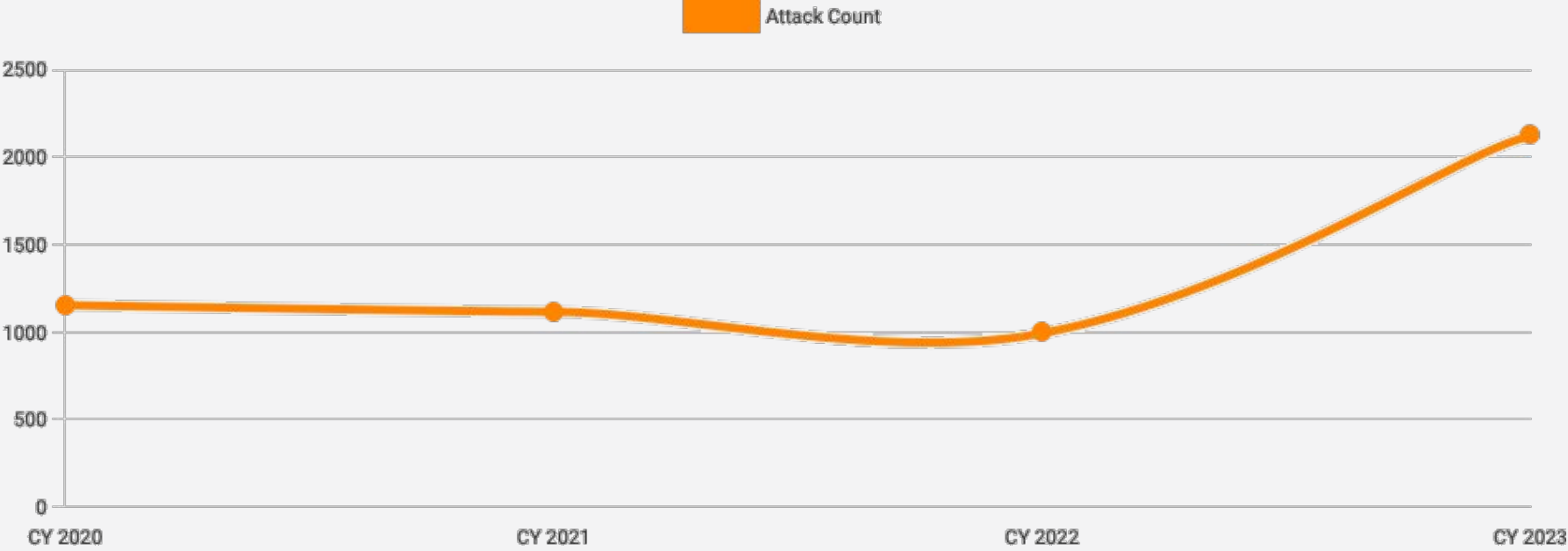
COUNTRIES WITH **CURRENT**
LEGISLATION SIMILAR to GDPR

