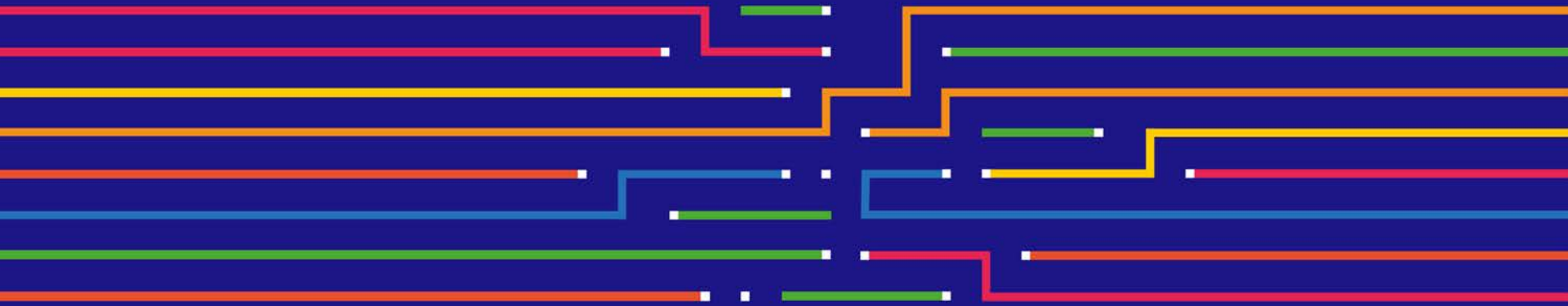


RedCLARA
NETWORK ENGINEERING GROUP

INTEGRATED MONITORING PORTAL FOR LATIN AMERICAN NRENs

Tiago Monsores, Lead Network Engineer

What is RedCLARA?

RedCLARA is the result of cooperation between Latin American countries to create a high-capacity network dedicated to research and education.

What is RedCLARA?

We strengthen the development of science, education, culture and innovation in Latin America, through the innovative use of networks, infrastructure and advanced information technologies.

What is RedCLARA?

Today this cooperation has 9 countries totaling 15,759,828 km² of territory. This vast territory must be covered by national networks, making it possible to reach the most diverse regions.

RNP

cedia

REUNA
Ciencia y Educación en Red

RENATA
COLOMBIA

InnovaRed
Red Nacional de Investigación
y Educación de Argentina

RaU

CONARE

ragie

cudi


GÉANT


INTERNET2


canarie


TENET
South Africa


SINET6

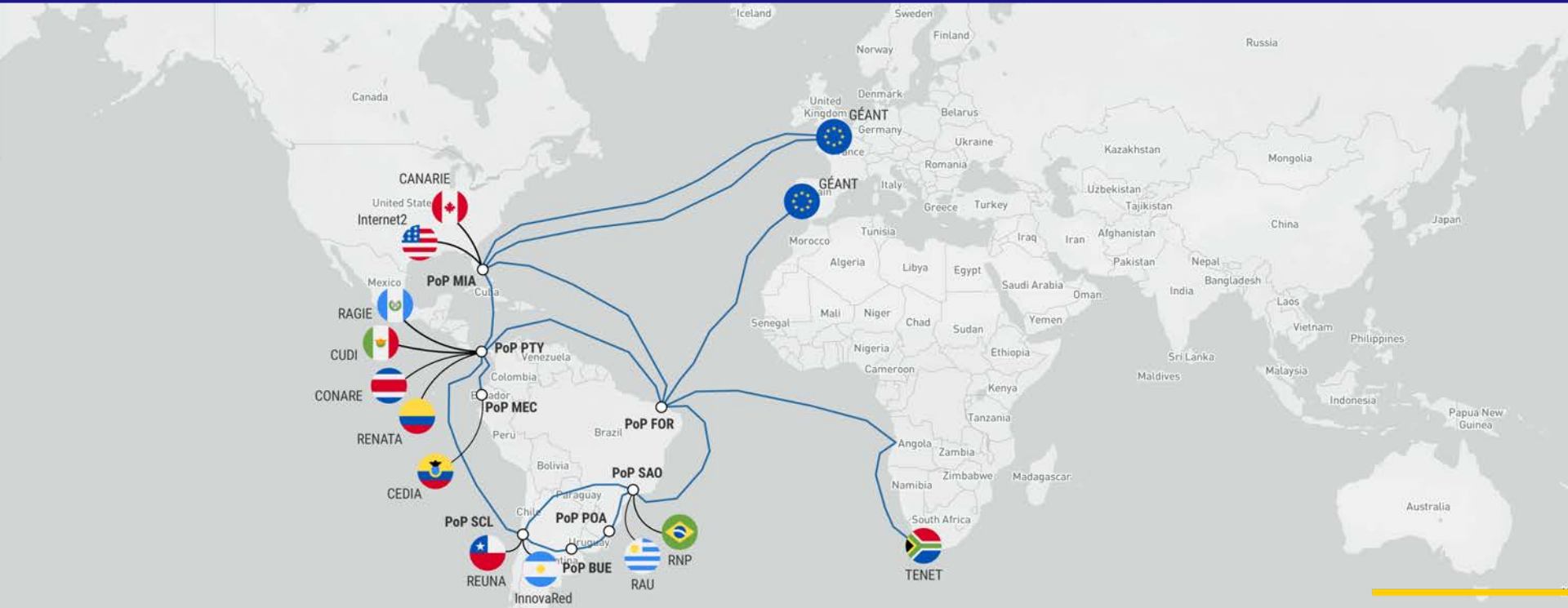

ESnet
ENERGY SCIENCES NETWORK


AmLight ExP
Americas Lightpaths Express & Protect


SoX
Southern Crossroads


NSRC
Network Startup Resource Center

RedCLARA
NETWORK ENGINEERING GROUP



Network characteristics

- High capacity: all backbone links are +100Gbps
- Predictability: traffic flows through a coherent path
- Security: MANRS participant with all 4 actions implemented + 100% score
- Robust monitoring

