Visualize to Fortify

Backing GeoIP Blocking with Real Firewall Data

Hitesh Upadhyay – hitesh.upadhyay@itec.suny.edu
Michael Kozlowski – michael.kozlowski@itec.suny.edu
Travis G. Kench, CISSP – travis.kench@itec.suny.edu

SUNY ITEC Information Technology Exchange Center

Safe Harbor Statement

Our discussion may include predictions, estimates, or other information that might be considered forward-looking. While these forward-looking statements represent our current judgment on what the future holds, they are subject to risks and uncertainties that could cause actual results to differ materially. You are cautioned not to place undue reliance on these forward-looking statements, which reflect our opinions only as of the date of this presentation.

Three People Walk Into a Firewall...

One of us loves data so much, they probably have firewall logs framed on their wall.

Hitesh Upadhyay

One of us thinks GeoIP is a perfectly normal dinner conversation topic.

Mike Kozlowski

And one of us is just here to make sure no one blocks Canada by accident.

Travis G. Kench

SUNY ITEC Information Technology Exchange Center

Geo-IP Filtering Research Project

SUNY ITEC | Information Technology Exchange Center

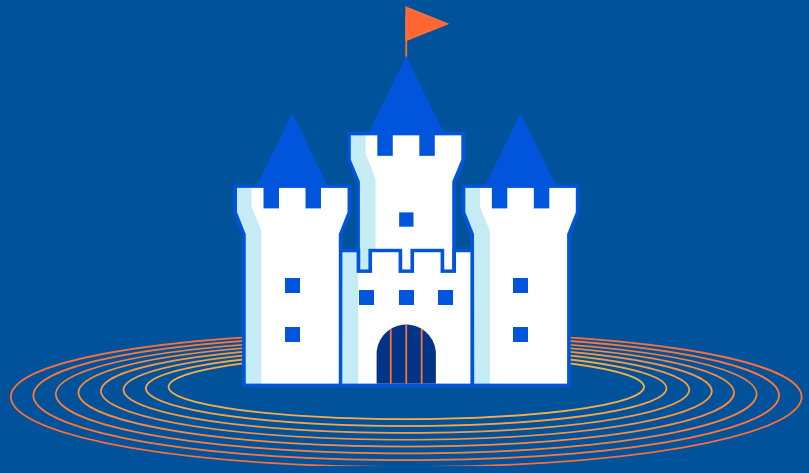
Sources	Main Takeaways	Recommended Blocks
U.S. Department of State: International Traffic in Arms Regulations (ITAR) - Country Policies	It is the policy of the United States to deny licenses and other approvals for exports and imports of defense articles and defense services, destined for or originating in certain countries. Specific policies of denial for individual countries are articulated in ITAR § 126.1.	Afghanistan, Belarus, Burma, Central African Republic, China, Cuba, Cyprus, Democratic Republic of the Congo (formerly Zaire), Eritrea, Ethiopia, Haiti, Hong Kong, Iran, Iraq, Kyrgyzstan, Lebanon, Libya, Nicaragua, North Korea, Russia, Somalia, Sudan, South Sudan, Syria, Venezuela, Zimbabwe
U.S. Department of Treasury: Office of Foreign Assets Control (OFAC) - Sanctions Programs and Country Information	The Office of Foreign Assets Control (OFAC) administers a number of different sanctions programs. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.	Comprehensively sanctioned countries: Cuba, Iran, North Korea, Syria, Ukraine (Crimea, Donetsk, and Luhansk Regions) Targeted Sanctioned countries: Balkans, Belarus, Burundi, Central African Republic, Democratic Republic of the Congo, Hong Kong, Iraq, Lebanon, Libya, Mali, Myanmar (formerly Burma), Nicaragua, Russia/Ukraine, Somalia, Sudan, South Sudan, Venezuela, Yemen, Zimbabwe
U.S. Department of Commerce: Export Administration Regulations (EAR) - Sanctioned Destinations	The Export Administration Regulations (EAR) is administered by Bureau of Industry and Security (BIS) to regulate the export of goods and technologies for national security and foreign policy purposes.	Comprehensively sanctioned countries: Cuba, Iran, North Korea, Syria, Ukraine (Crimea, Donetsk, and Luhansk Regions) Targeted Sanctioned countries: Iraq
U.S. Office of the Director of National Intelligence	Identifies the Big Four (China, Iran, North Korea, Russia) as threat actors which represent enduring and active threats to the United States and its interests, including government, private-sector, and	China, Iran, North Korea, Russia

Sources	Main Takeaways	Recommended Blocks
Code of Federal Regulations Title 28 C.F.R. Part 202 and Executive Order 14117	Institutions must protect sensitive U.S. data from exploitation or unauthorized access by certain foreign countries, and GeoIP blocking is a practical technical safeguard that helps address this federal mandate.	China, Cuba, Iran, North Korea, Russia, Venezuela
Cloudflare Common Policies	Cloudflare has categorized certain nations as being high risk.	Afghanistan, Belarus, Congo (Kinshasa), Cuba, Iran, Iraq, North Korea, Myanmar, Russia, Sudan, Syria, Ukraine, Zimbabwe
CrowdStrike 2025 Global Threat Report	CrowdStrike does not make any specific recommendations for countries to block, as threat actors often use proxy servers and VPNs, but the nation states listed are categories that CrowdStrike has specific entries for since they include active APTs.	Russia, Vietnam, North Korea, South Korea, Syria, Iran, Pakistan, Georgia, Colombia, China, Kazakhstan, Egypt, India, Turkey
Google Cloud Security Cybersecurity Forecast 2025	Mandiant believes that the nations with the most amount of cyber threat activity are a group they call "The Big Four" - China, Iran, North Korea, and Russia. See attachment for details.	China, Iran, North Korea, Russia
CISA: Nation-State Actors	Lists countries with APTs which pose elevated threats on their Cyber Threats & Advisories page. Recommends a Zero Trust solution or utilizing a jump server to prevent external traffic from entering the network without access.	China, Iran, North Korea, Russia

Sources	Main Takeaways	Recommended Blocks
FBI Criminal Justice Information Services Security Policy	Stresses the importance of filtering by location and blocking unsolicited requests for maintaining a secure network presence.	None Specified
NSA Network Infrastructure Security Guide	Highly recommends a Zero Trust solution for maintaining network integrity, creating robust ACLs, creating sufficient network perimeters, including one or more DMZ subnets to limit lateral access, as well as a NIDS or packet capturing service.	None Specified
NIST SP 800-41 (Guidelines on Firewalls and Firewall Policy)	Recommends filtering traffic based on source and destination without giving explicit recommendations for locations to block.	None Specified
Palo Alto Networks Security Policies Best Practices	Palo Alto recommends a zero-trust posture that allows for policy rules that specify the exact source and destination for traffic for applications, and only allowing traffic from geographical regions in which you conduct business.	None Specified

Geo-IP Filtering Research Summary

Defensive Options:

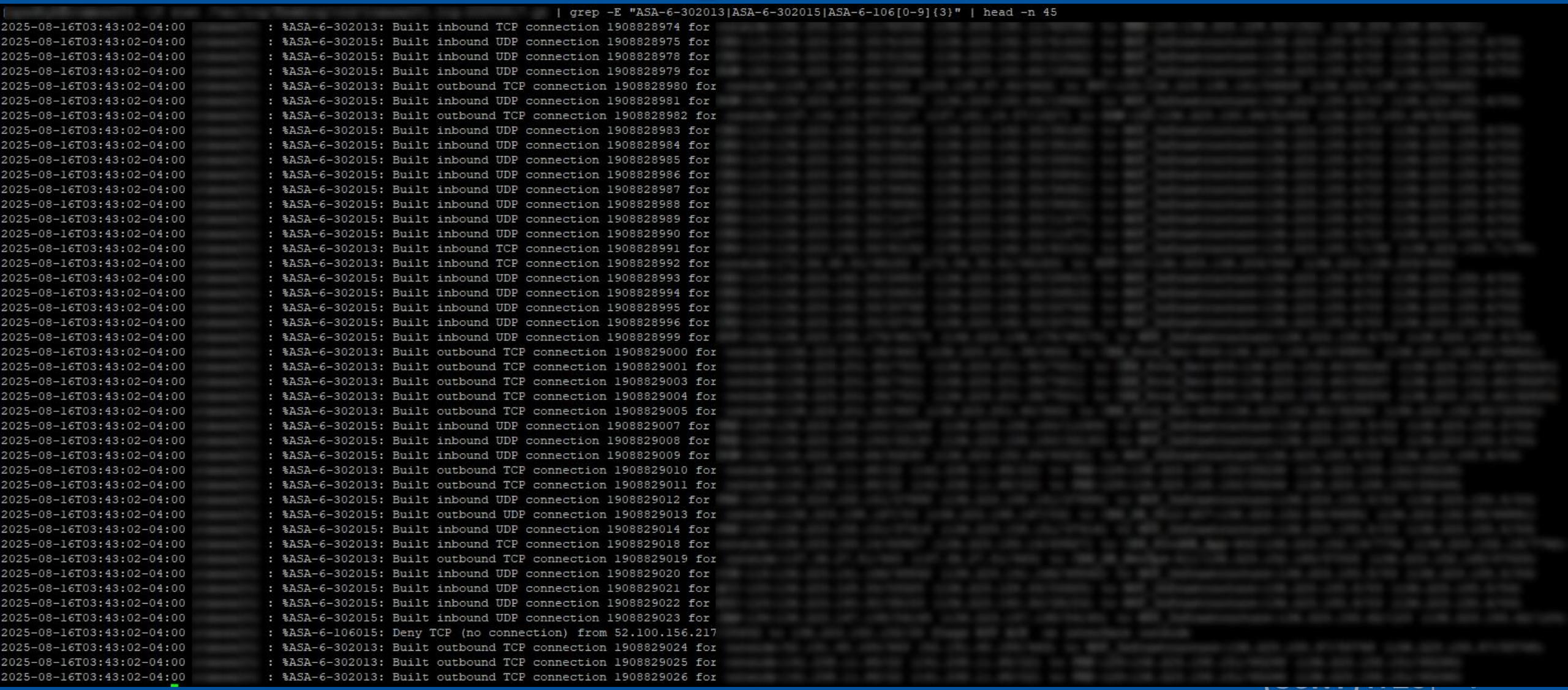


- **Conservative Approach**
  - Logic: Restrict traffic to the big 4 APTs.
  - Countries: China, Iran, North Korea, Russia
- **Moderate Approach**
  - Logic: Restrict traffic to and from comprehensively sanctioned countries, targeted sanctioned countries, and those countries specifically named as threat actors targeting the United States through the various data resources cited in this research.
  - Countries: Afghanistan, Balkans, Belarus, Brazil, Burma, Burundi, Central African Republic, China, Colombia, Congo (Kinshasa), Cuba, Egypt, Georgia, Hong Kong, Iran, Iraq, Kazakhstan, Lebanon, Libya, Nicaragua, North Korea, Mali, Myanmar, Pakistan, Russia, South Korea, Somalia, Sudan, Syria, Turkey, Ukraine, Venezuela, Vietnam, Yemen, Zimbabwe

Exploratory Analysis of Firewall Log for the week of - 2025/08/10 - 2025/08/17

SUNY ITEC | Information Technology Exchange Center

How to go from this:

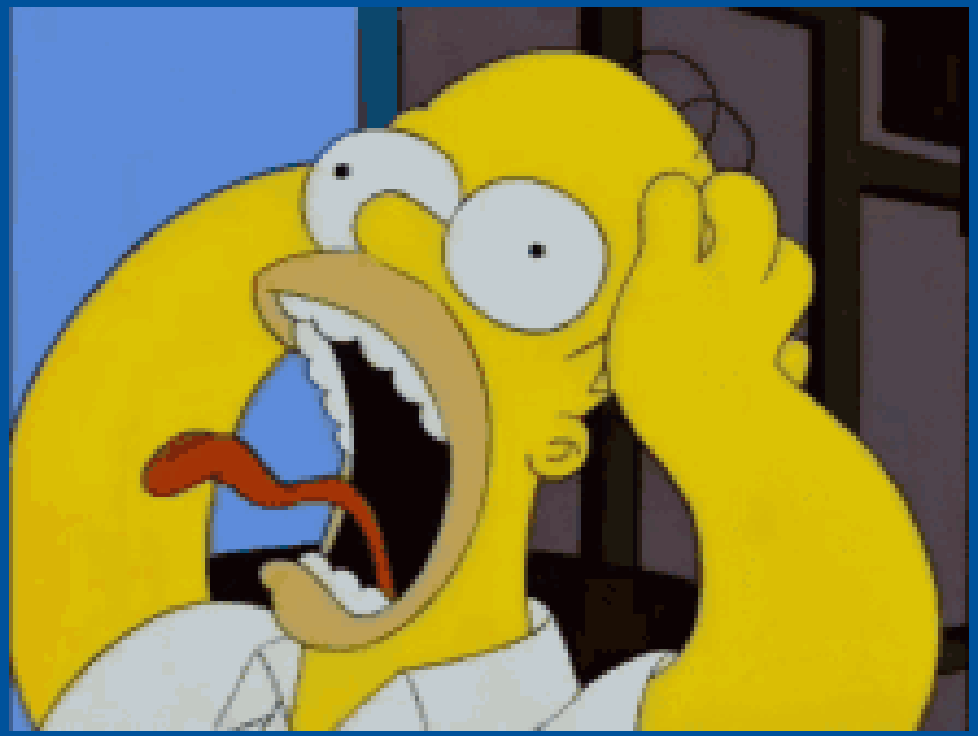


To this:

	timestamp	event	direction	protocol	source_ip	source_port	destination_ip	destination_port	interface	source_country	source_ip_asn
2	2025-08-10T03:50:01-04:00	built	inbound	tcp	[redacted]	46421	[redacted]	1521	[redacted]	United States	AS398756
37	2025-08-10T03:50:01-04:00	built	inbound	tcp	[redacted]	63081	[redacted]	389	[redacted]	United States	AS398914
39	2025-08-10T03:50:01-04:00	deny	inbound	tcp	[redacted]	1059	[redacted]	25	[redacted]	United States	AS8075
94	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	46422	[redacted]	1521	[redacted]	United States	AS398756
99	2025-08-10T03:50:02-04:00	deny	inbound	tcp	[redacted]	25565	[redacted]	54660	[redacted]	Russia	AS50340
117	2025-08-10T03:50:02-04:00	deny	inbound	tcp	[redacted]	4556	[redacted]	443	[redacted]	United States	AS8075
127	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	53558	[redacted]	443	[redacted]	United States	AS19148
129	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	31950	[redacted]	22	[redacted]	United States	AS5719
145	2025-08-10T03:50:02-04:00	deny	inbound	tcp	[redacted]	25565	[redacted]	30634	[redacted]	Russia	AS50340
156	2025-08-10T03:50:02-04:00	deny	inbound	tcp	[redacted]	443	[redacted]	44756	[redacted]	Canada	AS36483
161	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	53299	[redacted]	1521	[redacted]	United States	AS13536
162	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	58787	[redacted]	443	[redacted]	Singapore	AS14061
174	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	15456	[redacted]	1521	[redacted]	United States	AS398756
178	2025-08-10T03:50:02-04:00	deny	inbound	tcp	[redacted]	25565	[redacted]	8878	[redacted]	Russia	AS50340
201	2025-08-10T03:50:02-04:00	built	inbound	tcp	[redacted]	37384	[redacted]	10001	[redacted]	United States	AS14618

Steps before Data Analysis (1/2)

Step 1:



Scream

Step 2:

Sit and Code

Steps before Data Analysis (2/2)

Prior to Data Collection:

- Create a virtualenv on the Server to run python scripts
- Install latest version of python on it
- Create a VM for analysis purposes, and assign it a minimum of 32G of RAM
- Install the following packages and modules on it for data analysis:
  - Pandas
  - Numpy
  - Matplotlib
  - Seaborn
  - Statistics
  - Regex
  - CSV
  - Geoip2
  - Ipinfo
  - Ipaddress
  - Dask
  - Geopandas
  - Shapely.geometry
  - Plotly

Data Collection:

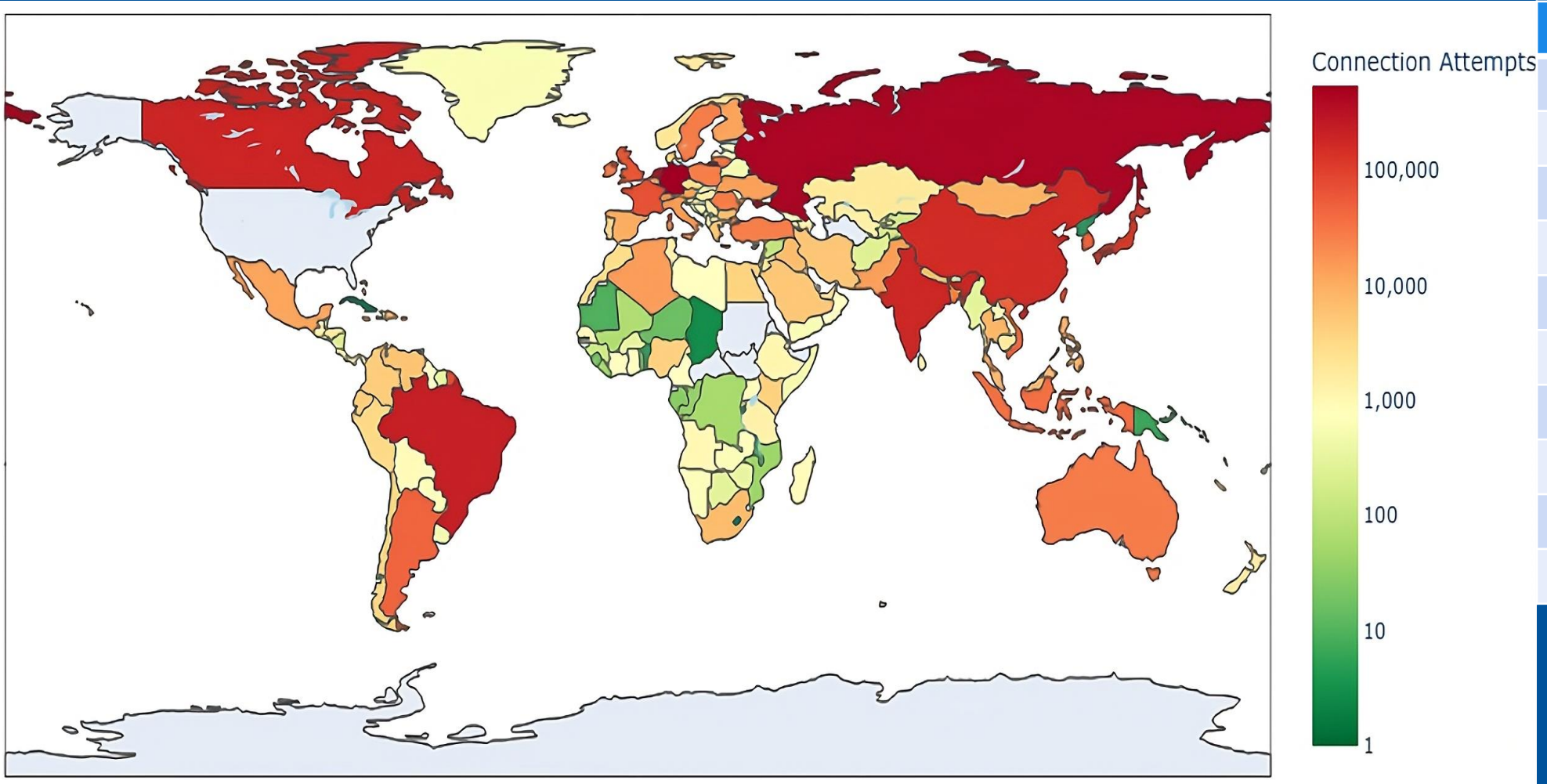
- Selecting data source
- Only filter for Built and Deny traffic for analysis
- Running python script to convert the data into the following columns:
  - Timestamp
  - Event
  - Direction
  - Protocol
  - Source_IP
  - Source_Port
  - Destination_IP
  - Destination_Port
  - Interface
- Repeating the process for 7 days worth of logs
- Moving the CSV Files to a VM from analysis

Data Refinement:

- Replacing hostname entries
- Removing private network traffic
- Utilizing .mmdb file from ipinfo to add the following columns based on the Source_IP:
  - Source_Country
  - Source_IP_ASN
- Repeating the process for 7 different .csv files
- Once this is done, you can now use the dask module to combines all the files into one large dataframe.
- Utilize this dataframe for performing data analysis.

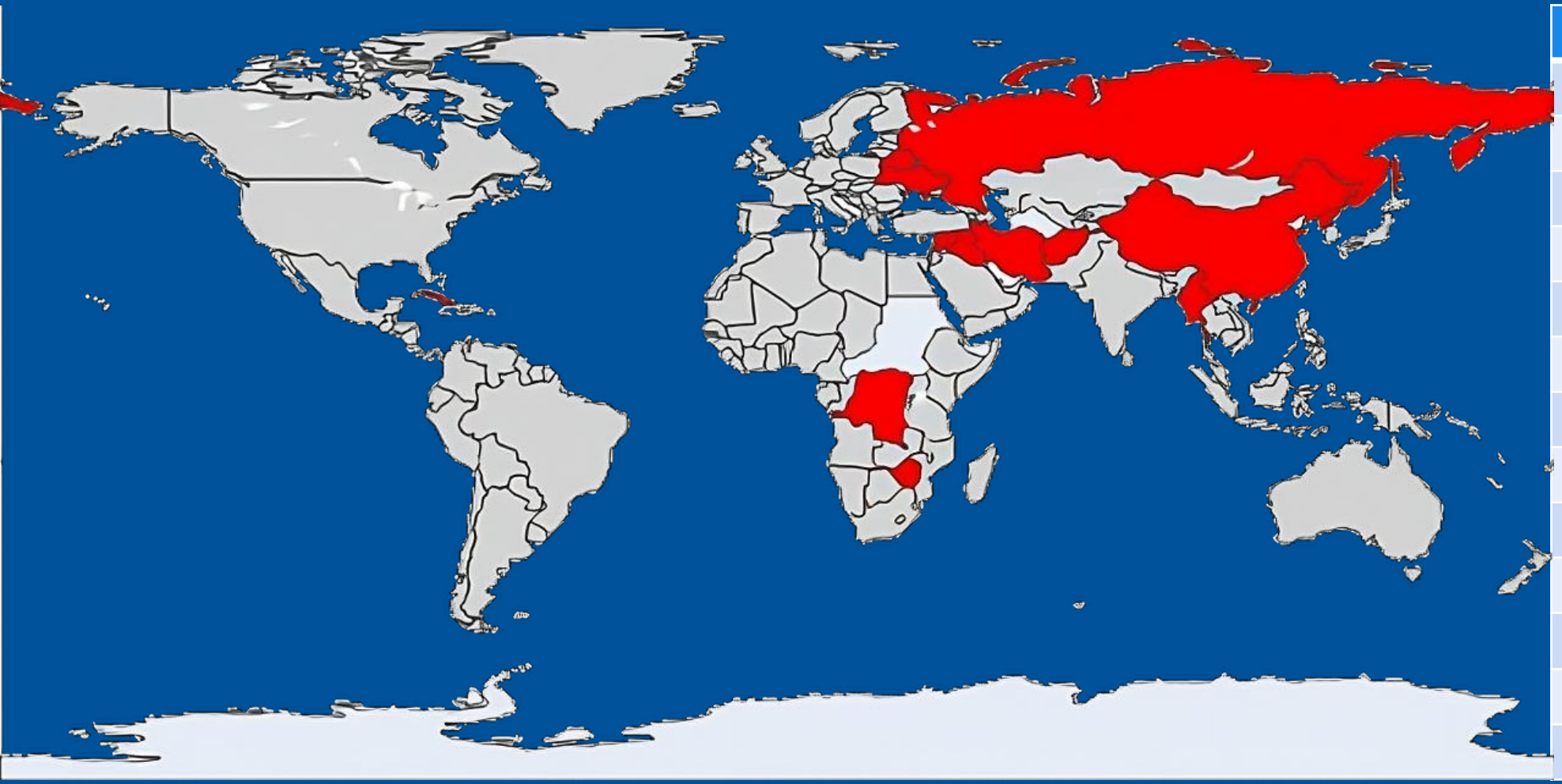
Results of Data Analysis

Inbound traffic in 1 week (outside US)



Country	Count
Germany	545534
Singapore	518507
Russia	444885
Netherlands	306293
Brazil	219204
Canada	191613
India	178670
China	159701
Japan	115664
Hong Kong	87245

Traffic from High-Risk Countries (1/2)

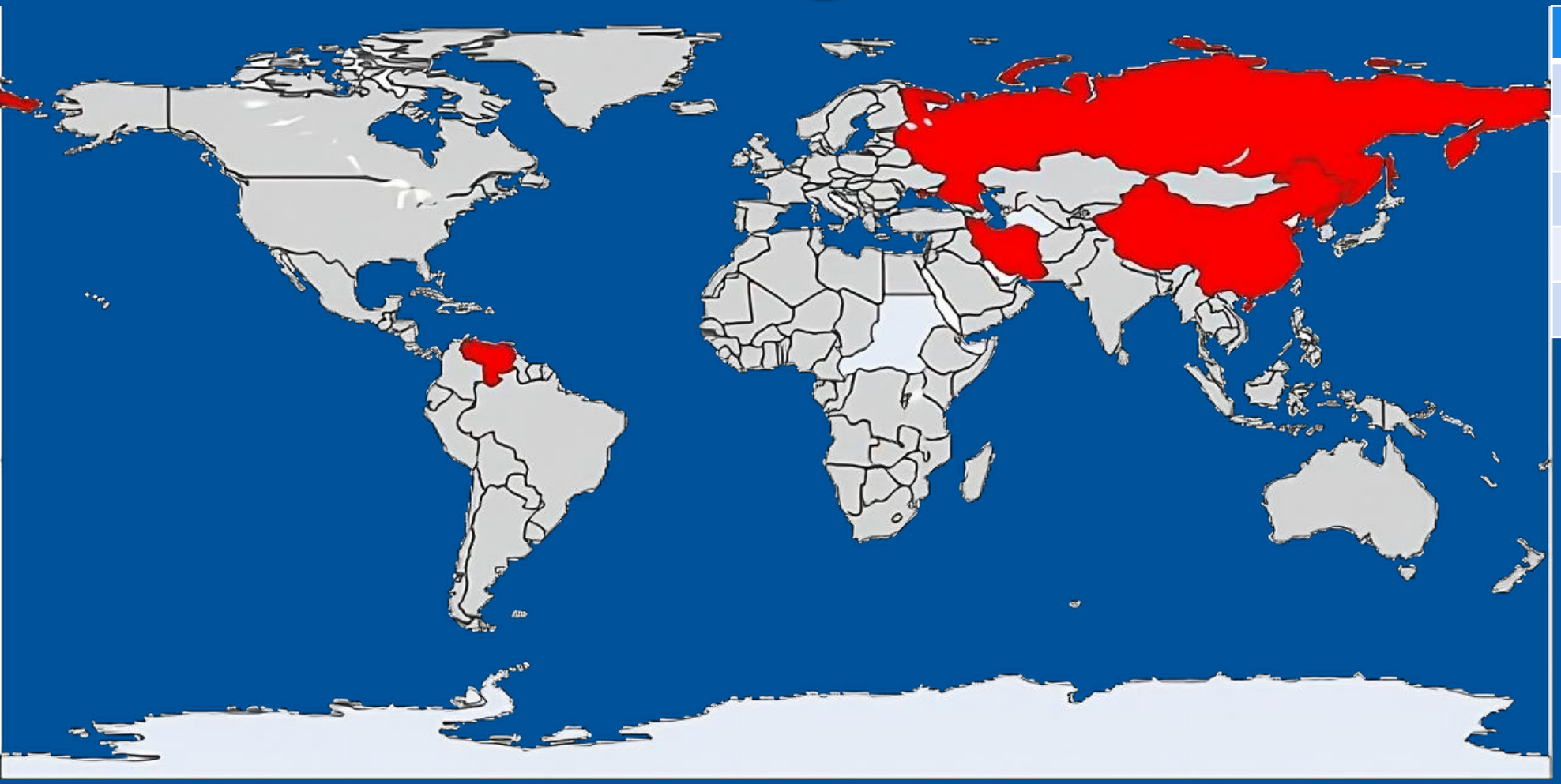


Country	Count
Russia	444885
China	159701
Ukraine	13592
Iraq	7065
Iran	5432
Belarus	439
Zimbabwe	329
Myanmar	291
Afghanistan	239
Syria	114
Democratic Republic of Congo	59
North Korea	5
Cuba	2

Countries Categorized as High Risk by Cloudflare - Afghanistan, Belarus, China, Democratic Republic of the Congo, Cuba, Iran, Iraq, North Korea, Myanmar, Russia, Sudan, Syria, Ukraine, Zimbabwe.

SUNY ITEC Information Technology Exchange Center

Traffic from High-Risk Countries (2/2)

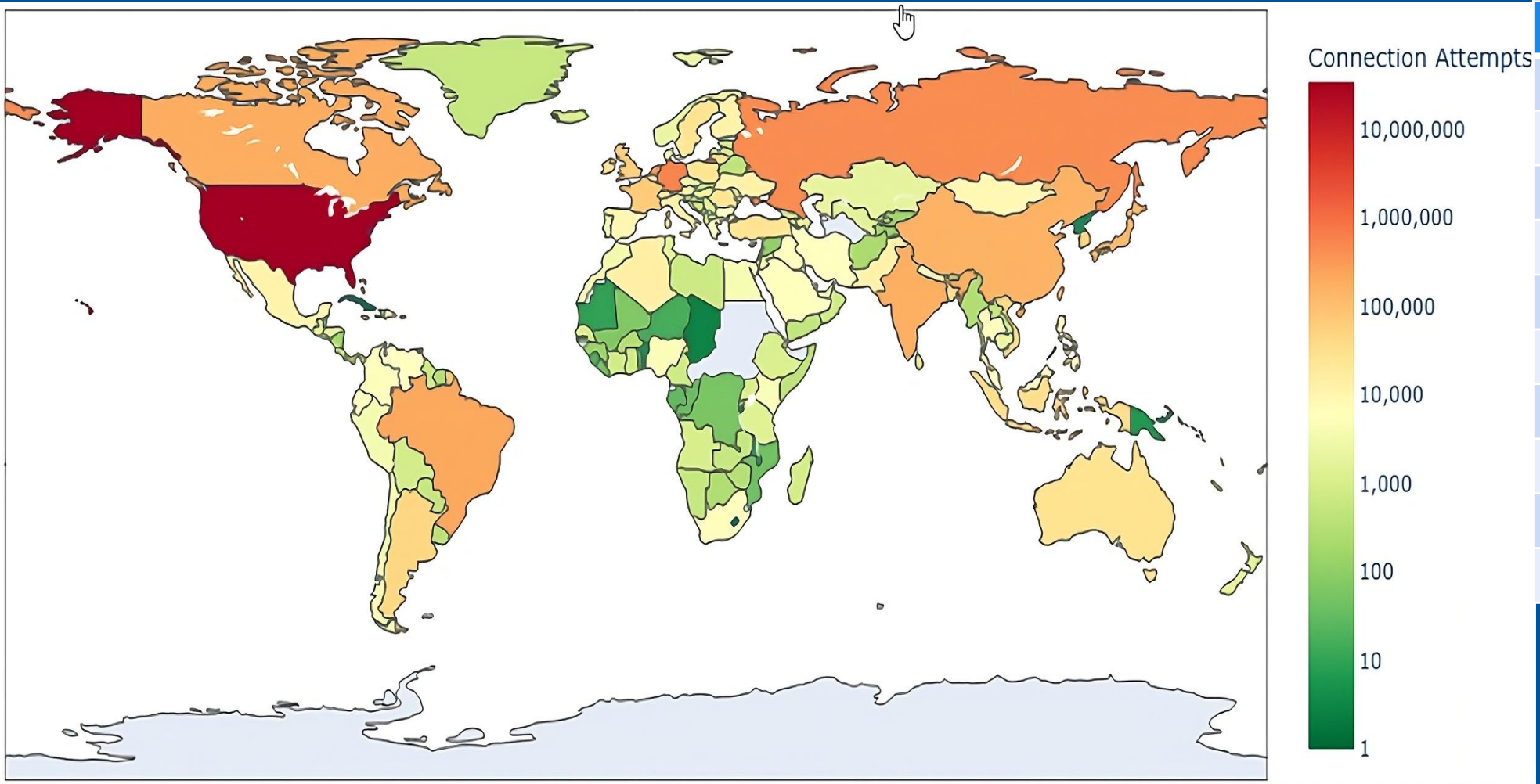


Country	Count
Russia	444885
China	159701
Venezuela	5805
Iran	5432
North Korea	5

Countries Categorized as High Risk by Executive Data Security Program Order 14117 - China, Iran, North Korea, Russia, Venezuela