9%

COUNTRIES WITH **DRAFT**
LEGISLATION SIMILAR to GDPR

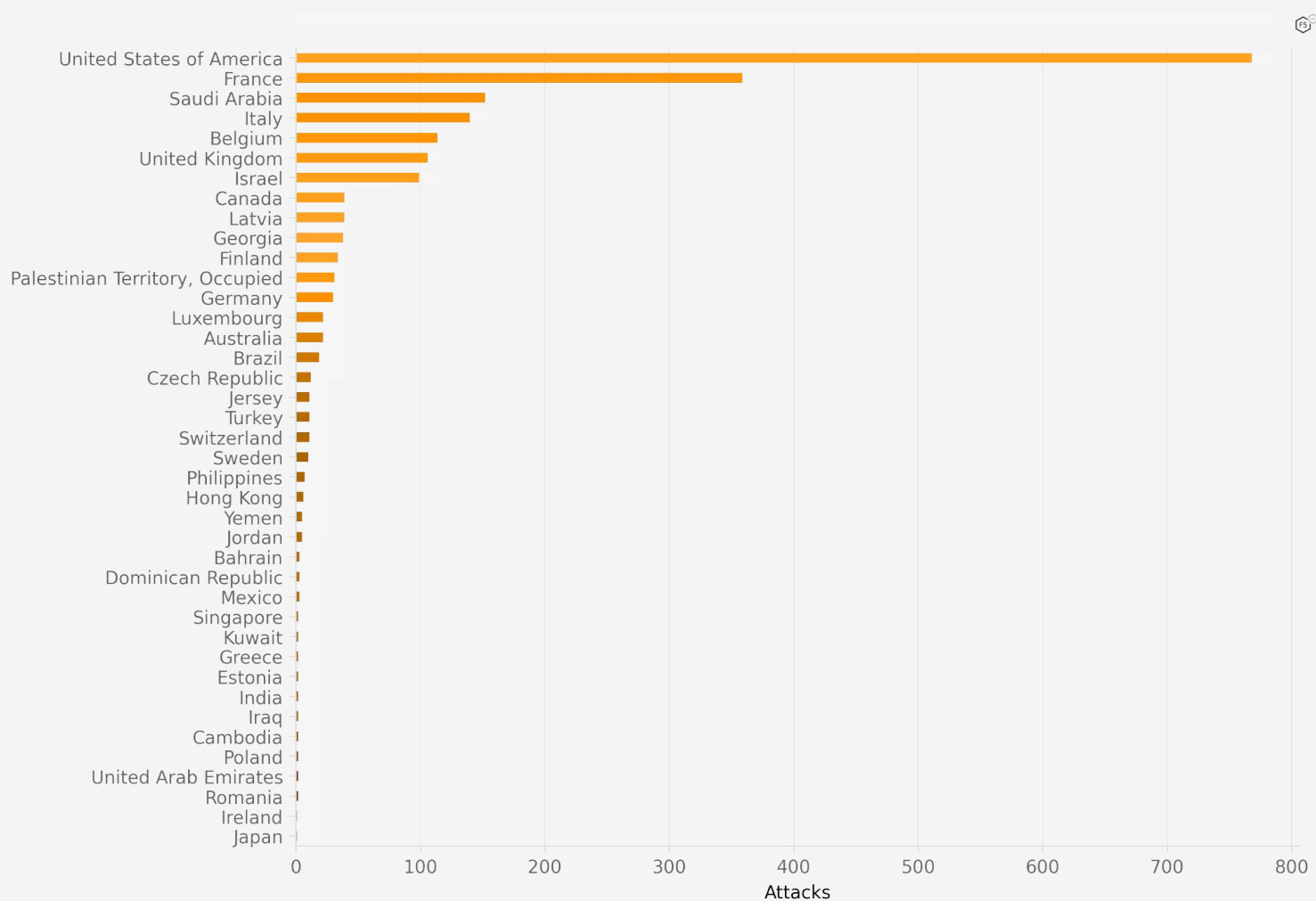
UN Trade and Development Commission Data
(<https://unctad.org/page/data-protection-and-privacy-legislation-worldwide>)

DDoS attacks by numbers:



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

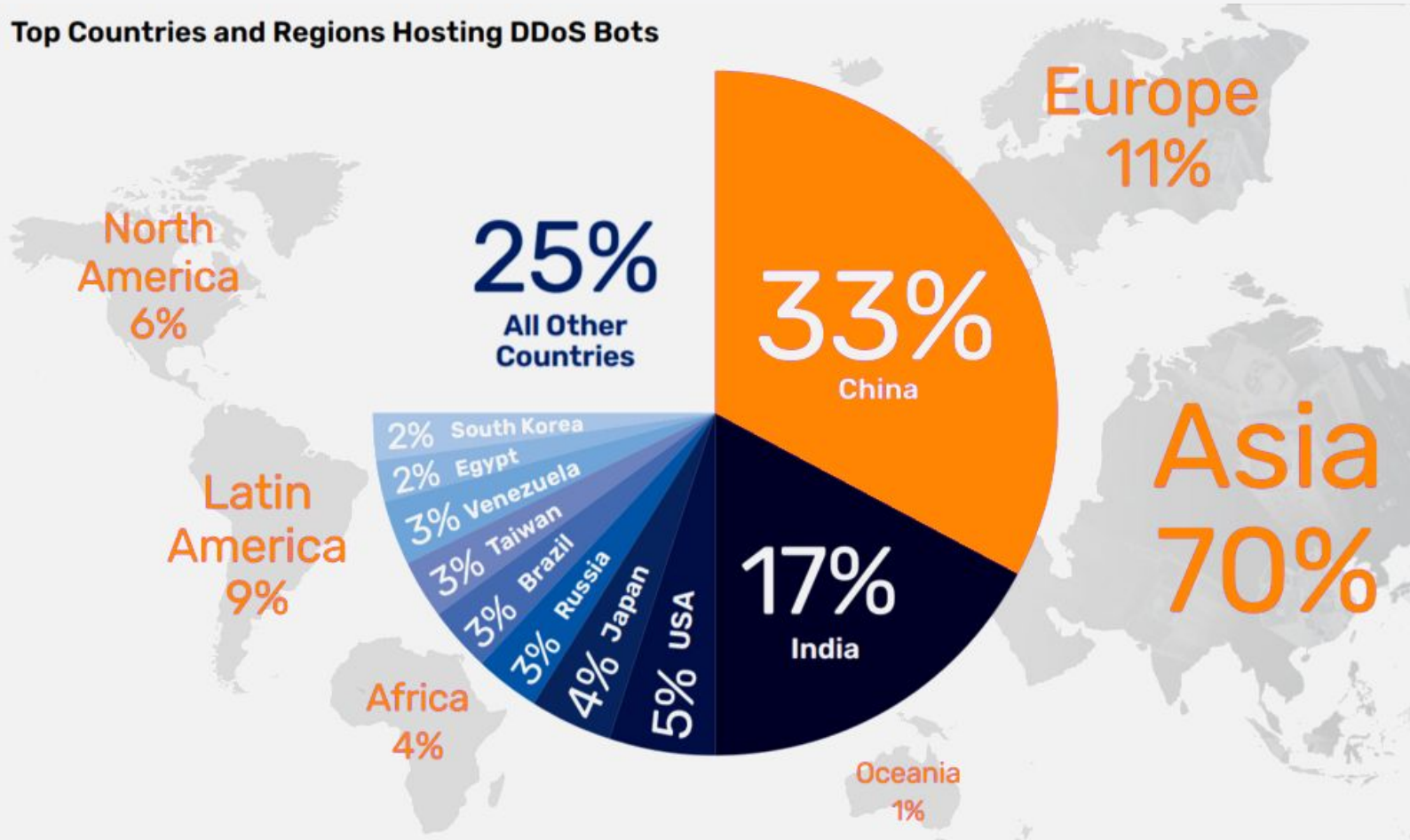
DDoS attacks by number and geography:



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 and Regions Hosting DDoS Bots