NEG Systems

Grafana
Network traffic monitoring

chronograf
Virtual machines monitoring

graylog
Management of log messages

ElastiFlow
Collects and analyzes network flows

Oxidized
Configuration backup and management

ZABBIX
Monitoring and alerting system

Pushover
Push notifications system

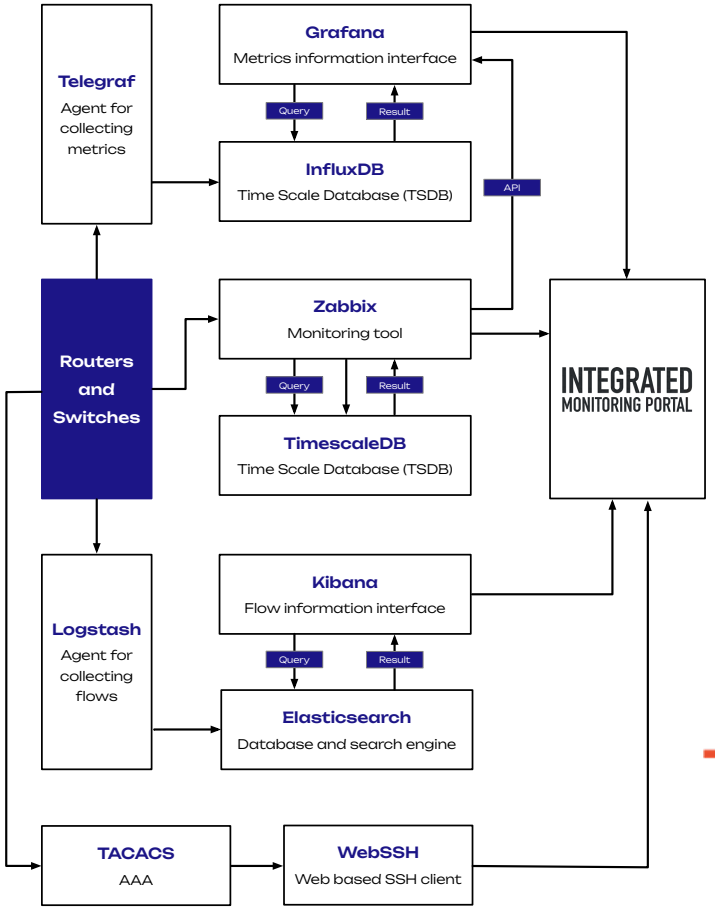
TACACSGUI
User authentication, and command authorization and accounting

ROUTINATOR
RPKI validation system

Integrated Monitoring Portal

- One of the most requested features from RedCLARA members was network visibility
- Network monitoring was present, but information was internal

Architecture

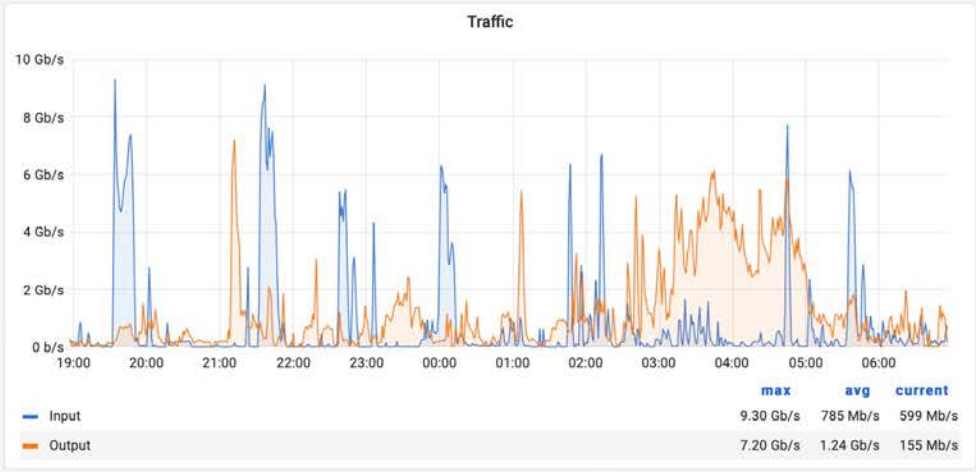


Graphical Interface and Authentication

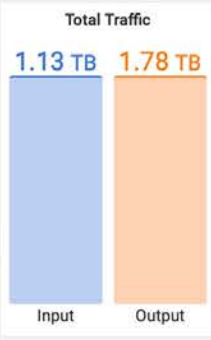
- Graphical interface built with Drupal
- Drupal is an open source Content Management System (CMS)
- Authentication uses Shibboleth for federated login
- Created by SEG (System Engineering Group)

Traffic and BGP Monitoring

- SNMP metrics collected with Telegraf using a polling time of 30 seconds
- Latency measured with IP SLA
- Data is stored in InfluxDB
- Availability and Alerts provided by Zabbix
- Dashboards built with Grafana

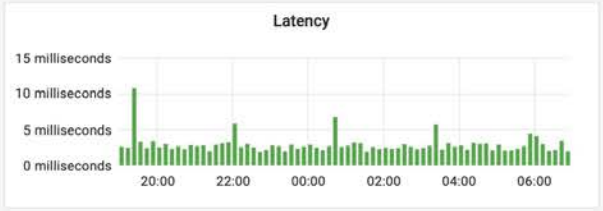


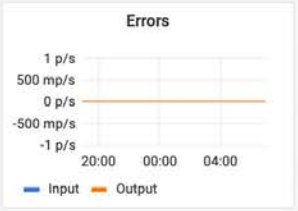
RedCLARA NETWORK ENGINEERING GROUP

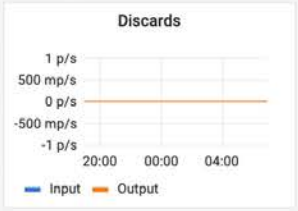


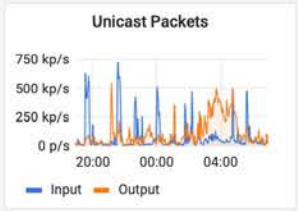
BGP state	Established
Uptime	108 d 12:11:46
SLA (last 30 days)	100.0000%

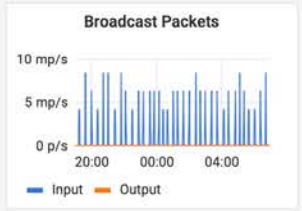
Accepted prefixes 3	Denied prefixes 0
Advertised prefixes 5,854	Suppressed prefixes 2,875
Withdrawn prefixes 542	Prefixes limit 1.05 Mil