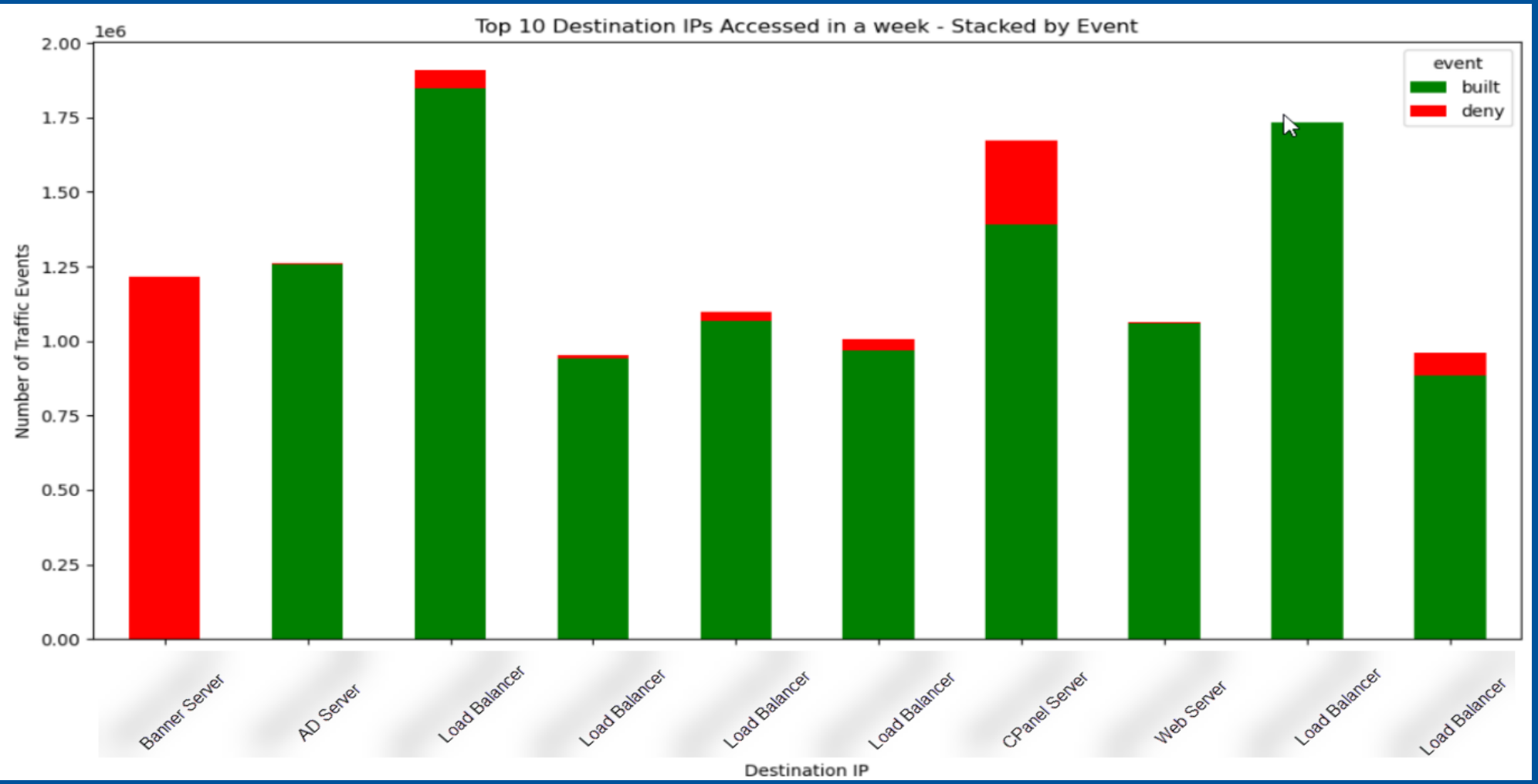
SUNY ITEC Information Technology Exchange Center

Overall Traffic Analysis (1/4)



Country	Count
United States	34672994
Germany	545534
Singapore	518507
Russia	444885
Netherlands	306293
Brazil	219204
Canada	191613
India	178670
China	159701
Japan	115664

Overall Traffic Analysis (2/4)

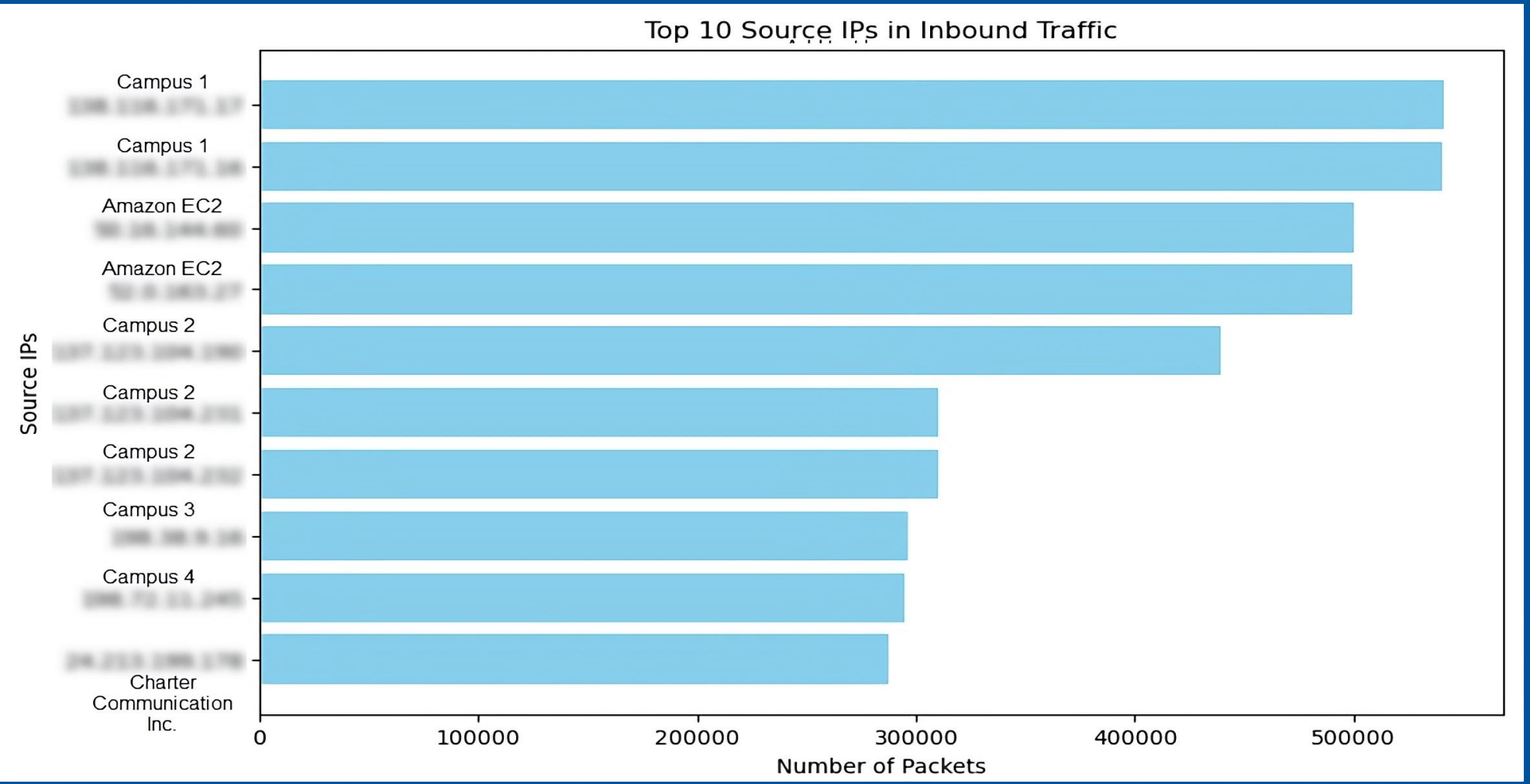


Top 10 Destination Servers:

- 6 Load balancers (different Campus VLANs)
- 1 AD Server
- 1 CPanel Server
- 1 Banner Server
- 1 Web Server

Note: This is just built/deny traffic from logs.

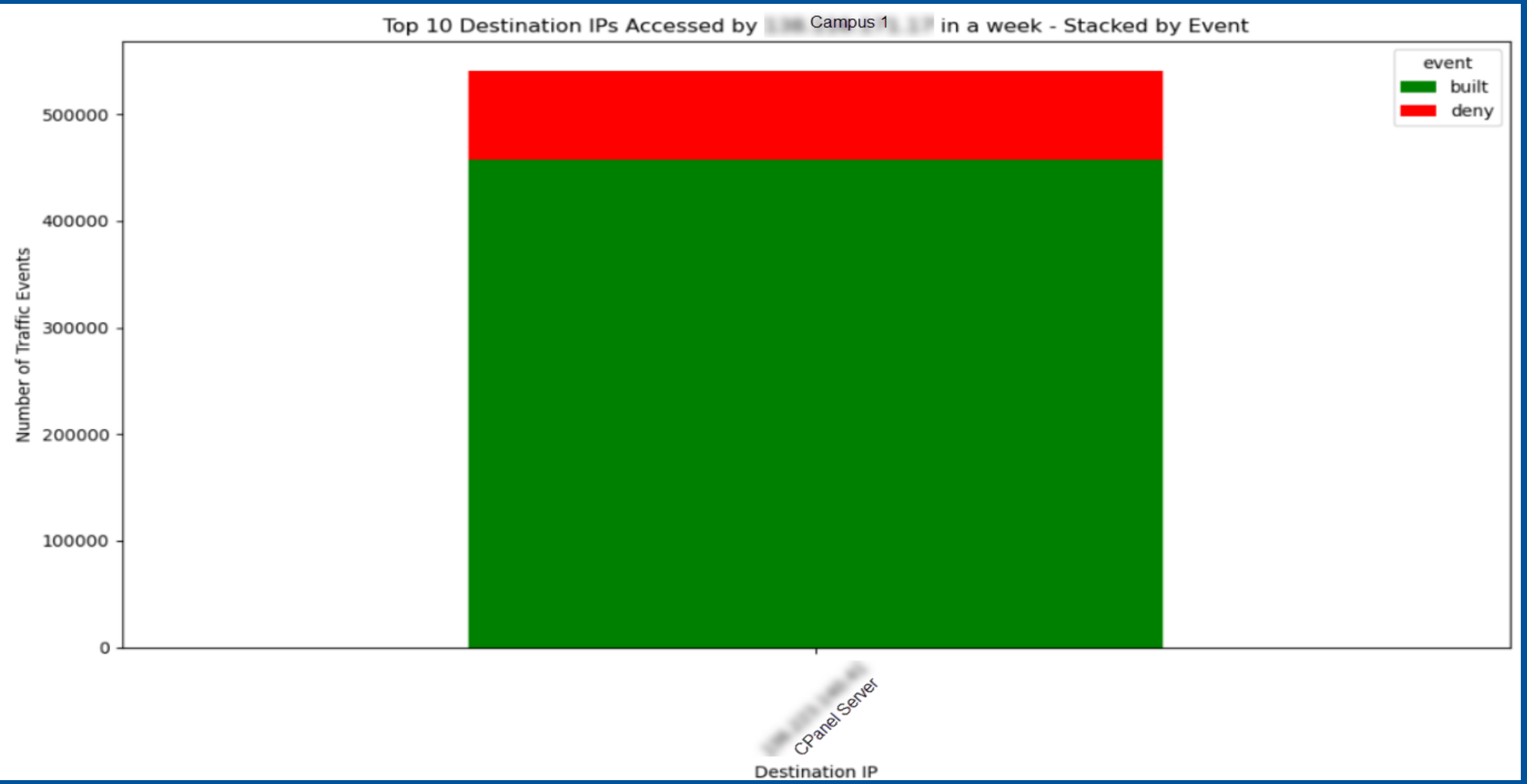
Overall Traffic Analysis (3/4)



Top 10 Source IPs:

- 7 IPs belonging to 4 different campuses
- 2 IPs from Amazon EC2 instances (mostly belonging to a campus)
- 1 IP from Charter Communication Inc.

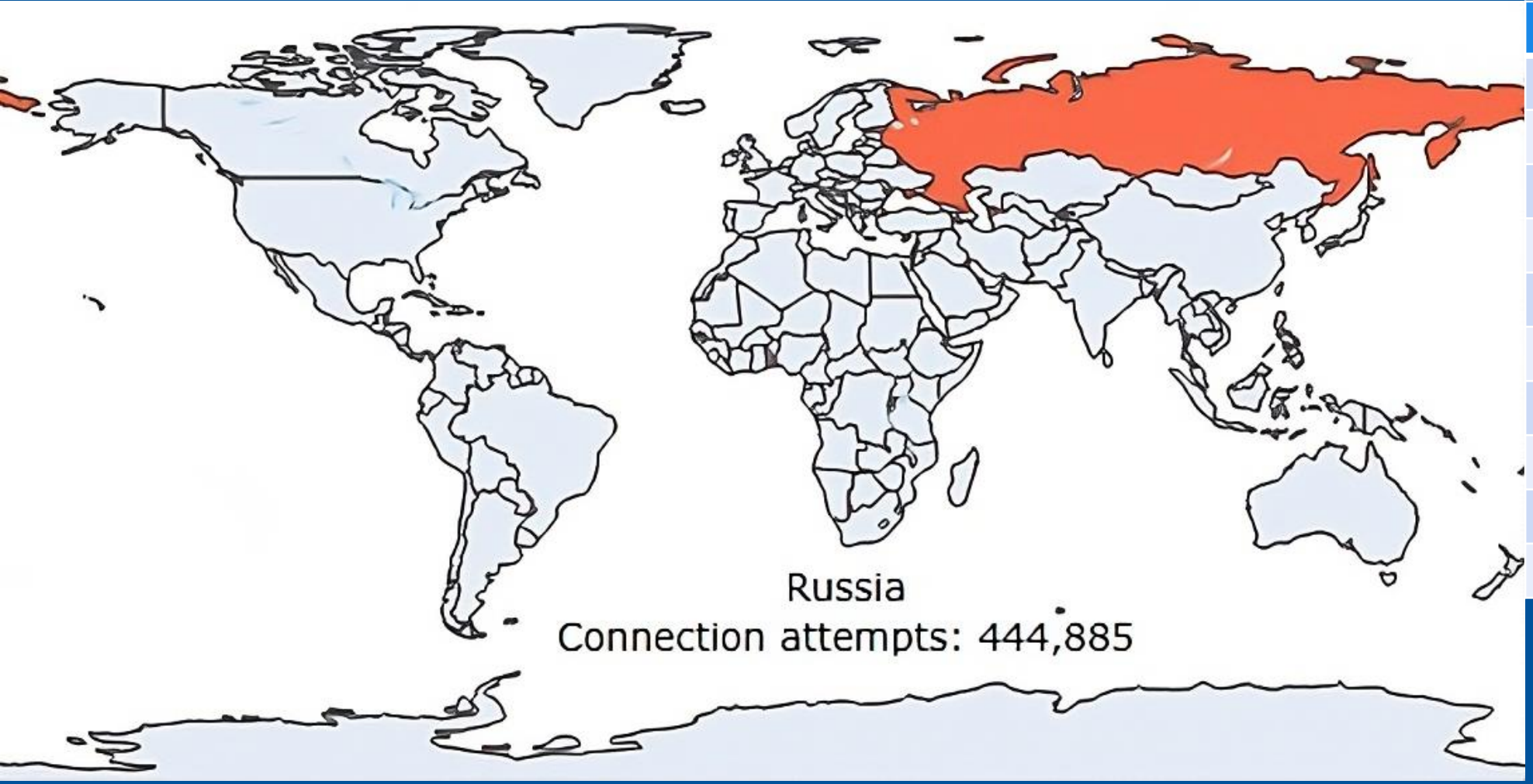
Overall Traffic Analysis (4/4)



- IP from Campus 1 generated most traffic.
- All traffic from the IP was destined to the Cpanel server.