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

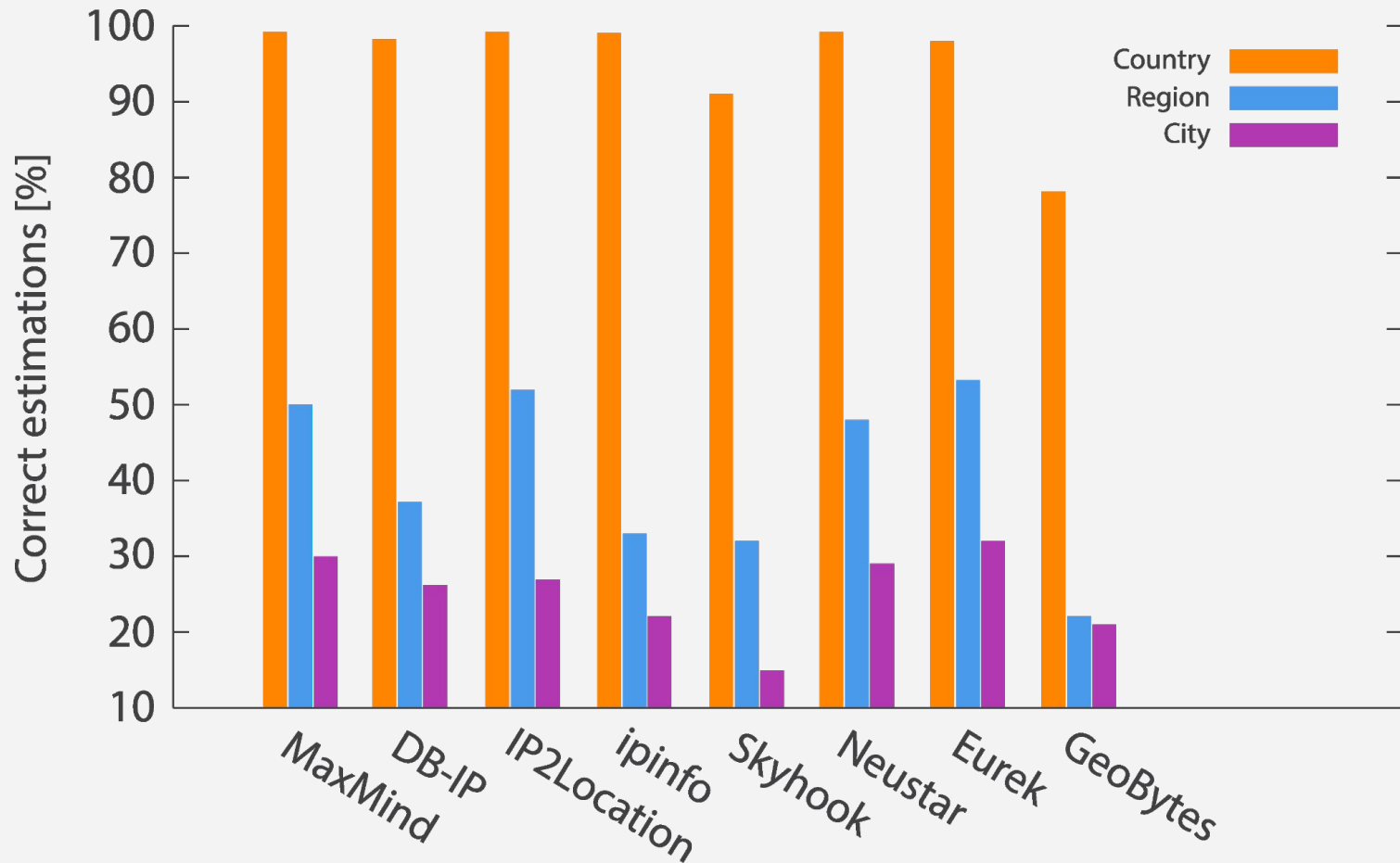
end-policy-map

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:



Policies by Country in IRP:

The screenshot displays the NOCTION IRP interface. At the top, the NOCTION logo and navigation icons are visible. The main area is titled 'Policies' and shows 'Routing Policies' and 'Flowspec Policies' tabs. A search bar is present with the text 'Search by prefix/asn/cou'. Below the search bar, there are filters for '1 Redirect', '2 Throttle', '21 Drop', and '26 Redirect IP'. An 'ADD NEW RULE' button is also visible.

The 'Country Policies [8]' section is expanded, showing a list of countries with checkboxes. The 'Albania' row is selected, and a 'Flowspec Policy' modal is open. The modal is titled 'Flowspec Policy' and shows the following details:

- Policy type:** Drop
- Potentially Affected:** 280 Prefixes
- Policy state:** ENABLED (with a DISABLED button)
- Policy notes:** Notes..
- Exempted ASN(s):** (empty field with an ADD button)
- Exempted prefix(es):** (empty field with an ADD button)