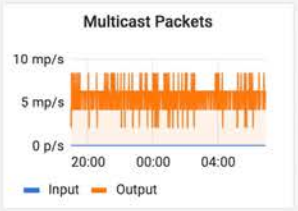


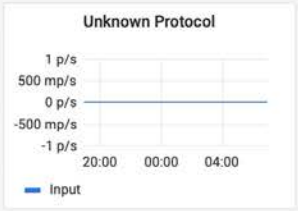




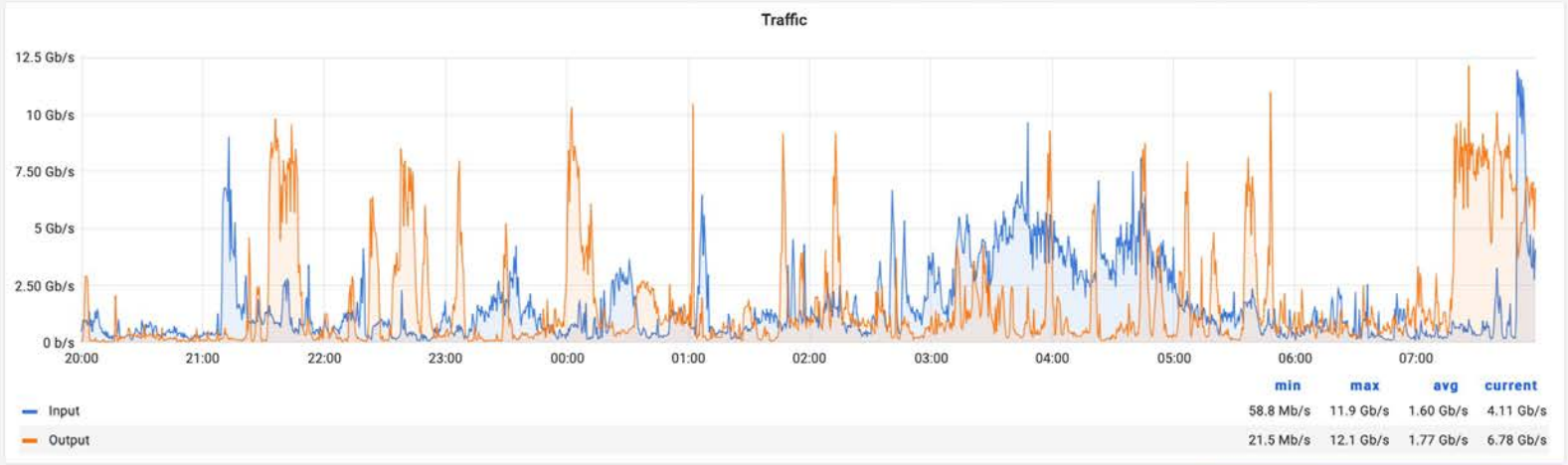


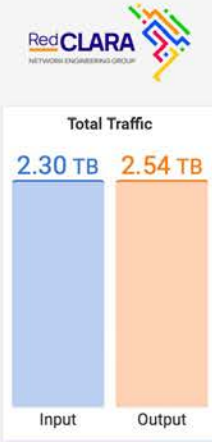


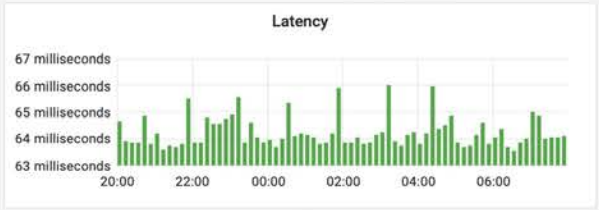


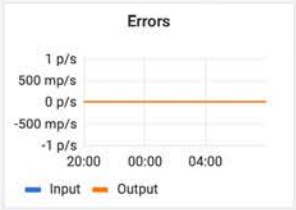


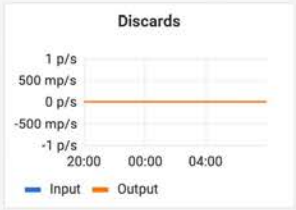
Alerts — Last 30 days


Traffic
12.5 Gb/s
10 Gb/s
7.50 Gb/s
5 Gb/s
2.50 Gb/s
0 b/s
20:00
21:00
22:00
23:00
00:00
01:00
02:00
03:00
04:00
05:00
06:00
07:00
min
max
avg
current
Input
58.8 Mb/s
11.9 Gb/s
1.60 Gb/s
4.11 Gb/s
Output
21.5 Mb/s
12.1 Gb/s
1.77 Gb/s
6.78 Gb/s

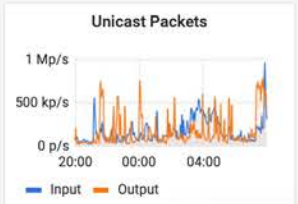

RedCLARA
Total Traffic
2.30 TB
2.54 TB
Input
Output

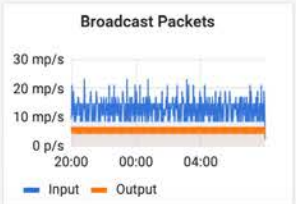

Latency
67 milliseconds
66 milliseconds
65 milliseconds
64 milliseconds
63 milliseconds
20:00
22:00
00:00
02:00
04:00
06:00

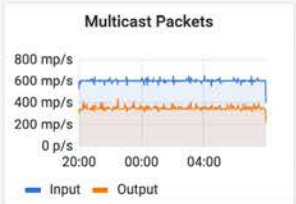

Errors
1 p/s
500 mp/s
0 p/s
-500 mp/s
-1 p/s
20:00
00:00
04:00
Input
Output

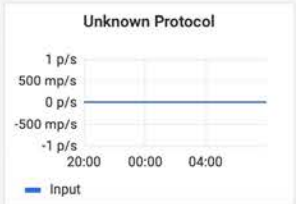

Discards
1 p/s
500 mp/s
0 p/s
-500 mp/s
-1 p/s
20:00
00:00
04:00
Input
Output

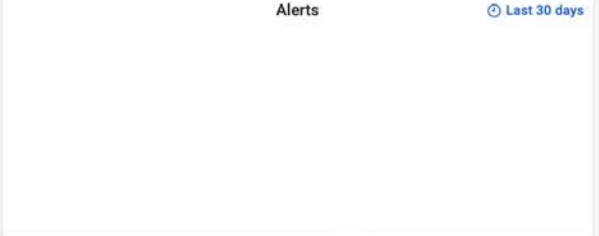

Status
Up
Availability
100.0000%


Unicast Packets
1 Mp/s
500 kp/s
0 p/s
20:00
00:00
04:00
Input
Output


Broadcast Packets
30 mp/s
20 mp/s
10 mp/s
0 p/s
20:00
00:00
04:00
Input
Output


Multicast Packets
800 mp/s
600 mp/s
400 mp/s
200 mp/s
0 p/s
20:00
00:00
04:00
Input
Output


Unknown Protocol
1 p/s
500 mp/s
0 p/s
-500 mp/s
-1 p/s
20:00
00:00
04:00
Input


Alerts
Last 30 days

Network Flows Monitoring

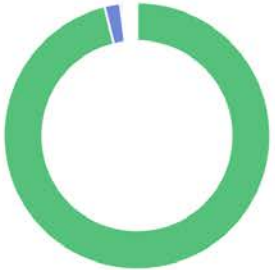
- Netflow v9 is configured on the routers
- Only 0.01% of the packets are sampled
- Flows are exported to Logstash
- Data is enriched and sent to Elasticsearch
- Dashboards are made for Kibana and are part of ElastiFlow

RedCLARA

Servers and Clients (bytes)

- 200.17.30.65
- 2001:12d0:8120::65
- 200.236.31.10
- 200.236.31.3
- 200.144.255.251
- 129.247.239.1
- 2001:67c:1148:200...
- 200.236.31.8
- 129.247.239.11
- 200.17.30.43
- 2001:67c:1148:200...
- 200.144.248.188

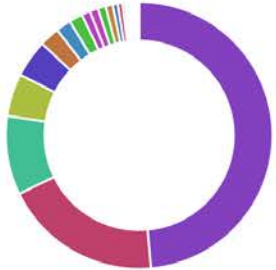
Services (bytes)



- etlservicemgr (TC...
- rsync (TCP/873)
- https (TCP/443)
- https (UDP/443)
- ldoms-migr (TCP/...
- ssh (TCP/22)
- ipsec-nat-t (UDP/...
- http (TCP/80)
- TCP/24659
- TCP/9619
- smtp (TCP/25)
- bip (TCP/4376)

RST ACK FIN
PSH SYN

Autonomous Systems (bytes)