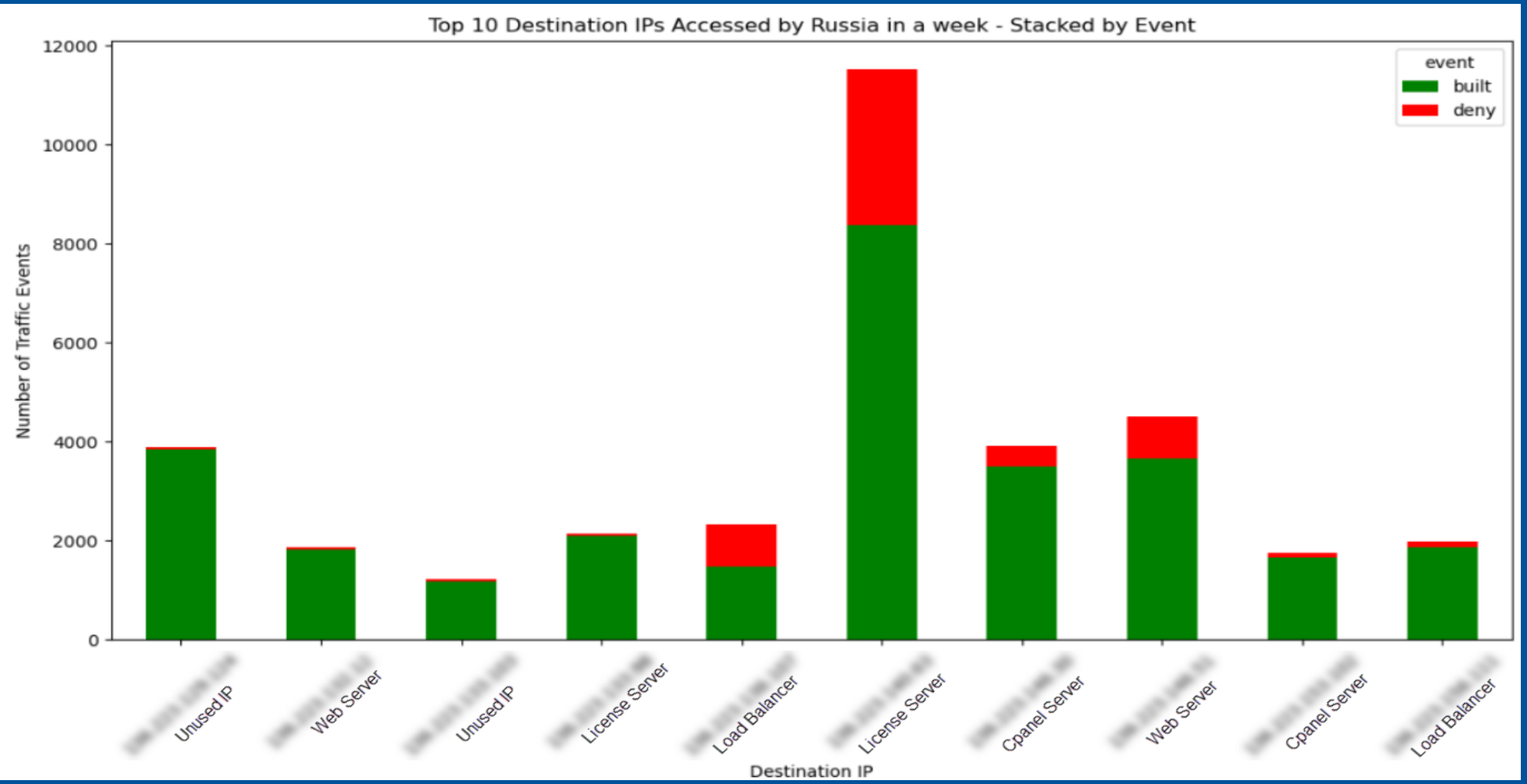
Note: This is just built/deny traffic from logs.

Traffic Analysis – Russia (1/4)



IP	Count
185.187.90.106	260588
82.148.29.238	111172
89.111.148.109	19065
178.22.24.29	4988
141.105.66.247	4706
185.17.0.32	4190
77.83.207.168	3241
31.131.251.240	2477
45.135.232.27	1810
45.135.232.187	1655

Traffic Analysis – Russia (2/4)



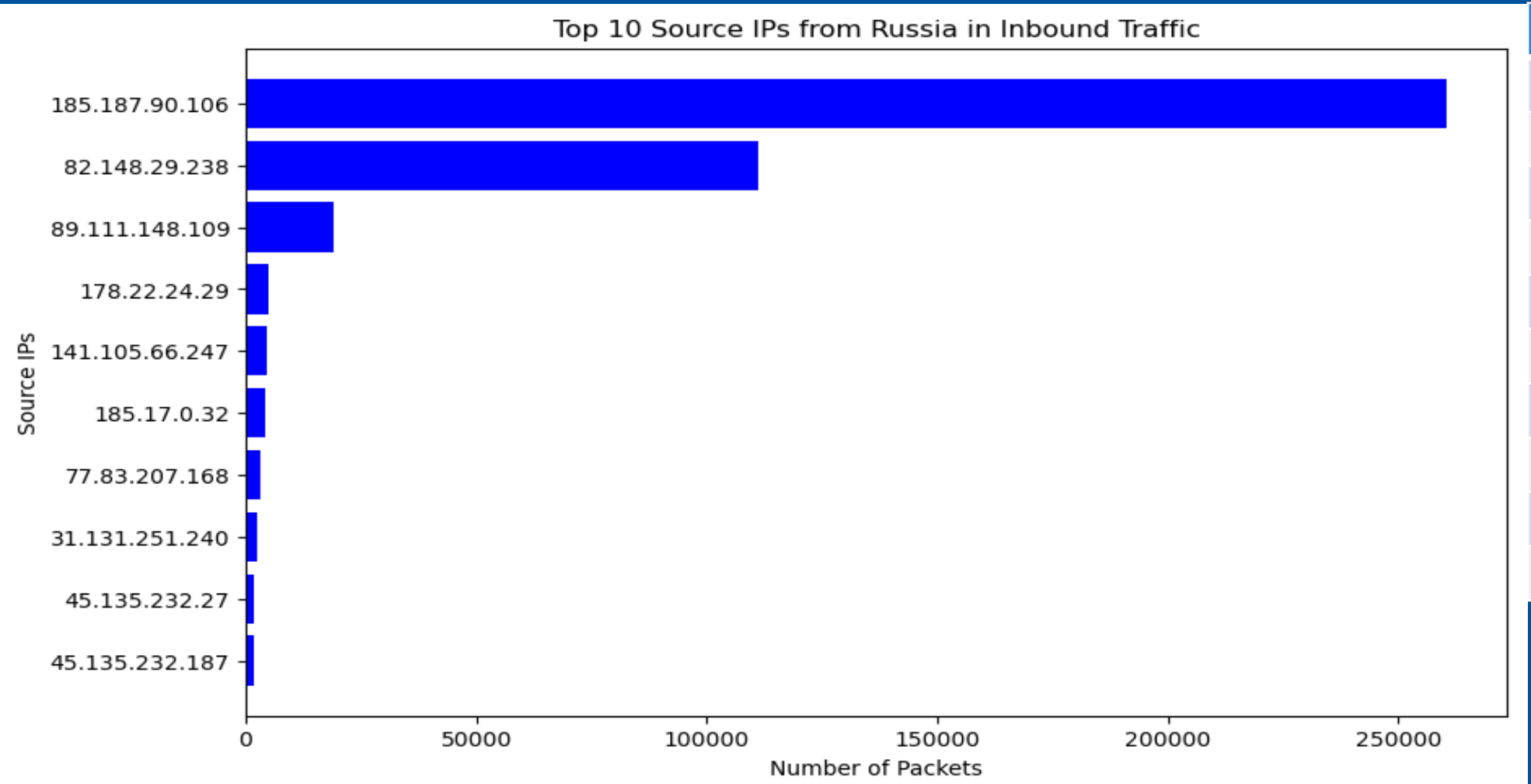
Top 10 Destination Servers:

- 4 Load balancers (different Campus VLANs)
- 2 CPanel Servers
- 2 Web Servers
- 2 License Servers

Note: This is just built/deny traffic from logs.

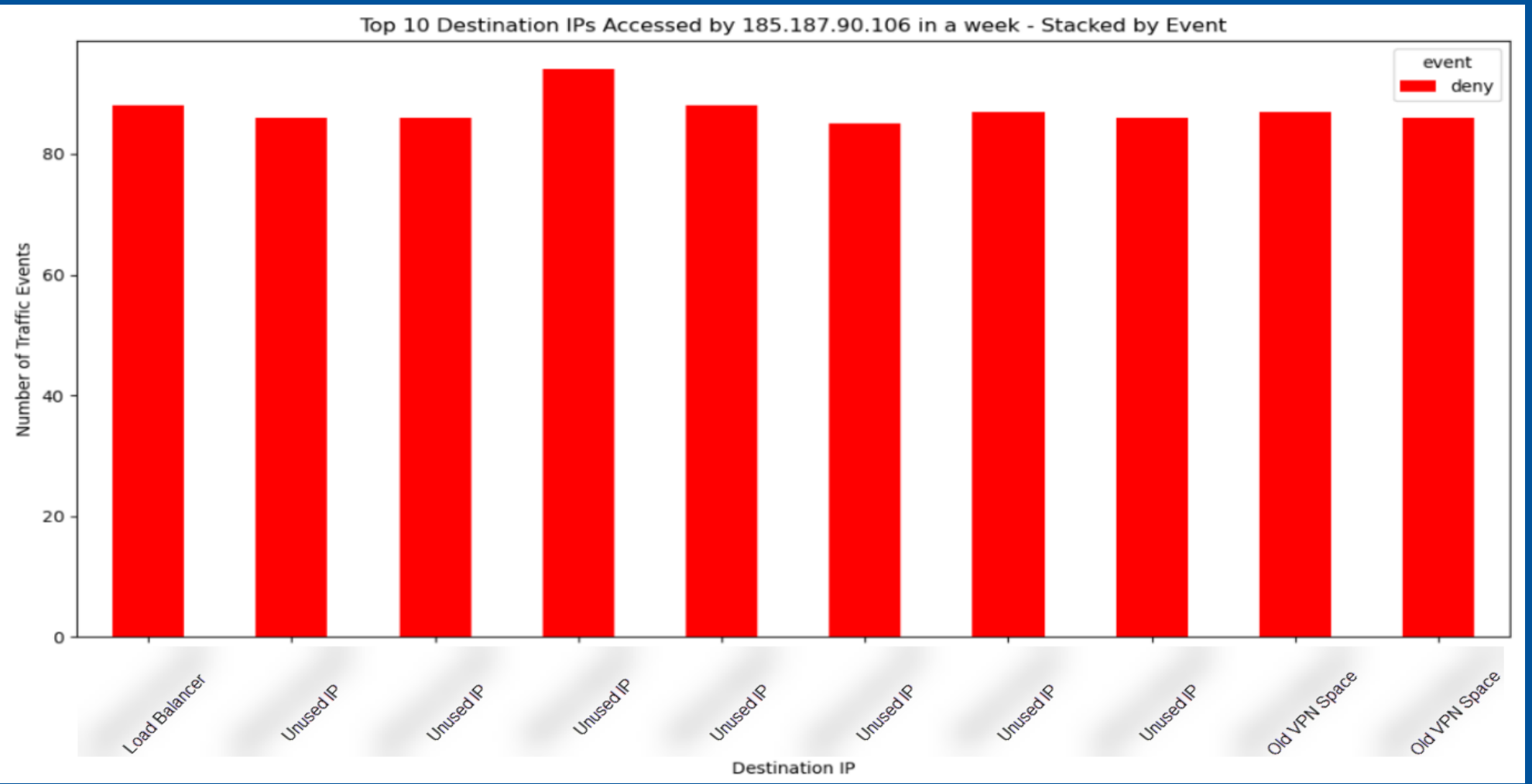
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – Russia (3/4)



IP	Flagged for Abuse
185.187.90.106	Yes
82.148.29.238	Yes
89.111.148.109	No
178.22.24.29	No
141.105.66.247	Yes
185.17.0.32	No
77.83.207.168	No
31.131.251.240	No
45.135.232.27	No
45.135.232.187	Yes

Traffic Analysis – Russia (4/4)



Top 10 Destination Servers for 185.187.90.106:

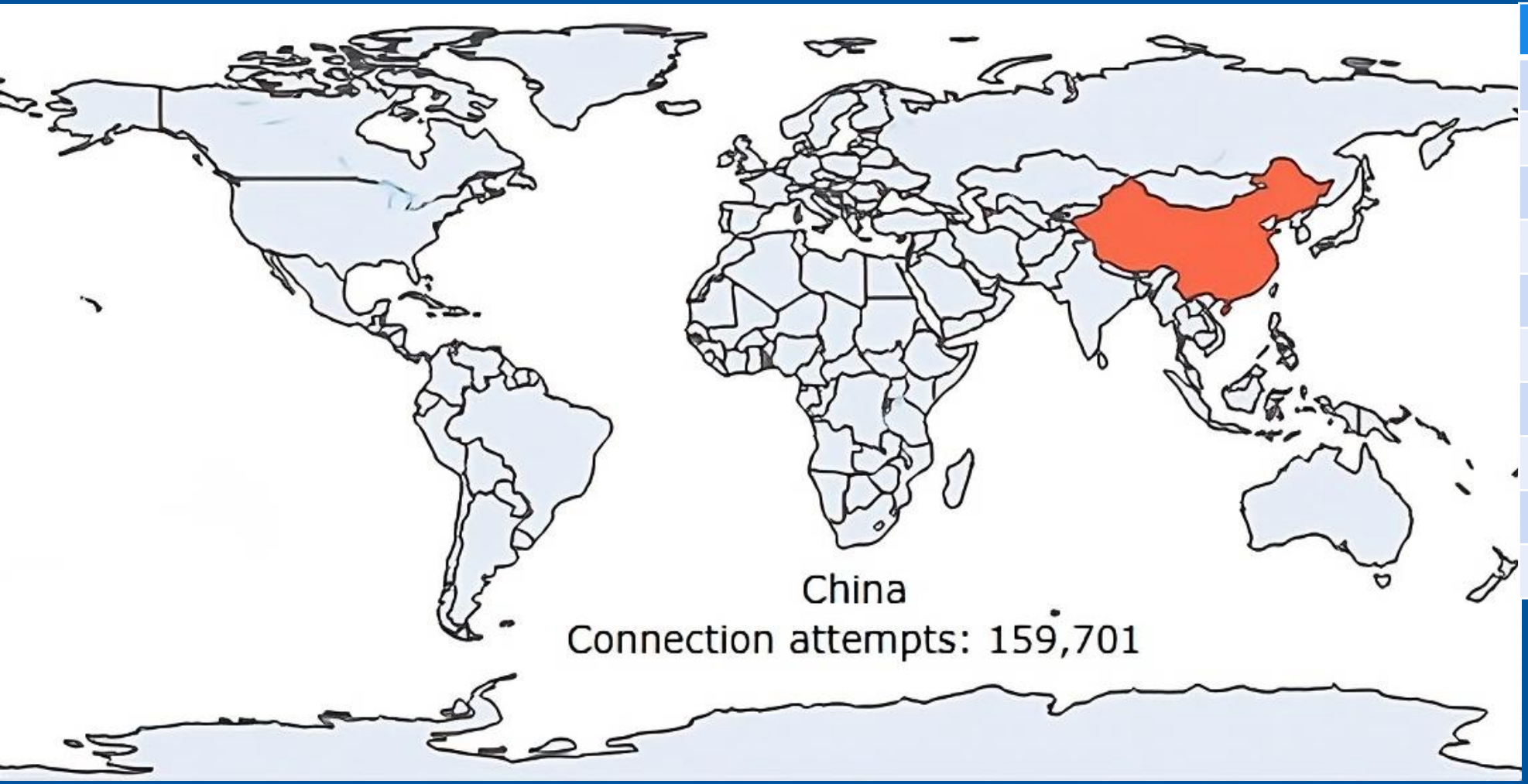
- 7 IPs were unused (different Campus VLANs)
- 1 Load balancers for a campus
- 2 IPs were in the Old VPN space

The destination port were varied for all the destination IPs. Some of them are listed here: 22409, 718, 6679, 52208, 5407, 374, 582.

Note: This is just built/deny traffic from logs.