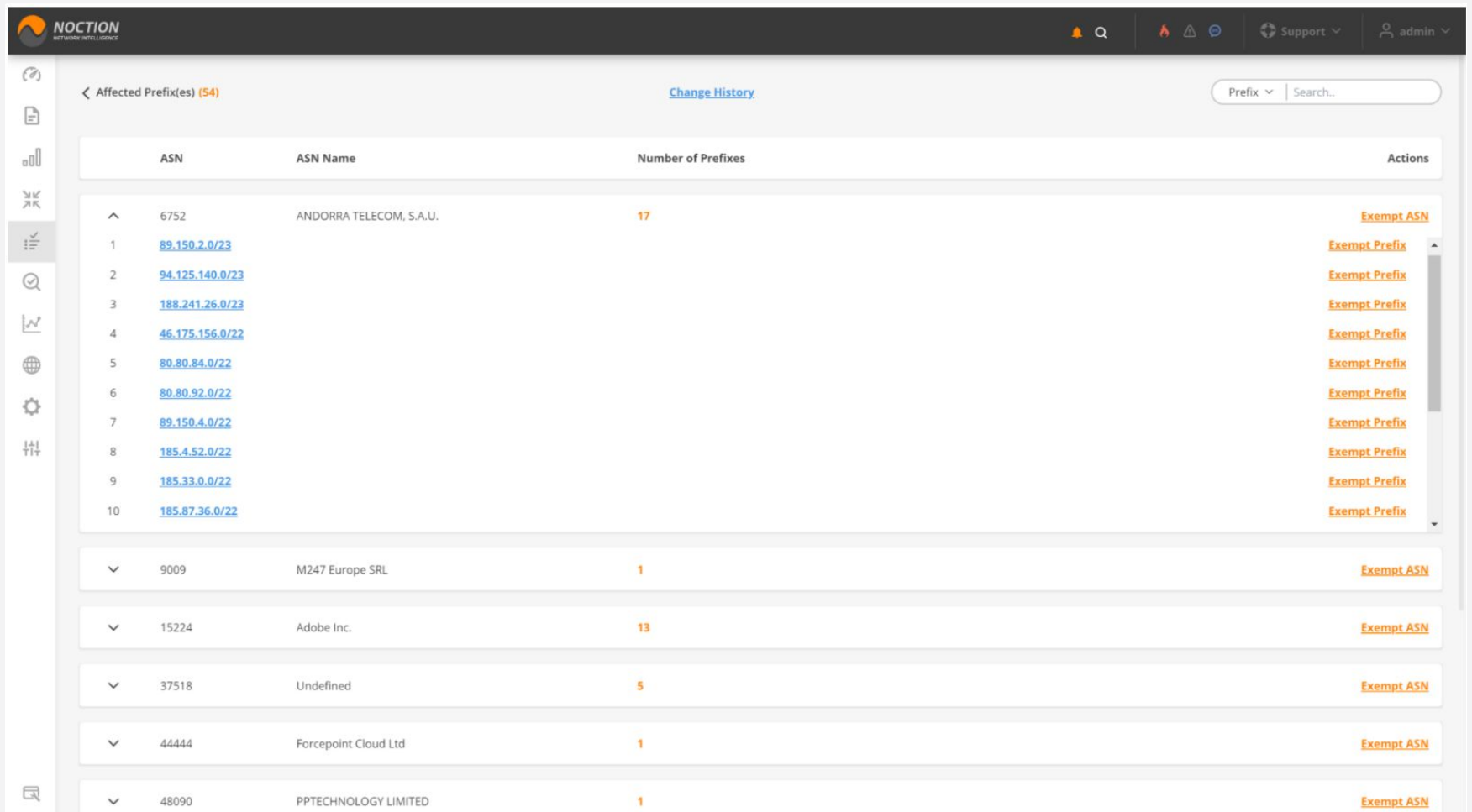
The modal also shows 'Step 3 from 3' and buttons for 'CANCEL', 'BACK', and 'SAVE'.

The background table shows the following data for Country Policies:

On/Off	Source	So
<input checked="" type="checkbox"/>	Albania	
<input checked="" type="checkbox"/>	Austria	
<input checked="" type="checkbox"/>	Angola	
<input checked="" type="checkbox"/>	Albania	
<input checked="" type="checkbox"/>	Andorra	
<input checked="" type="checkbox"/>	Afghanistan	
<input checked="" type="checkbox"/>	Bahamas	22
<input checked="" type="checkbox"/>	Costa Rica	22

The 'ASN Policies [2]' section is also visible at the bottom of the interface.

Affected Prefixes in Policies by Country:



The screenshot displays the NOCTION Network Intelligence interface. The main content area shows a table titled "Affected Prefix(es) (54)" with a "Change History" link. The table has four columns: "ASN", "ASN Name", "Number of Prefixes", and "Actions". The first entry is for ASN 6752 (ANDORRA TELECOM, S.A.U.) with 17 affected prefixes. A list of 10 prefixes is shown, each with an "Exempt Prefix" action. Below this, other ASNs are listed with their respective prefix counts and "Exempt ASN" actions.

ASN	ASN Name	Number of Prefixes	Actions
6752	ANDORRA TELECOM, S.A.U.	17	Exempt ASN
1	89.150.2.0/23		Exempt Prefix
2	94.125.140.0/23		Exempt Prefix
3	188.241.26.0/23		Exempt Prefix
4	46.175.156.0/22		Exempt Prefix
5	80.80.84.0/22		Exempt Prefix
6	80.80.92.0/22		Exempt Prefix
7	89.150.4.0/22		Exempt Prefix
8	185.4.52.0/22		Exempt Prefix
9	185.33.0.0/22		Exempt Prefix
10	185.87.36.0/22		Exempt Prefix
9009	M247 Europe SRL	1	Exempt ASN
15224	Adobe Inc.	13	Exempt ASN
37518	Undefined	5	Exempt ASN
44444	Forcepoint Cloud Ltd	1	Exempt ASN
48090	PPTECHNOLOGY LIMITED	1	Exempt ASN

THANK YOU

Have questions?

info@noction.com | www.noction.com

omaculechi@noction.com