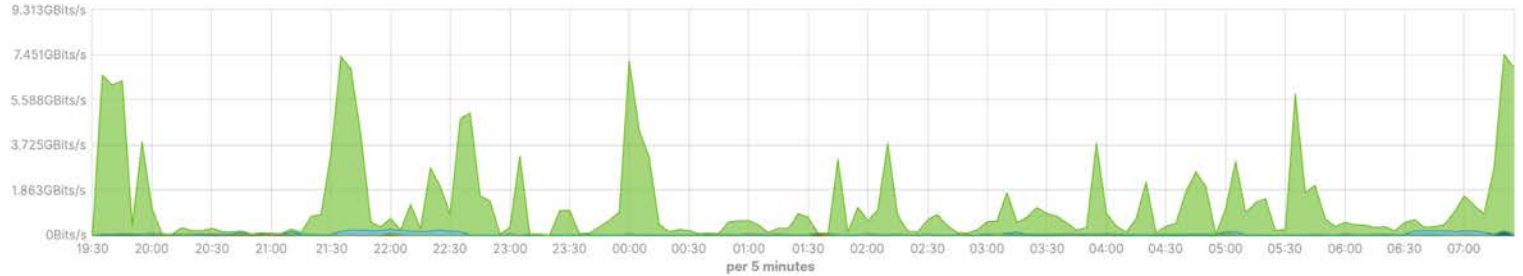
- UNIVERSIDADE DE...
- Entidad Publica E...
- Deutsches Elektro...
- SURFnet bv (1103)
- Verein zur Foerder...
- Consortium GARR ...
- Karlsruhe Institute ...
- Consorci Institut d...
- Fundacao da UFP...
- Queen Mary and ...
- Renater (2200)
- Universidad Nacio...

IP Versions and Protocols (bytes)

- IPv4
- IPv6
- TCP
- UDP
- ICMP
- GRE
- ESP
- IPv6-ICMP

bruteforce telnet
apache cms sasl auth
phpmyadmin http postfix
ssh email ftp
wordpress
spam bot mailer
suspicious

Services (bits/s)



Top Clients	Bytes	Packets	Flow Records
147.156.117.68	99.74MB	70,070	1,978
147.156.117.71	86.27MB	60,635	1,621
2001:638:700:f0c0::1:b	14.566MB	10,196	298
193.206.153.244	13.765MB	9,757	228
2001:638:700:f0c0::1:d	13.263MB	9,278	295
141.34.192.140	12.834MB	9,000	256
2001:638:700:f0c0::1:c	12.826MB	8,973	283
141.34.192.138	12.806MB	8,984	243
141.34.192.142	12.702MB	8,904	247
200.16.16.13	12.63MB	8,830	207
		567,715	**40,328**

Export: Raw Formatted

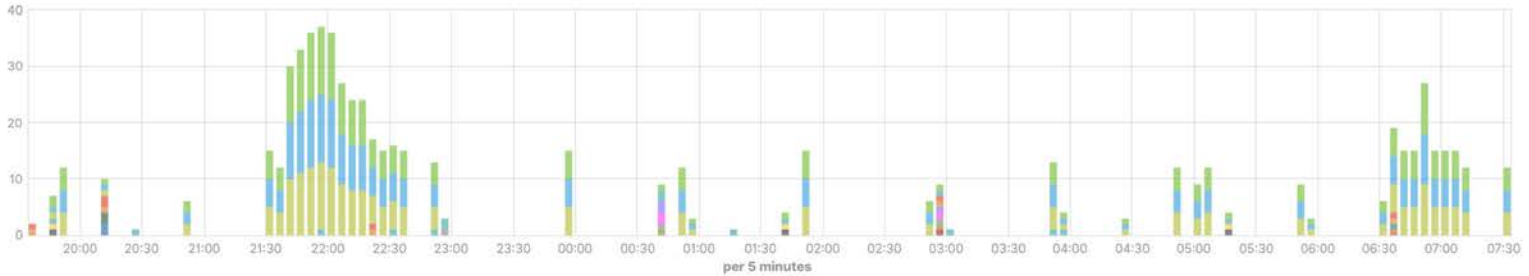
1 2 3 4 5 ... 50 »

Top Servers	Bytes	Packets	Flow Records
200.17.30.65	373.994MB	262,572	7,099
2001:12d0:8120::65	326.538MB	228,774	5,621
200.236.31.10	11.058MB	7,731	110
200.236.31.3	2.284MB	1,607	123
200.144.255.251	1.524MB	1,323	747
129.247.239.1	1.005MB	768	220
2001:67c:1148:200::89	716.516KB	10,151	5,555
200.236.31.8	703.125KB	480	59
129.247.239.11	513.066KB	586	484
200.17.30.43	470.084KB	368	310
		567,715	**40,328**

Export: Raw Formatted

1 2 3 4 5 ... 50 »

IP Reputations (flows)



IP Reputations	Flows
http	217
cms	212
wordpress	212
ssh	16
email	6
postfix	5
apache	3
bot	3
bruteforce	3
phpmyadmin	3

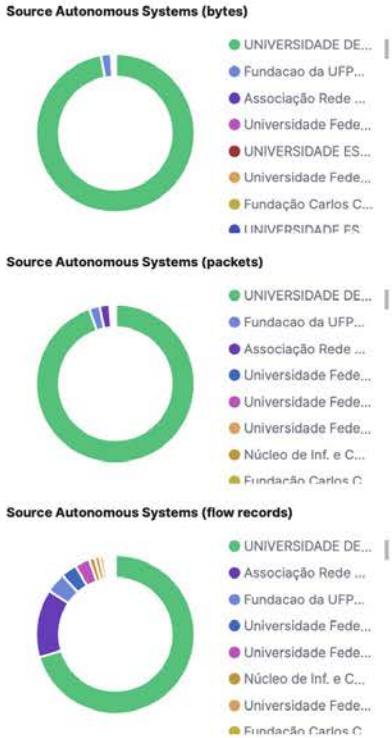
Export: Raw Formatted

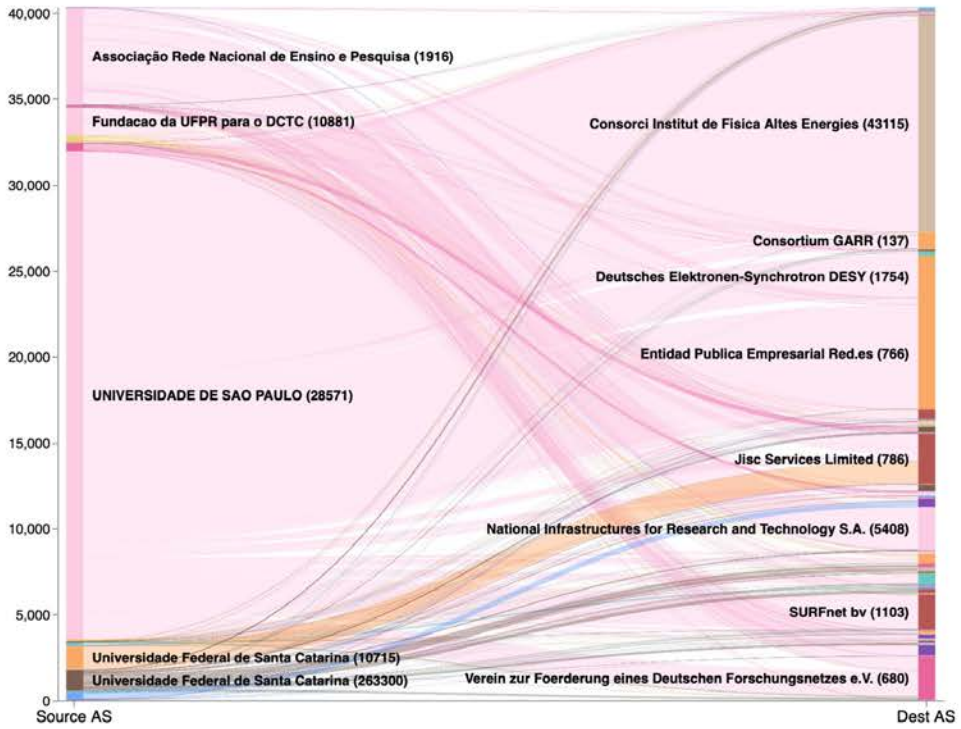
Public Threats	IP Address	Flows
200.16.16.13	200.16.16.13	209
128.232.21.75	128.232.21.75	2
192.42.116.17	192.42.116.17	1
200.129.150.3	200.129.150.3	1
200.129.173.3	200.129.173.3	1
200.135.196.251	200.135.196.251	1
200.27.72.243	200.27.72.243	1
95.183.249.4	95.183.249.4	1