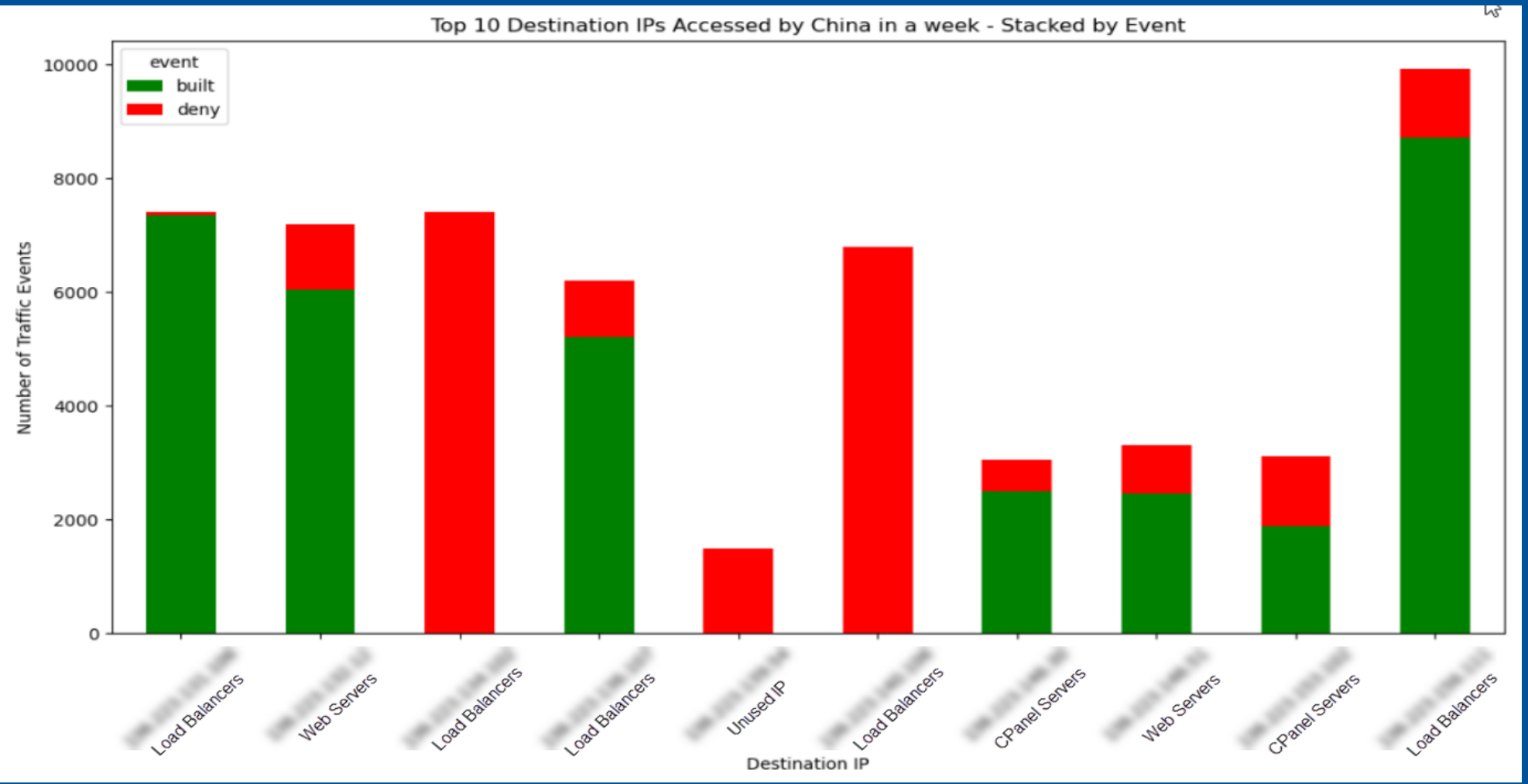
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – China (1/4)



Country	Count
117.68.67.83	11966
218.60.100.155	11671
36.150.90.83	11568
106.74.32.234	11501
119.167.174.59	9680
124.65.39.4	8137
182.242.52.190	7721
113.249.101.172	7034
157.0.3.36	5563
60.165.65.54	4974

Traffic Analysis – China (2/4)



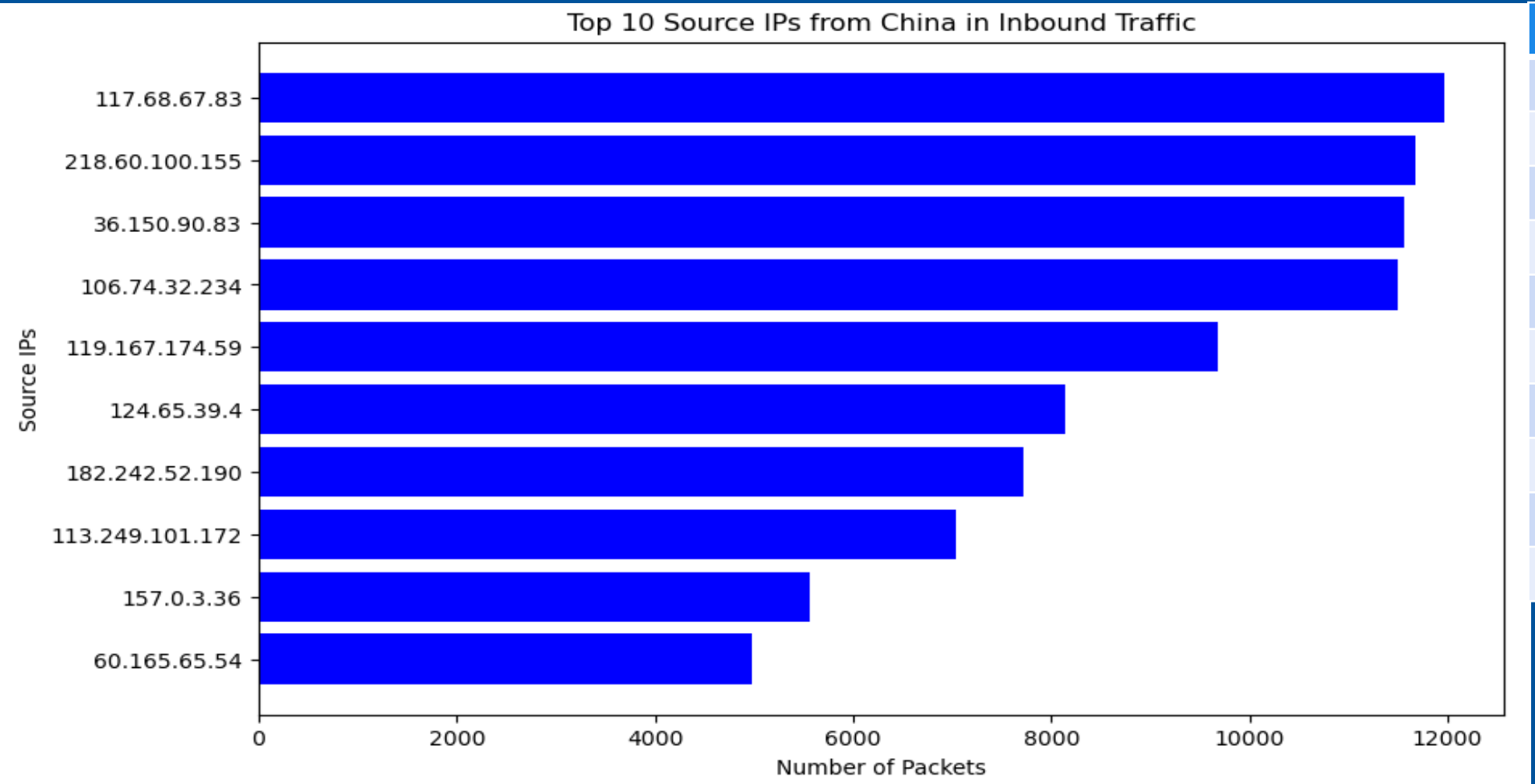
Top 10 Destination Servers:

- 5 Load balancers (different Campus VLANs)
- 2 CPanel Servers
- 2 Web Servers
- 1 Unused IP

Note: This is just built/deny traffic from logs.

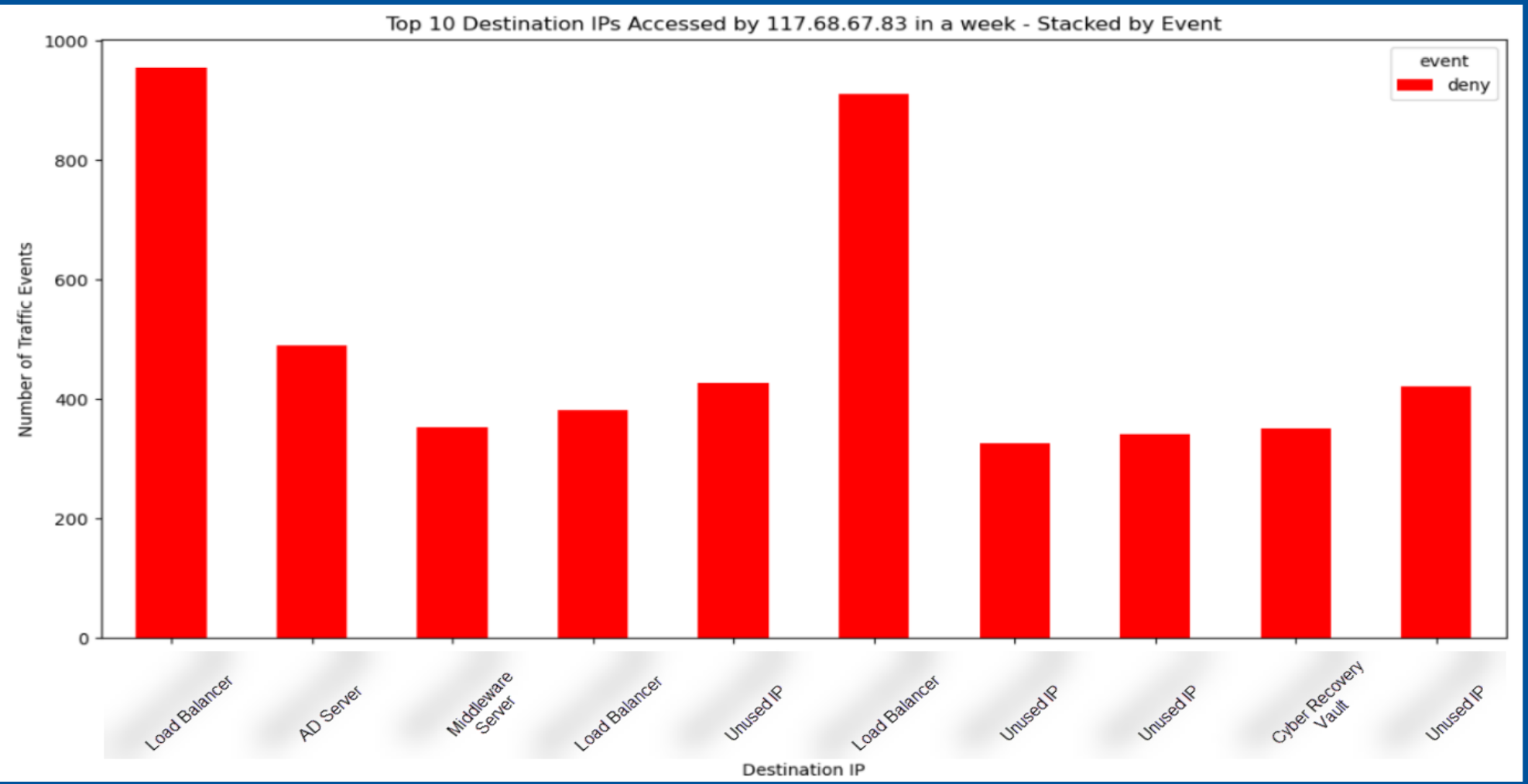
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – China (3/4)



Country	Flagged for Abuse
117.68.67.83	No
218.60.100.155	No
36.150.90.83	No
106.74.32.234	No
119.167.174.59	No
124.65.39.4	Yes
182.242.52.190	No
113.249.101.172	Yes
157.0.3.36	No
60.165.65.54	No

Traffic Analysis – China (4/4)



Top 10 Destination Servers for 117.68.67.83:

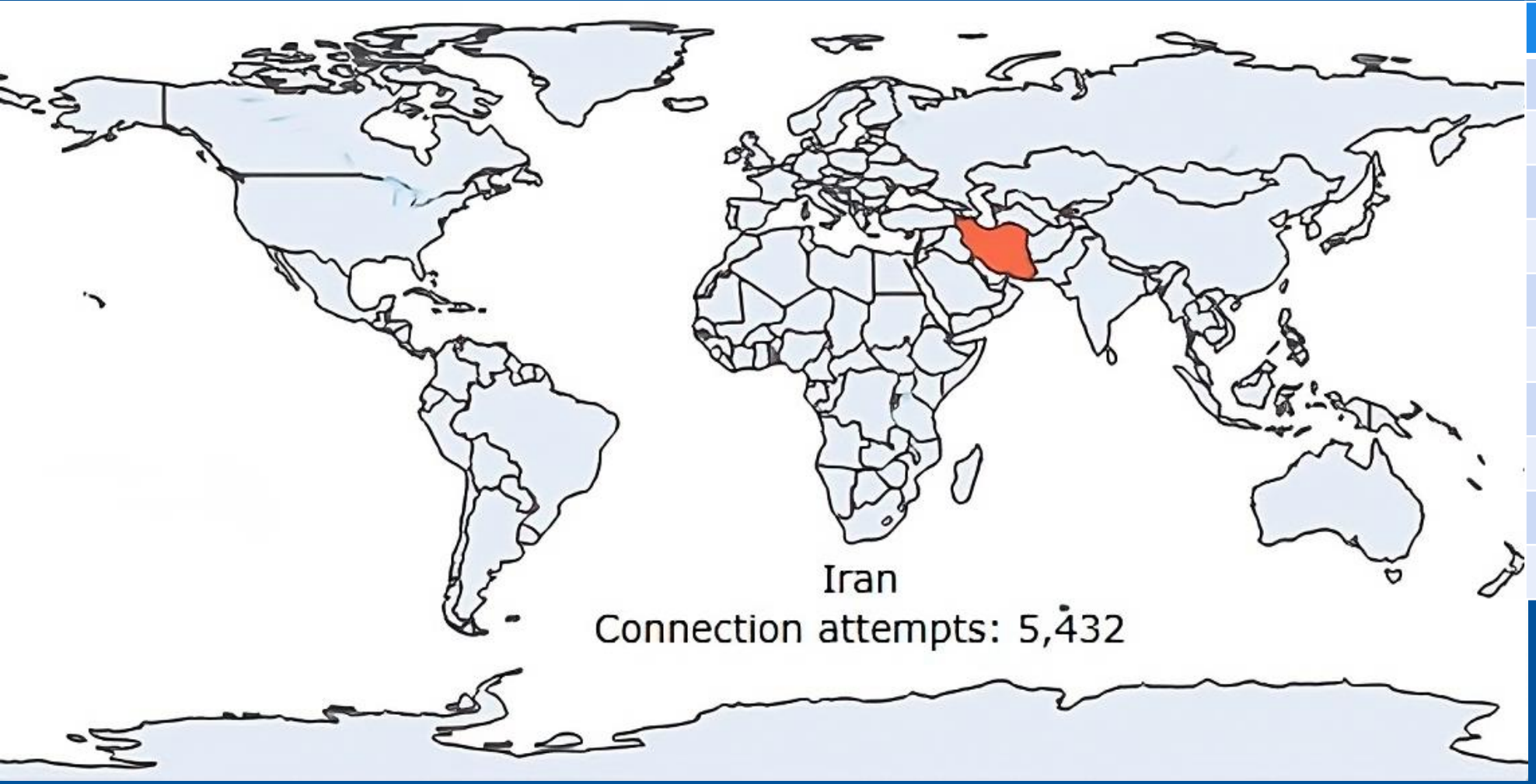
- 4 IPs were unused (different Campus VLANs)
- 3 Load balancers for a campus
- 1 AD Server
- 1 Middleware Server
- 1 Cyber Recovery Vault

The destination port were varied for all the destination IPs. Some of them are listed here: 18377, 19407, 12381, 13666, 21377, 25951, 59376, 2039, 60416, 63711.

Note: This is just built/deny traffic from logs.

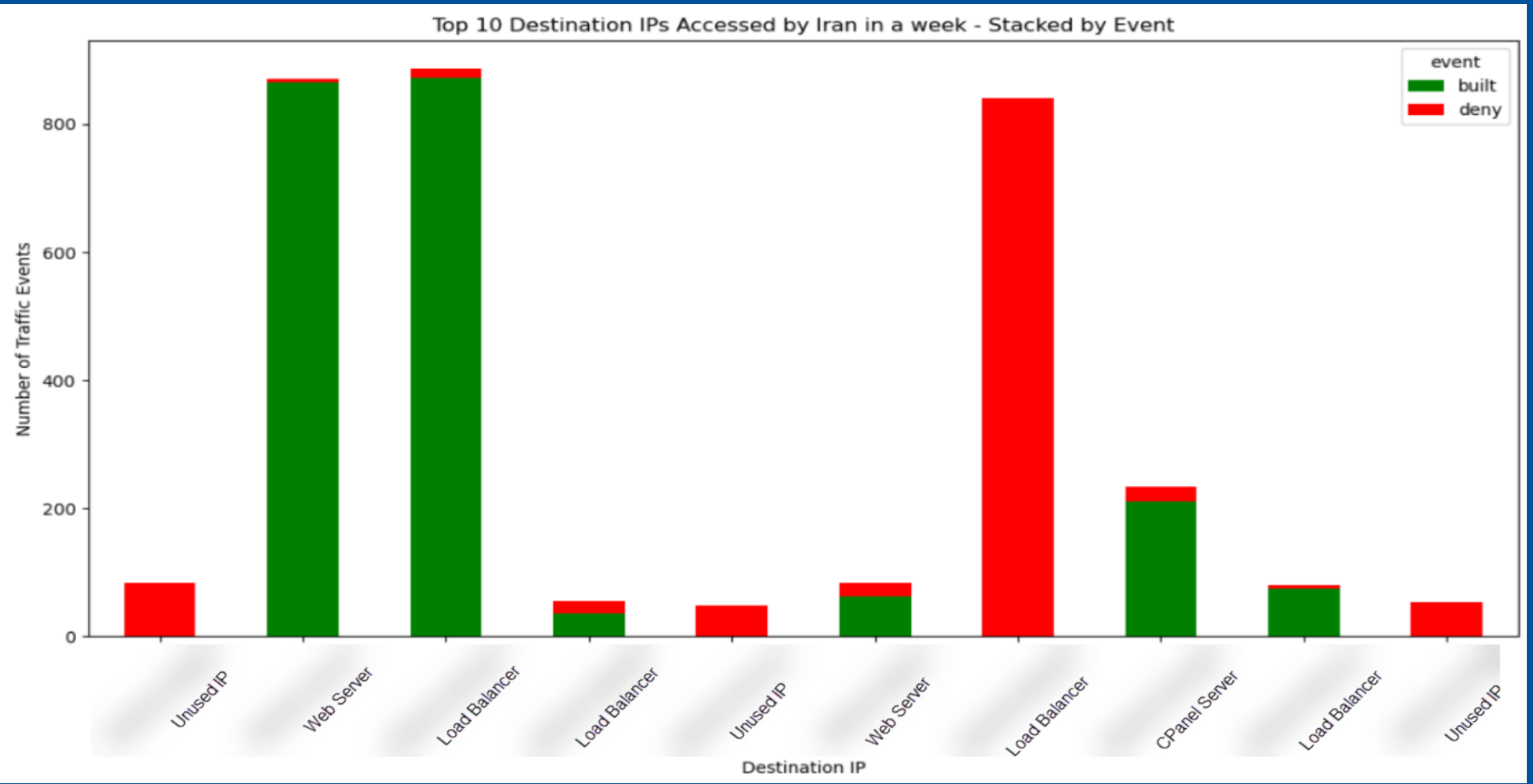
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – Iran (1/4)