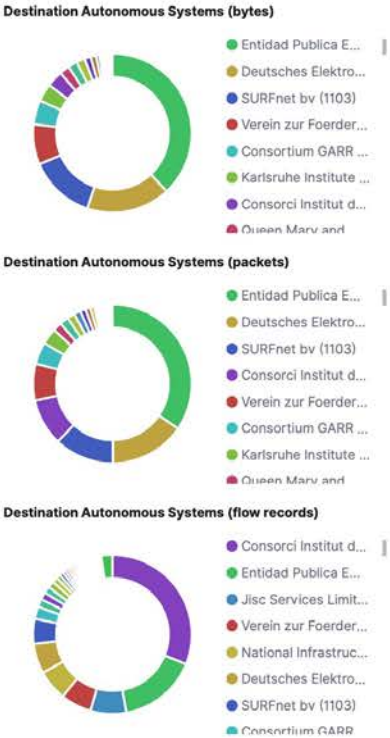
Export: Raw Formatted

High-Risk Clients	IP Address	Flows
150.162.1.6	150.162.1.6	8
143.54.2.91	143.54.2.91	3
131.227.80.119	131.227.80.119	1
150.165.77.215	150.165.77.215	1
193.144.81.195	193.144.81.195	1
194.94.23.191	194.94.23.191	1
200.16.80.9	200.16.80.9	1

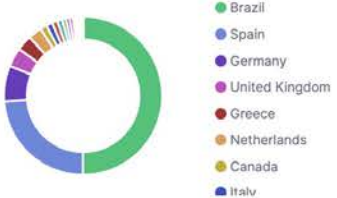
Export: Raw Formatted


Source Autonomous Systems (bytes)
UNIVERSIDADE DE...
Fundacao da UFP...
Associação Rede ...
Universidade Fede...
UNIVERSIDADE ES...
Universidade Fede...
Fundação Carlos C...
Source Autonomous Systems (packets)
UNIVERSIDADE DE...
Fundacao da UFP...
Associação Rede ...
Universidade Fede...
Universidade Fede...
Universidade Fede...
Núcleo de Inf. e C...
Source Autonomous Systems (flow records)
UNIVERSIDADE DE...
Associação Rede ...
Fundacao da UFP...
Universidade Fede...
Universidade Fede...
Núcleo de Inf. e C...
Universidade Fede...

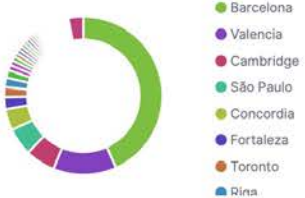

40,000
35,000
30,000
25,000
20,000
15,000
10,000
5,000
0
Associação Rede Nacional de Ensino e Pesquisa (1916)
Fundacao da UFPR para o DCTC (10881)
UNIVERSIDADE DE SAO PAULO (28571)
Universidade Federal de Santa Catarina (10715)
Universidade Federal de Santa Catarina (263300)
Consorci Institut de Física Altes Energies (43115)
Consortium GARR (137)
Deutsches Elektronen-Synchrotron DESY (1754)
Entidad Publica Empresarial Red.es (766)
Jisc Services Limited (786)
National Infrastructures for Research and Technology S.A. (5408)
SURFnet bv (1103)
Verein zur Foerderung eines Deutschen Forschungsnetzes e.V. (680)
Source AS
Dest AS


Destination Autonomous Systems (bytes)
Entidad Publica E...
Deutsches Elektro...
SURFnet bv (1103)
Verein zur Foerder...
Consortium GARR ...
Karlsruhe Institute ...
Consorci Institut d...
Destination Autonomous Systems (packets)
Entidad Publica E...
Deutsches Elektro...
SURFnet bv (1103)
Consorci Institut d...
Verein zur Foerder...
Consortium GARR ...
Karlsruhe Institute ...
Destination Autonomous Systems (flow records)
Consorci Institut d...
Entidad Publica E...
Jisc Services Limit...
Verein zur Foerder...
National Infrastruc...
Deutsches Elektro...
SURFnet bv (1103)

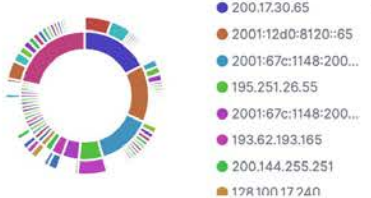
Countries (flow records)



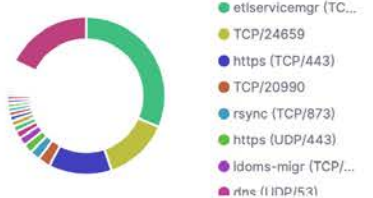
Cities (flow records)



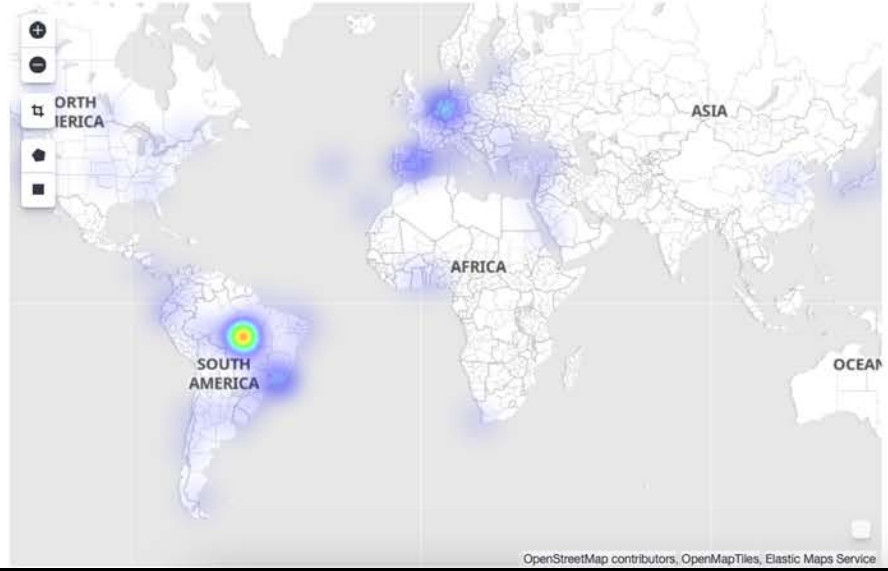
Servers and Clients (flow records)