Country	Count
185.60.136.200	1656
2.189.5.162	856
2.189.5.142	848
85.133.225.6	355
93.113.238.152	274
87.236.166.2	208
185.136.194.162	164
93.113.238.155	116
94.182.106.36	49
95.38.170.215	47

Traffic Analysis – Iran (2/4)

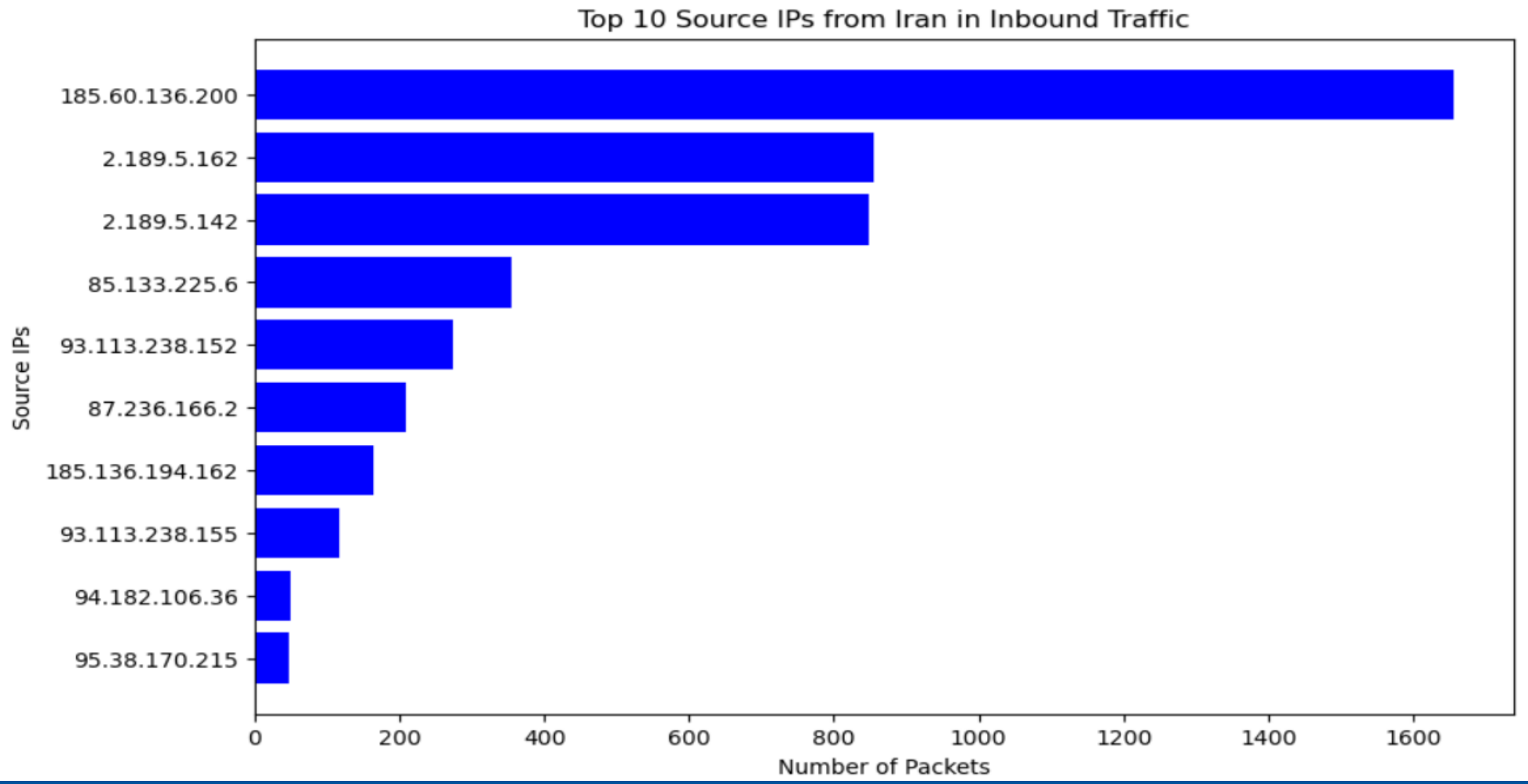


Top 10 Destination Servers:

- 4 Load balancers (different Campus VLANs)
- 3 Unused IP
- 2 Web Servers
- 1 CPanel Servers

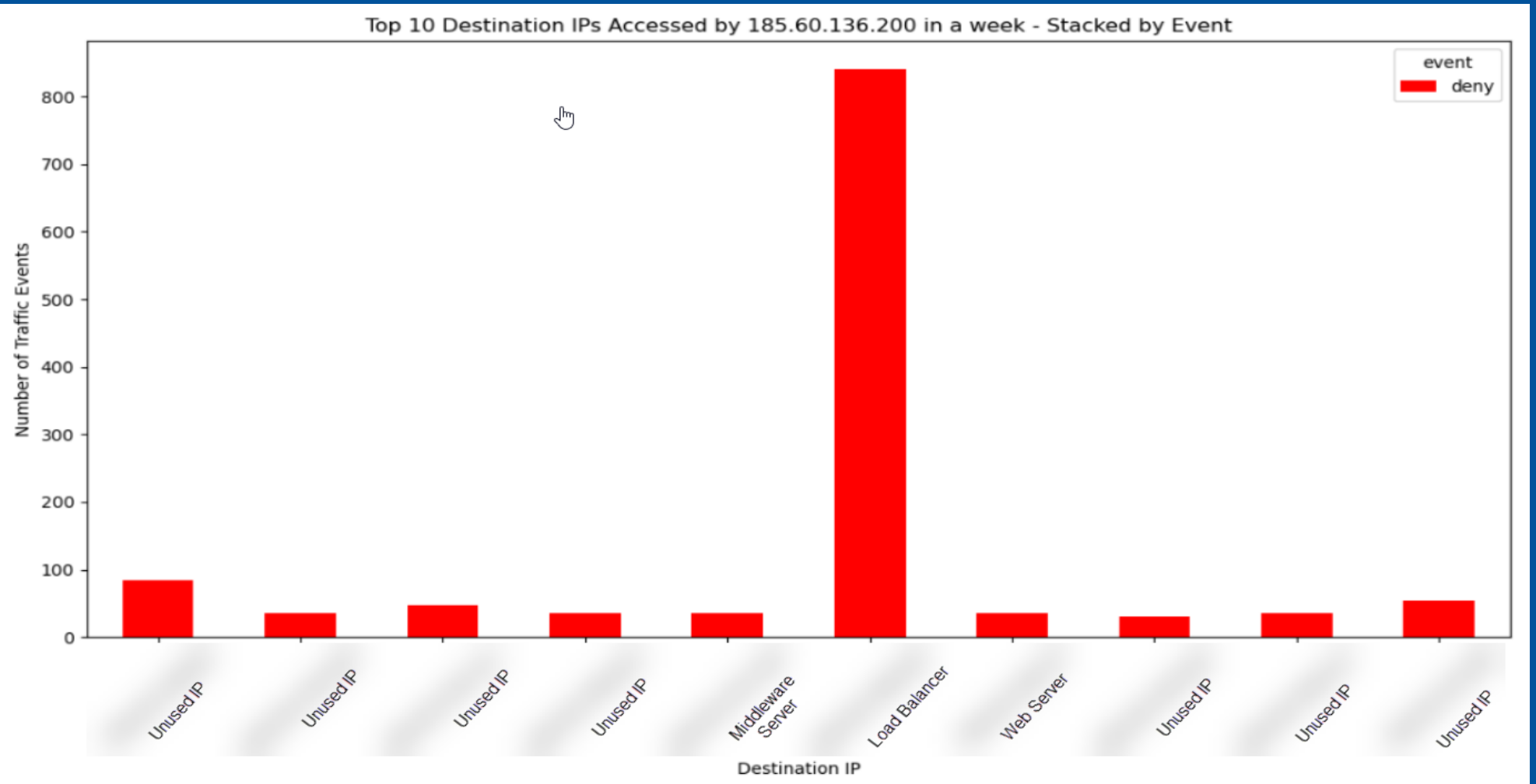
Note: This is just built/deny traffic from logs.

Traffic Analysis – Iran (3/4)



Country	Flagged for Abuse
185.60.136.200	Yes
2.189.5.162	Yes
2.189.5.142	Yes
85.133.225.6	Yes
93.113.238.152	No
87.236.166.2	Yes
185.136.194.162	Yes
93.113.238.155	No
94.182.106.36	Yes
95.38.170.215	Yes

Traffic Analysis – Iran (4/4)



Top 10 Destination Servers for 185.60.136.200:

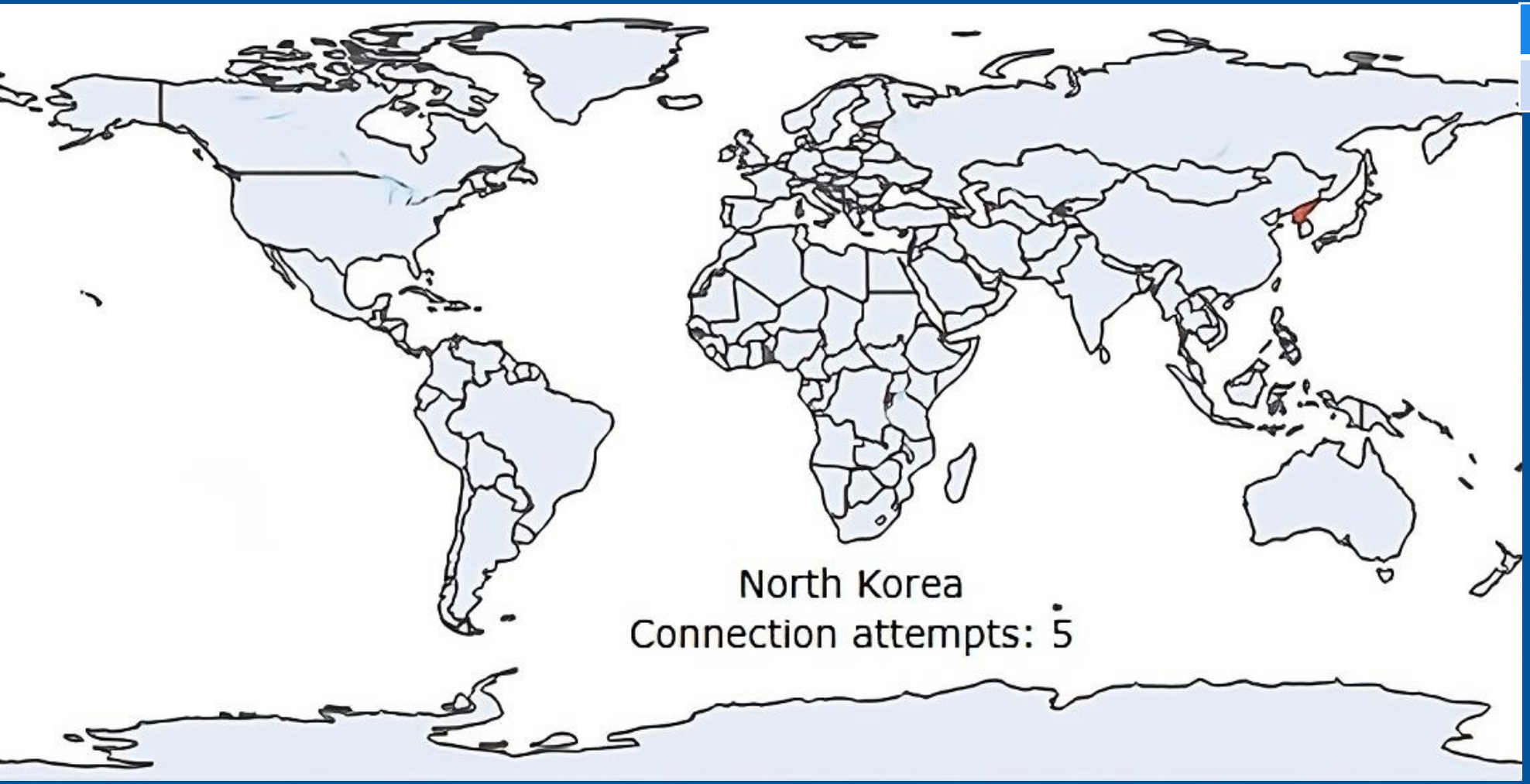
- 7 IPs were unused (different Campus VLANs)
- 1 Load balancer for a campus
- 1 Middleware Server
- 1 Web Server

The destination port was 22 for all the events related to the IP generating the most traffic.

Note: This is just built/deny traffic from logs.

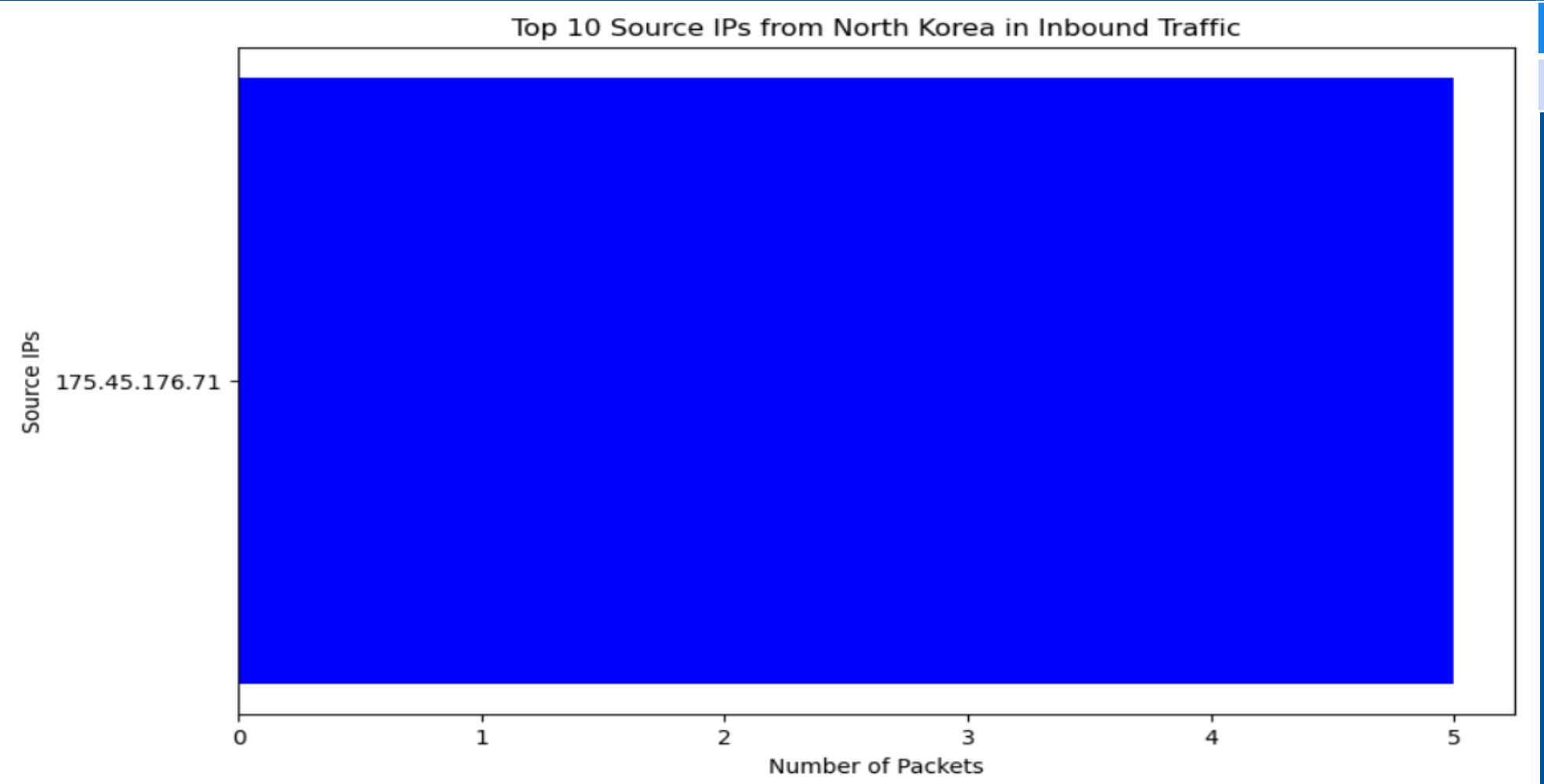
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – North Korea (1/3)



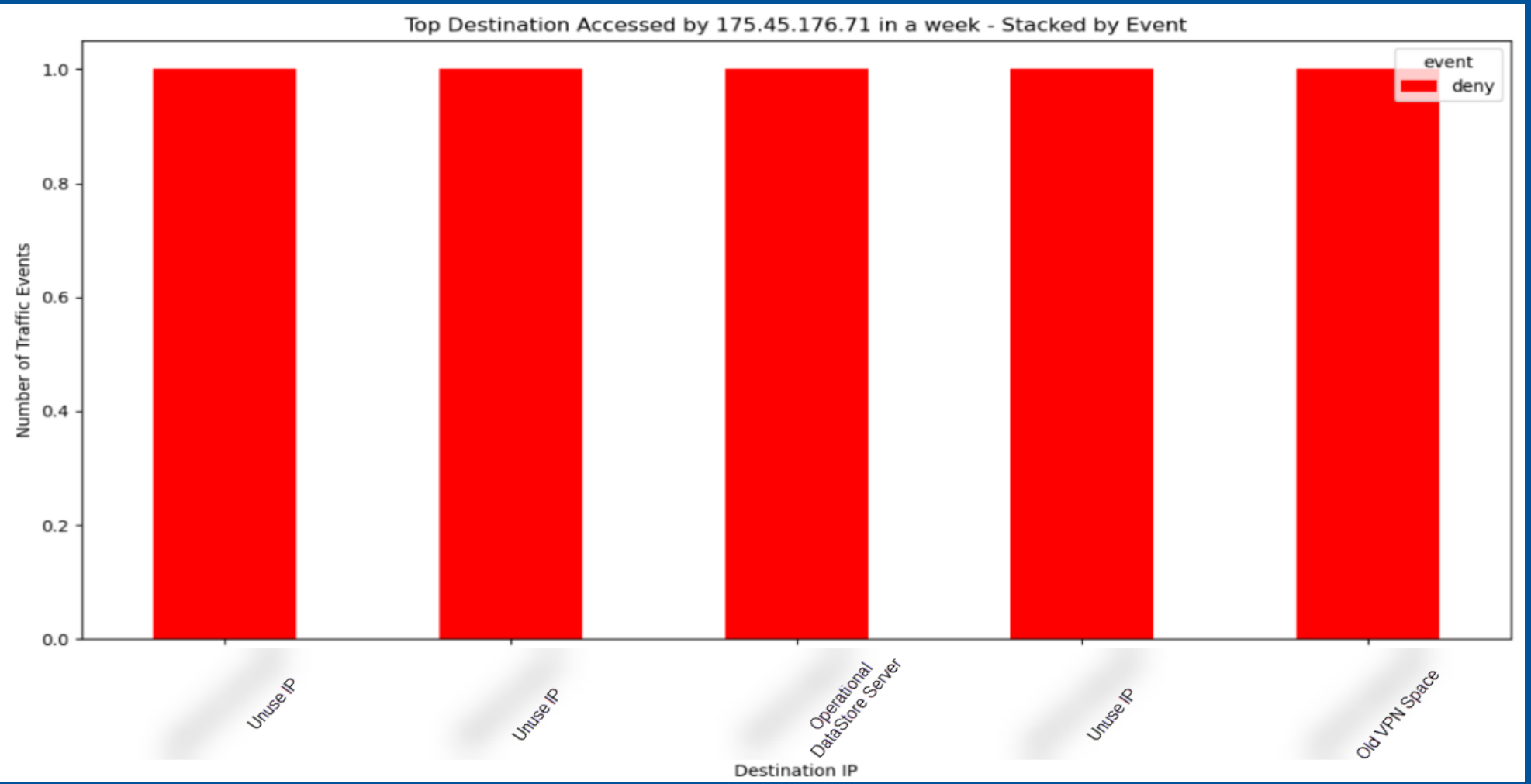
Country	Count
185.60.136.200	5

Traffic Analysis – North Korea (2/3)



Country	Flagged for Abuse
185.60.136.200	No

Traffic Analysis – North Korea (3/3)



Top 10 Destination Servers for 175.45.176.71:

- 3 IPs were unused (different Campus VLANs)
- 1 Operational DataStore Sever
- 1 IP in old VPN Space

The destination port were varied for all the destination IPs. Some of them are listed here: 58413, 64695, 22731, 45871, 38129.

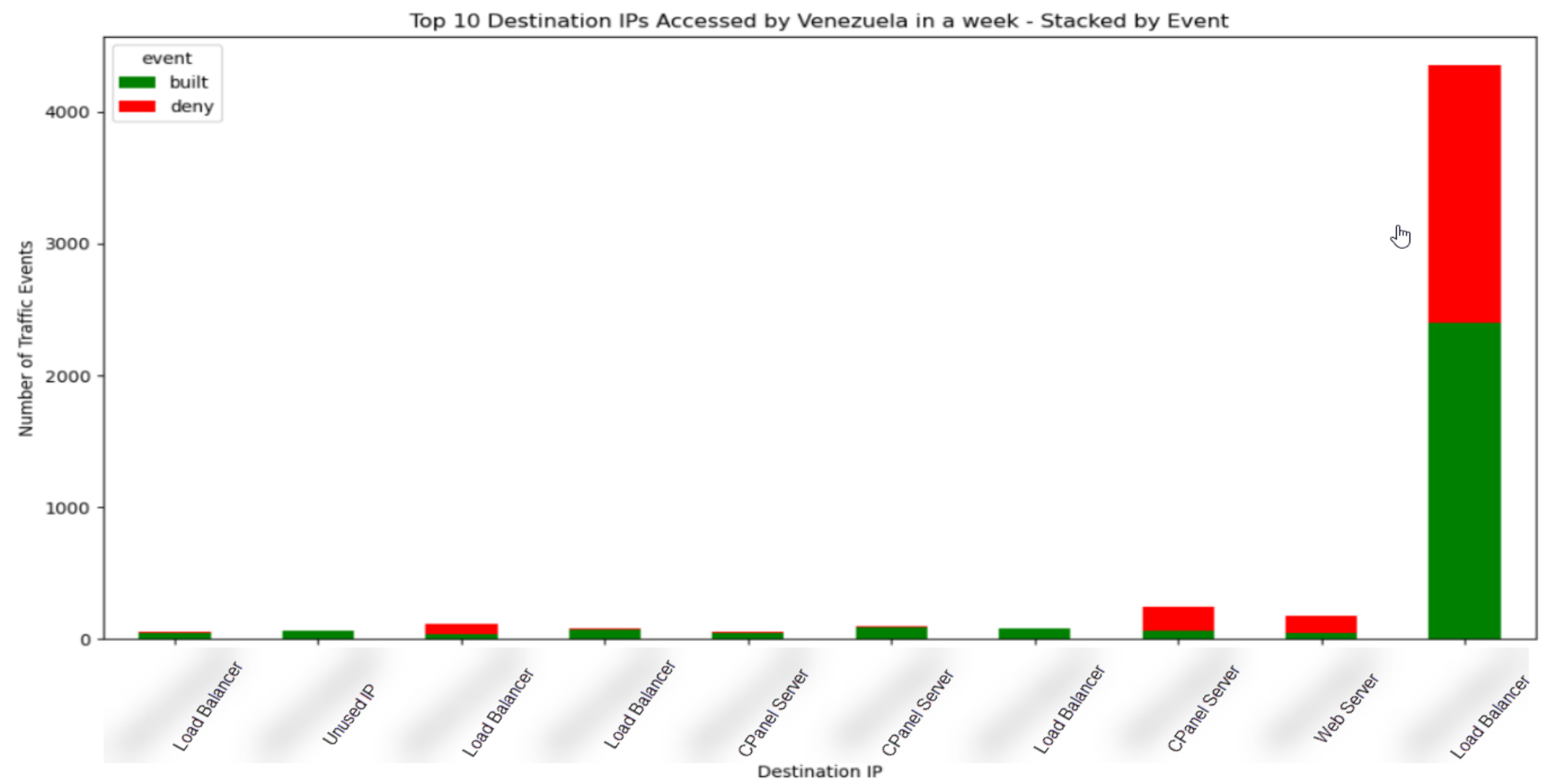
Note: This is just built/deny traffic from logs.

SUNY ITEC Information Technology Exchange Center

Traffic Analysis – Venezuela (1/4)

Country	Count
200.82.188.135	164
181.208.183.224	122
190.203.111.130	110
190.97.226.221	109
45.175.36.1	84
181.208.29.230	83
170.81.145.5	75
170.81.145.187	72
186.185.41.70	64
82.86.131.60	62

Traffic Analysis – Venezuela (2/4)



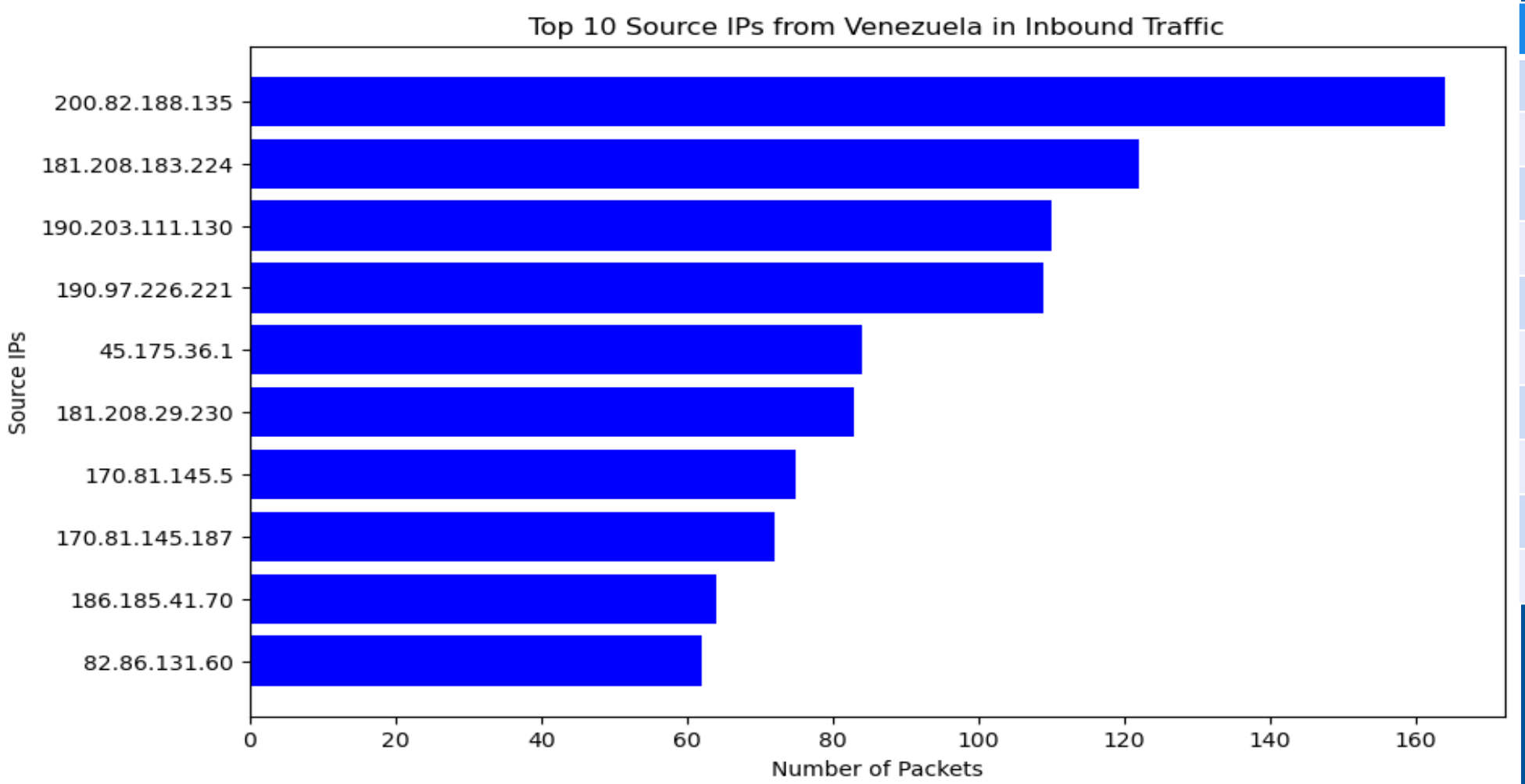
Top 10 Destination Servers:

- 5 Load balancers (different Campus VLANs)
- 3 CPanel Servers
- 1 Web Servers
- 1 Unused IP

Note: This is just built/deny traffic from logs.

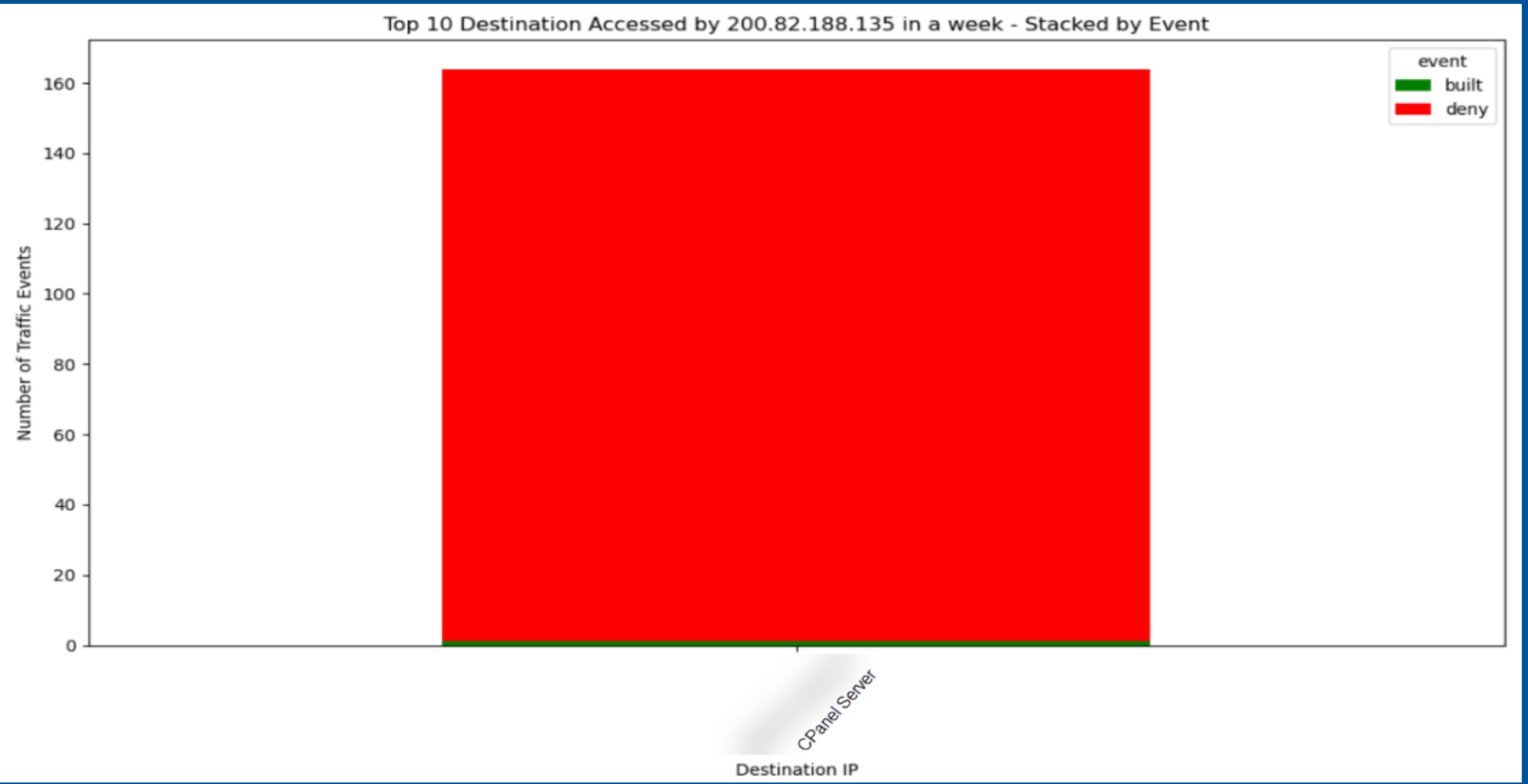
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – Venezuela (3/4)