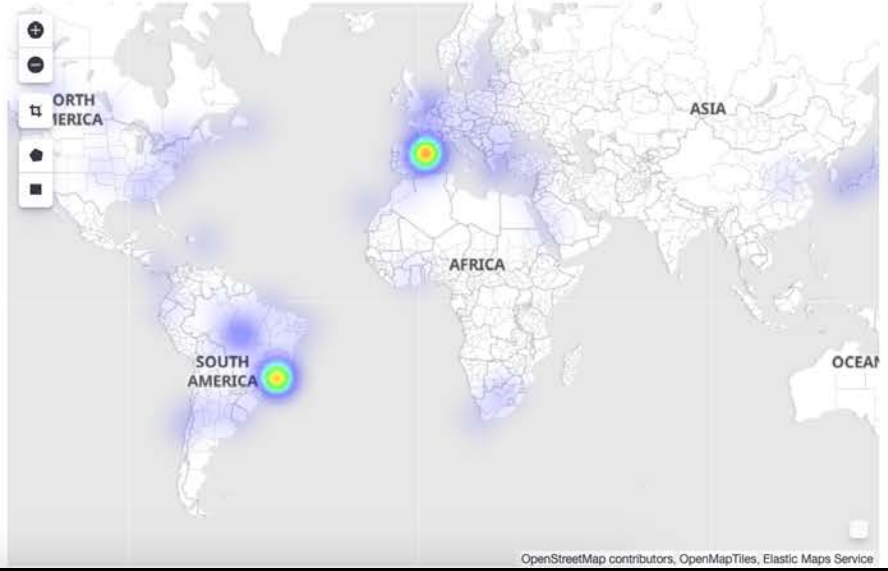
Services (flow records)



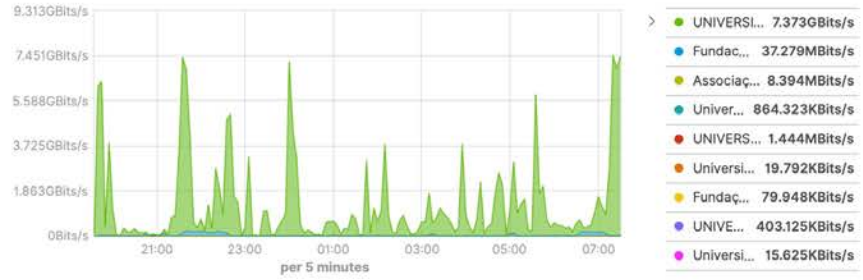
Client Locations (flow records)



Server Locations (flow records)

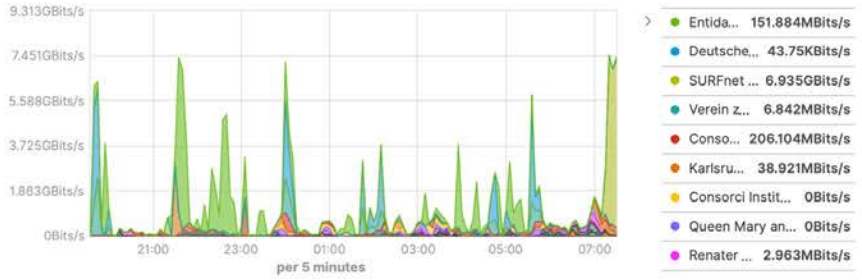


Source Autonomous Systems (bits/s)



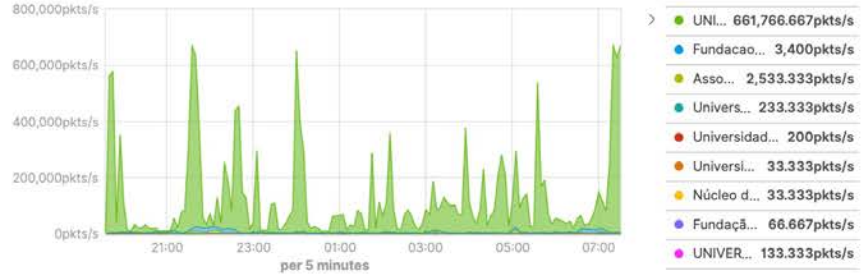
- UNIVERSI... 7.373GBits/s
- Fundac... 37.279MBits/s
- Associaç... 8.394MBits/s
- Univer... 864.323KBits/s
- UNIVERS... 1.444MBits/s
- Universi... 19.792KBits/s
- Fundaç... 79.948KBits/s
- UNIVE... 403.125KBits/s
- Universi... 15.625KBits/s

Destination Autonomous Systems (bits/s)



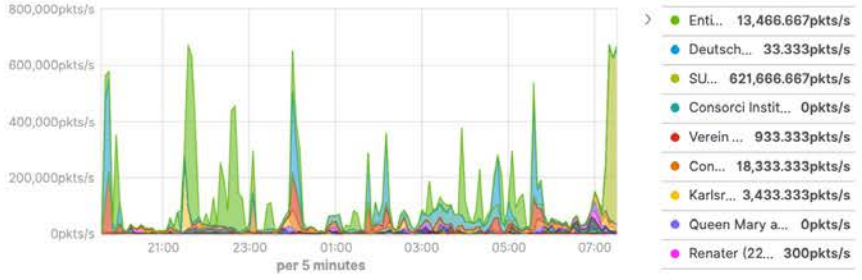
- Entida... 151.884MBits/s
- Deutsche... 43.75KBits/s
- SURFnet ... 6.935GBits/s
- Verein z... 6.842MBits/s
- Conso... 206.104MBits/s
- Karlsru... 38.921MBits/s
- Consorci Instit... 0Bits/s
- Queen Mary an... 0Bits/s
- Renater ... 2.963MBits/s

Source Autonomous Systems (pkts/s)



- UNI... 661,766.667pkts/s
- Fundacao... 3,400pkts/s
- Asso... 2,533.333pkts/s
- Univers... 233.333pkts/s
- Universidad... 200pkts/s
- Universi... 33.333pkts/s
- Núcleo d... 33.333pkts/s
- Fundaçã... 66.667pkts/s
- UNIVER... 133.333pkts/s

Destination Autonomous Systems (pkts/s)

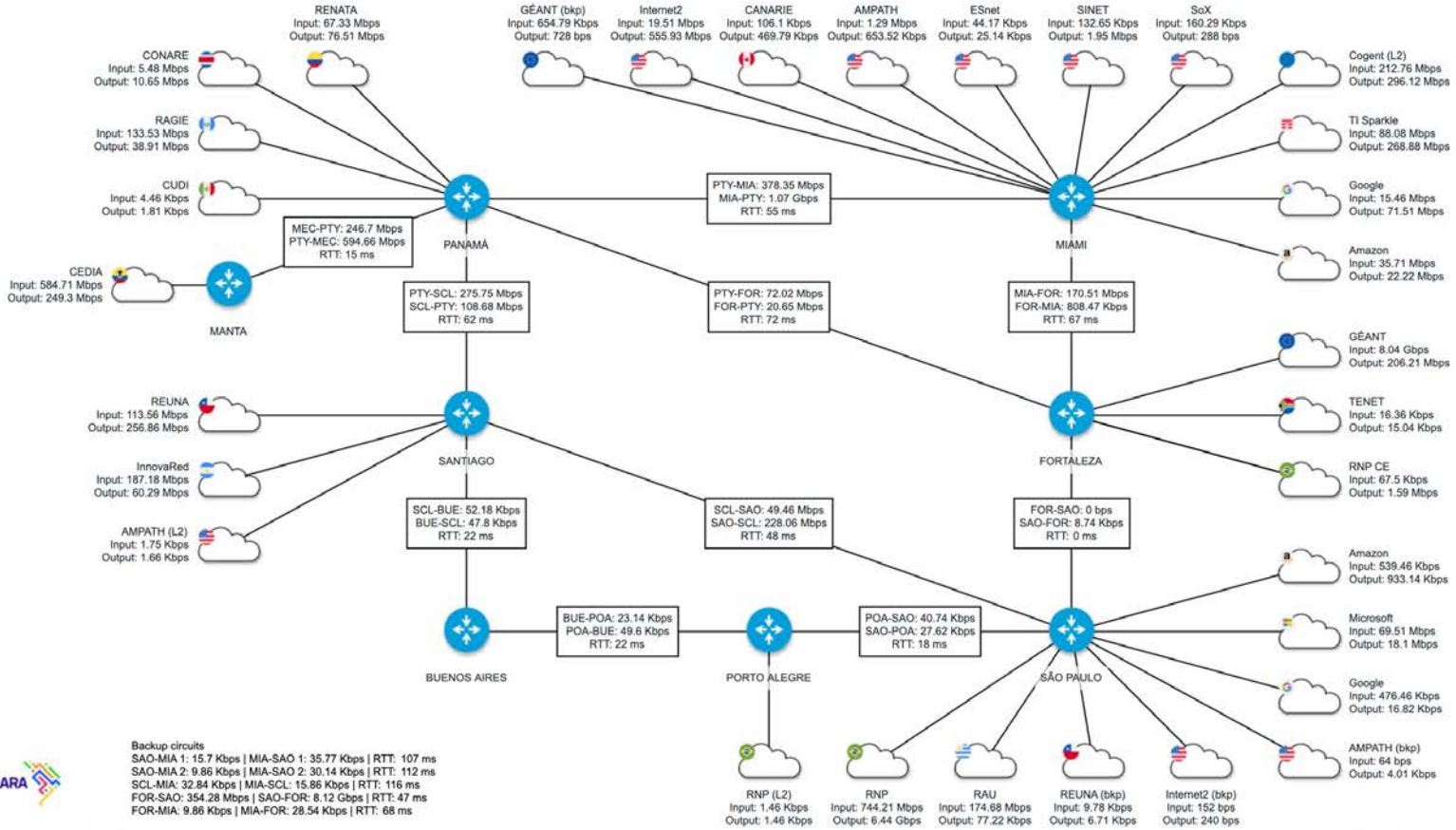


- Enti... 13,466.667pkts/s
- Deutsch... 33.333pkts/s
- SU... 621,666.667pkts/s
- Consorci Instit... 0pkts/s
- Verein ... 933.333pkts/s
- Con... 18,333.333pkts/s
- Karlsr... 3,433.333pkts/s
- Queen Mary a... 0pkts/s
- Renater (22... 300pkts/s

WeatherMap

ZABBIX

- The WeatherMap shows current backbone traffic and latency
- It has been built with Zabbix
- General view for backbone circuit outages


RENATA
Input: 67.33 Mbps
Output: 76.51 Mbps
GÉANT (bkp)
Input: 654.79 Kbps
Output: 728 bps
Internet2
Input: 19.51 Mbps
Output: 555.93 Mbps
CANARIE
Input: 106.1 Kbps
Output: 469.79 Kbps
AMPATH
Input: 1.29 Mbps
Output: 653.52 Kbps
ESnet
Input: 44.17 Kbps
Output: 25.14 Kbps
SINET
Input: 132.65 Kbps
Output: 1.95 Mbps
SoX
Input: 160.29 Kbps
Output: 288 bps
CONARE
Input: 5.48 Mbps
Output: 10.65 Mbps
RAGIE
Input: 133.53 Mbps
Output: 38.91 Mbps
CUDI
Input: 4.46 Kbps
Output: 1.81 Kbps
CEDIA
Input: 584.71 Mbps
Output: 249.3 Mbps
MANTA
MEC-PTY: 246.7 Mbps
PTY-MEC: 594.66 Mbps
RTT: 15 ms
PANAMÁ
PTY-MIA: 378.35 Mbps
MIA-PTY: 1.07 Gbps
RTT: 55 ms
MIAMI
Cogent (L2)
Input: 212.76 Mbps
Output: 296.12 Mbps
TI Sparkle
Input: 88.08 Mbps
Output: 268.88 Mbps
Google
Input: 15.46 Mbps
Output: 71.51 Mbps
Amazon
Input: 35.71 Mbps
Output: 22.22 Mbps
PTY-SCL: 275.75 Mbps
SCL-PTY: 108.68 Mbps
RTT: 62 ms
PTY-FOR: 72.02 Mbps
FOR-PTY: 20.65 Mbps
RTT: 72 ms
MIA-FOR: 170.51 Mbps
FOR-MIA: 808.47 Kbps
RTT: 67 ms
REUNA
Input: 113.56 Mbps
Output: 256.86 Mbps
InnovaRed
Input: 187.18 Mbps
Output: 60.29 Mbps
AMPATH (L2)
Input: 1.75 Kbps
Output: 1.66 Kbps
SANTIAGO
FORTALEZA
GÉANT
Input: 8.04 Gbps
Output: 206.21 Mbps
TENET
Input: 16.36 Kbps
Output: 15.04 Kbps
RNP CE
Input: 67.5 Kbps
Output: 1.59 Mbps
SCL-BUE: 52.18 Kbps
BUE-SCL: 47.8 Kbps
RTT: 22 ms
SCL-SAO: 49.46 Mbps
SAO-SCL: 228.06 Mbps
RTT: 48 ms
FOR-SAO: 0 bps
SAO-FOR: 8.74 Kbps
RTT: 0 ms
Amazon
Input: 539.46 Kbps
Output: 933.14 Kbps
Microsoft
Input: 69.51 Mbps
Output: 18.1 Mbps
Google
Input: 476.46 Kbps
Output: 16.82 Kbps
AMPATH (bkp)
Input: 64 bps
Output: 4.01 Kbps
BUE-POA: 23.14 Kbps
POA-BUE: 49.6 Kbps
RTT: 22 ms
POA-SAO: 40.74 Kbps
SAO-POA: 27.62 Kbps
RTT: 18 ms
BUENOS AIRES
PORTO ALEGRE
SÃO PAULO
RNP (L2)
Input: 1.46 Kbps
Output: 1.46 Kbps
RNP
Input: 744.21 Mbps
Output: 6.44 Gbps
RAU
Input: 174.68 Mbps
Output: 77.22 Kbps
REUNA (bkp)
Input: 9.78 Kbps
Output: 6.71 Kbps
Internet2 (bkp)
Input: 152 bps
Output: 240 bps
Backup circuits
SAO-MIA 1: 15.7 Kbps | MIA-SAO 1: 35.77 Kbps | RTT: 107 ms
SAO-MIA 2: 9.86 Kbps | MIA-SAO 2: 30.14 Kbps | RTT: 112 ms
SCL-MIA: 32.84 Kbps | MIA-SCL: 15.86 Kbps | RTT: 116 ms
FOR-SAO: 354.28 Mbps | SAO-FOR: 8.12 Gbps | RTT: 47 ms
FOR-MIA: 9.86 Kbps | MIA-FOR: 28.54 Kbps | RTT: 68 ms
2023-09-18 07:45:53

WebSSH

WebSSH

TACACSGUI

- Built with WebSSH (https://github.com/huashengdun/webssh)
- User authentication, command authorization and accounting done by TACACSGUI
- Only ping, traceroute and a set of show commands are allowed

```
Hu0/1/0/1.959      up          up          REUNA Copernicus (backup)
Hu0/1/0/1.2008     up          up          AMPATH Academic (backup)
Hu0/1/0/1.2375     up          up          RNP SuperComputing 2022
Hu0/1/0/1.2376     up          up          RNP DPDI Server PoP-SP
Hu0/1/0/1.2377     up          up          Rednesp SuperComputing 2023
Hu0/1/0/2          down        down        To RNP NoviFlow WB5132-F SAO-SP4-SW03 P26

RP/0/RSP0/CPU0:rtr-core-sao#show bgp summary
Mon Sep 18 07:45:27.501 UTC
BGP router identifier 200.0.205.1, local AS number 27750
BGP generic scan interval 60 secs
Non-stop routing is enabled
BGP table state: Active
Table ID: 0xe0000000   RD version: 4666047
BGP main routing table version 4666047
BGP NSR Initial initsync version 48946 (Reached)
BGP NSR/ISSU Sync-Group versions 4666047/0
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker         4666047    4666047    4666047    4666047     4666047     4666047

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
198.32.252.205    0 20080  378053  383966  4666047    0    0     1w5d       1592
198.71.45.210     0 11537 2238562  220434  4666047    0    0     6d15h     17819
200.0.204.157     0 11340  158336  956779  4666047    0    0     2d17h       147
200.0.204.178     0  1797  140628  736818  4666047    0    0      3w0d         3
200.0.204.214     0  1916  371948  930739  4666047    0    0     15w3d       687
200.0.205.2       0 27750  493856 1077149  4666047    0    0     15w3d      4321
200.0.205.3       0 27750 81229916 1078545  4666047    0    0      8w2d     20649
200.0.205.4       0 27750  156409 1077838  4666047    0    0     15w3d         0
200.0.205.5       0 27750  178904 1077838  4666047    0    0     15w3d       338
200.0.205.7       0 27750  156256 1080550  4666047    0    0     10w3d         0
200.0.205.8       0 27750  163157 1077838  4666047    0    0     15w3d        73
200.0.205.9       0 27750  165342 1077709  4666047    0    0     5d21h        93

RP/0/RSP0/CPU0:rtr-core-sao#
```

- eduroam information is collected from logs
- Logs are ingested to ELK Stak
- Custom dashboards have been created to output the information

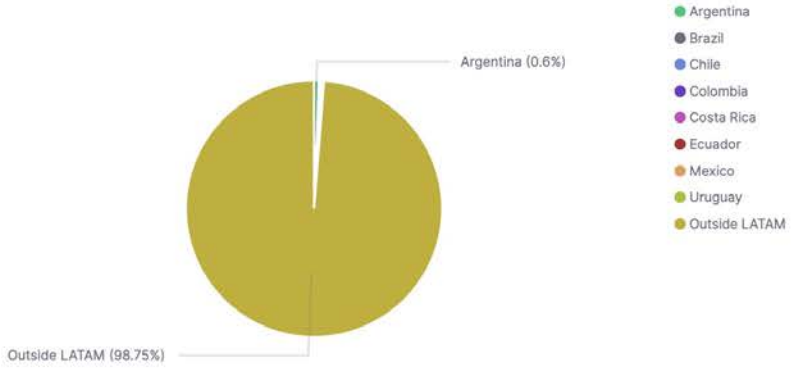
Brazil users authentications

1,094,568
Authentications

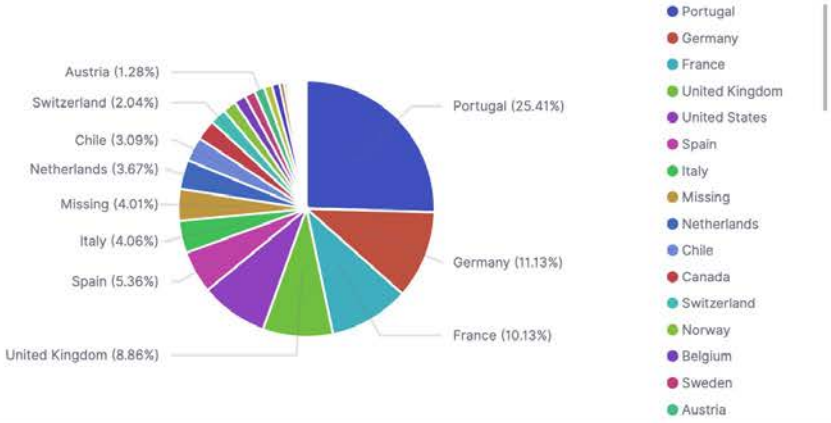
Foreign authentications in Brazil

426,724
Authentications

Countries visited by Brazil users



Foreign users authenticated in Brazil (by Country)



Cooperación Latino
Americana de Redes Avanzadas

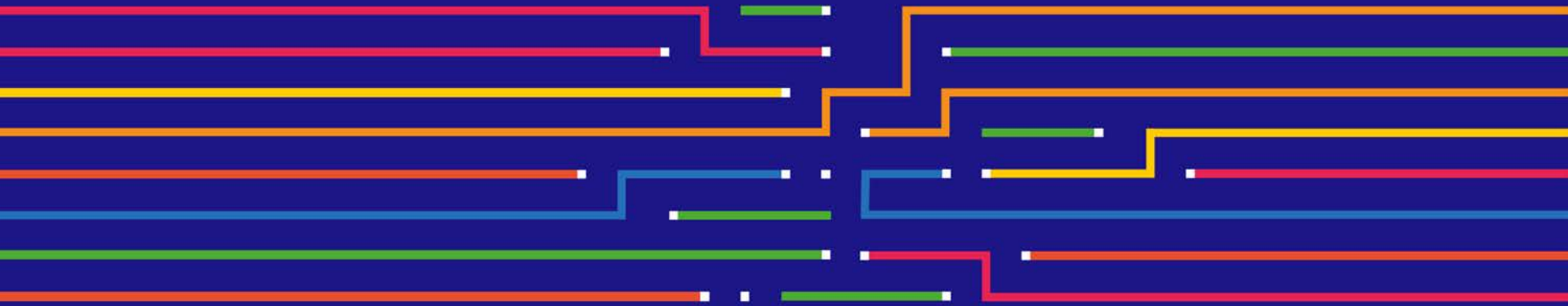
RedCLARA
NETWORK ENGINEERING GROUP

DEMO

TechEX2023

RedCLARA
NETWORK ENGINEERING GROUP

QUESTIONS?



RedCLARA
NETWORK ENGINEERING GROUP

redclara.net
tiago.monsores@redclara.net
linkedin.com/in/tiagomonsores