Country	Flagged for Abuse
200.82.188.135	No
181.208.183.224	No
190.203.111.130	No
190.97.226.221	No
45.175.36.1	No
181.208.29.230	No
170.81.145.5	No
170.81.145.187	No
186.185.41.70	No
82.86.131.60	No

Traffic Analysis – Venezuela (4/4)



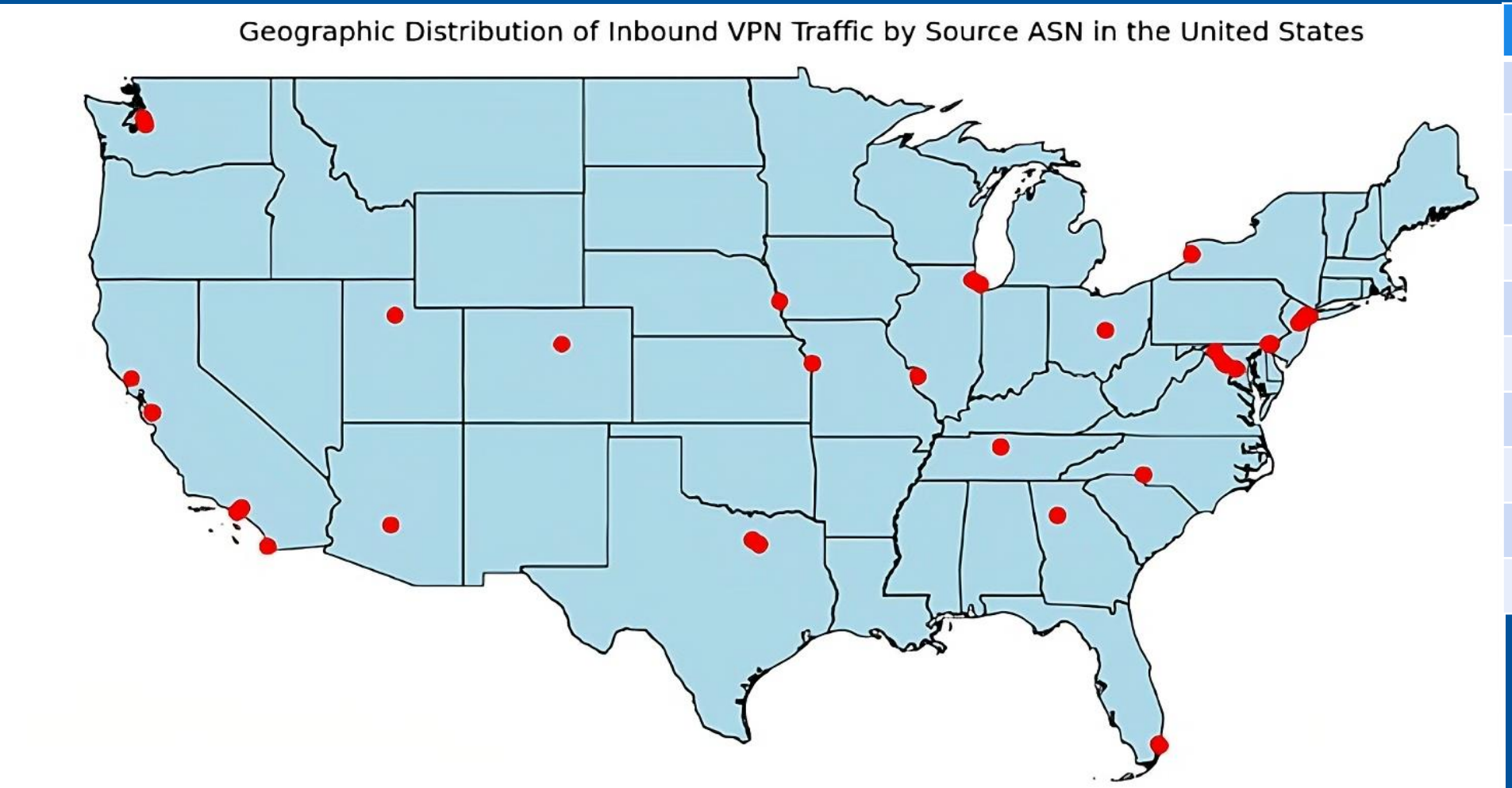
Analyzed traffic from the IP with most inbound traffic that week shows all traffic headed to a web hosting management platform.

The destination port was 443 for all the events related to the IP generating the most traffic.

Note: This is just built/deny traffic from logs.

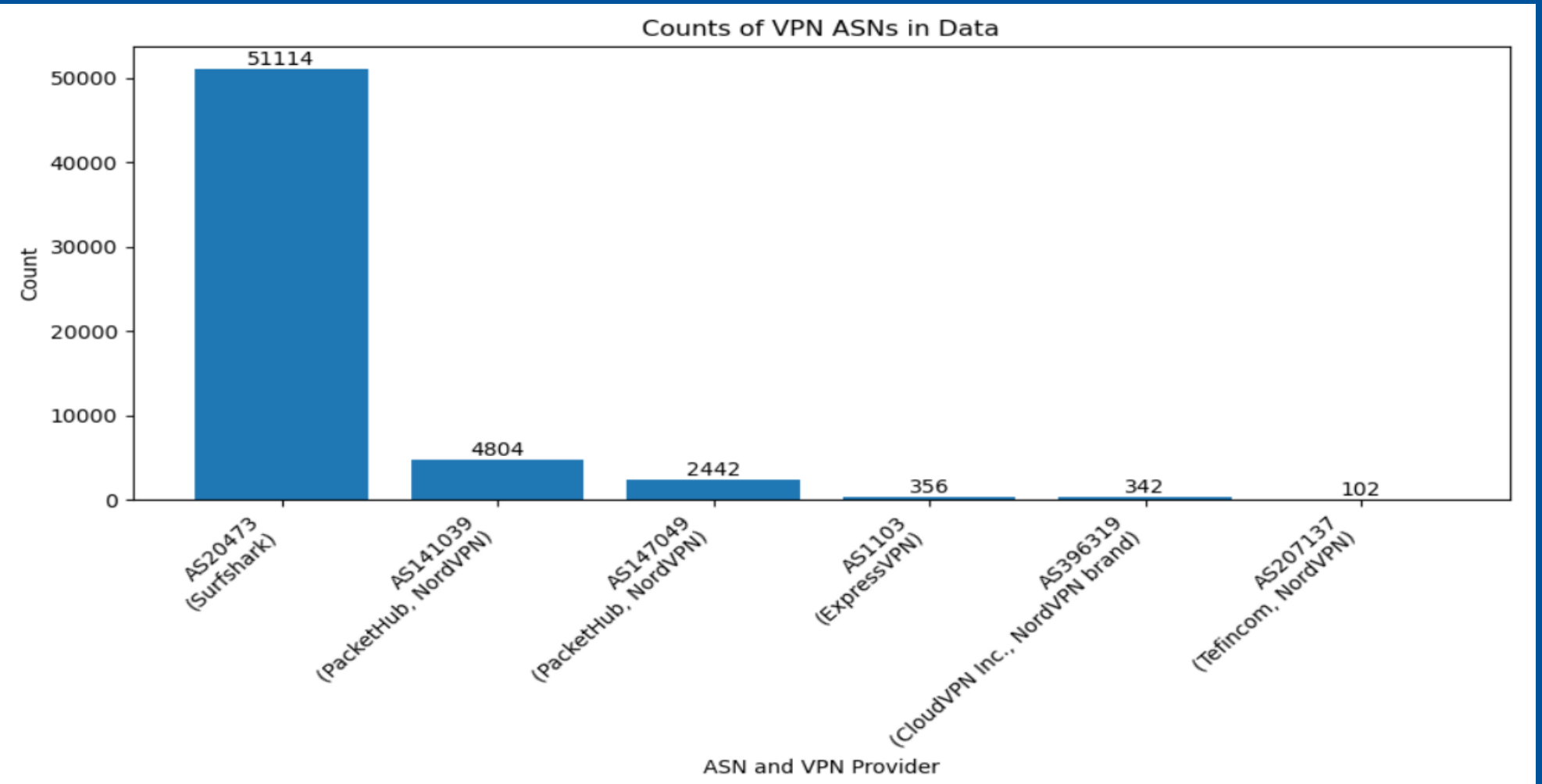
SUNY ITEC Information Technology Exchange Center

Traffic Analysis – VPN (1/4)



City	Count
New York City	348
Wilmington	247
Leesburg	227
Newark	142
Buffalo	139
Chicago	121
Dallas	76
Piscataway	69
El Segundo	66
Miami	28

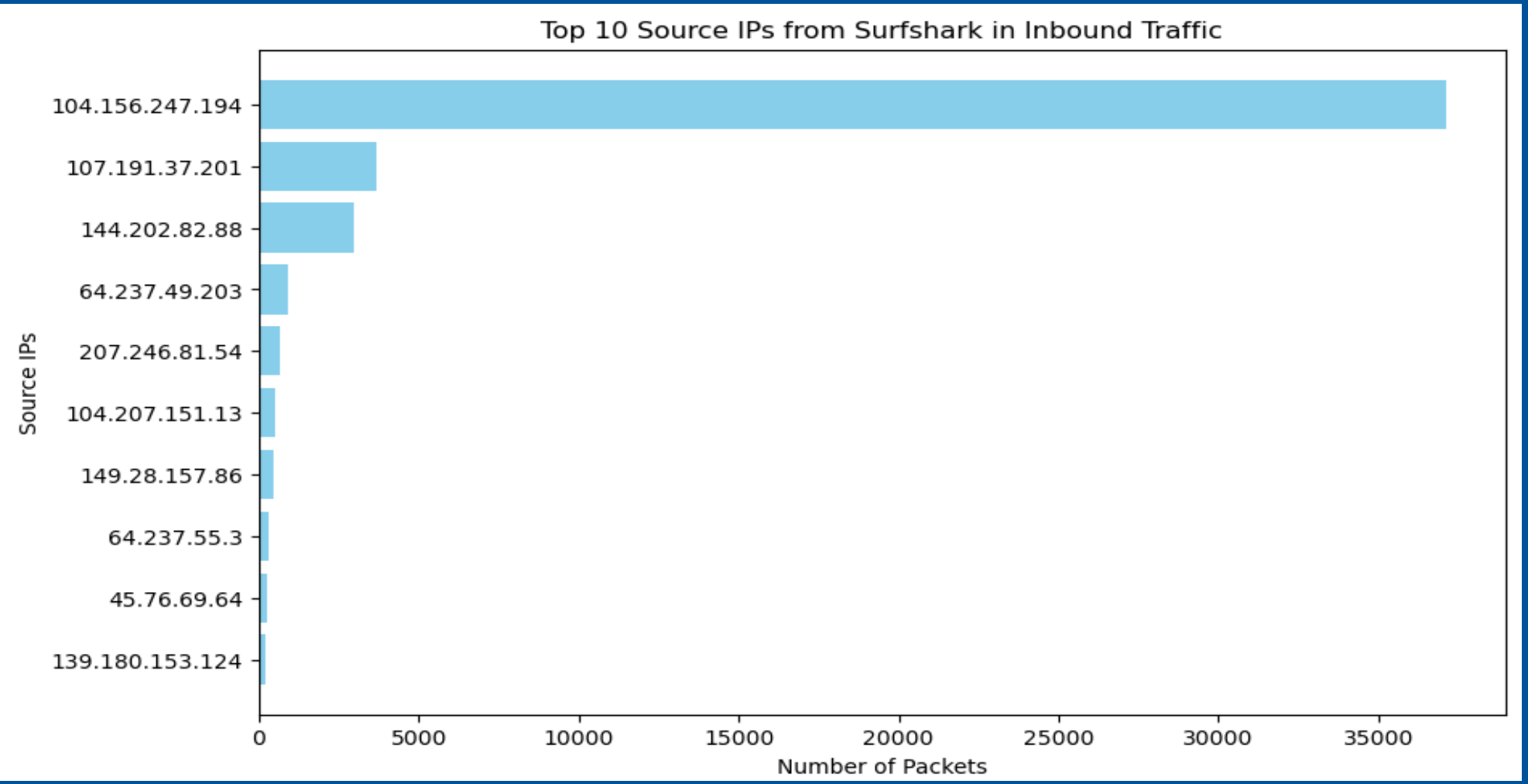
Traffic Analysis – VPN (2/4)



Considering only inbound traffic, there were a total of 59160 events recorded (including both 'built' and 'deny' actions) just from ASsN (Autonomous System Number) that belongs to Surfshark VPN, Nord VPN and Express VPN.

Note: This is just built/deny traffic from logs.

Traffic Analysis – VPN (3/4)

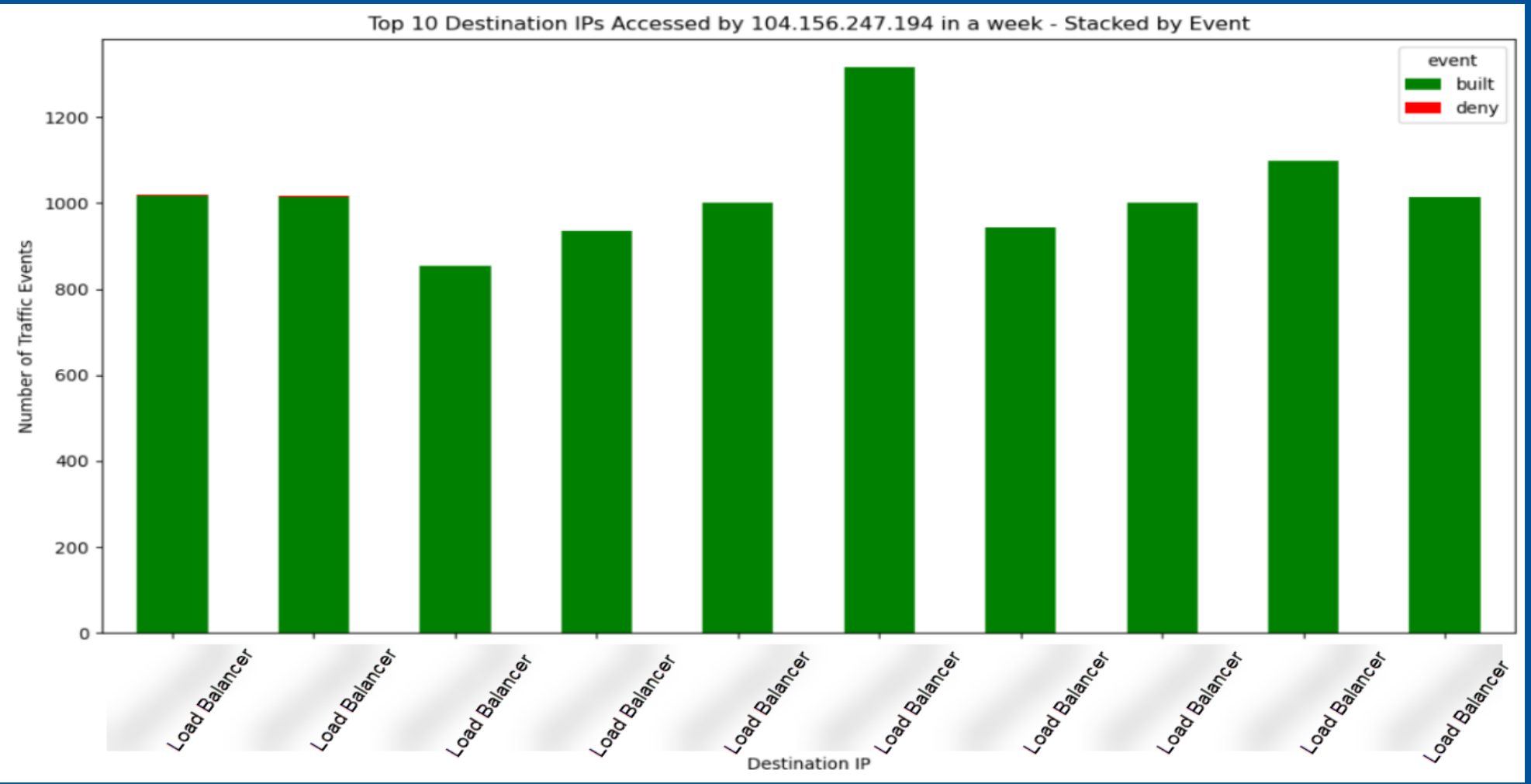


Considering only inbound traffic, there were a total of 51114 events recorded (including both 'built' and 'deny' actions) just from an ASN (Autonomous System Number) that belongs to Surfshark VPN.

Note: This is just built/deny traffic from logs.

SUNY ITEC Information Technology Exchange Center

Traffic Analysis – VPN (4/4)



Analyzed traffic from the IP with most inbound traffic that week shows all destination IPs were load balancers for different campus VLANs.

The destination ports were mostly 443, 10000, 9443, 10003 for all the events related to the IP generating the most traffic. These are mostly ports associated to Banner.

There is no way to tell whether this is one person accessing all these servers or different people assigned this IP at different times.

What's the solution to protecting yourself from people using VPN to bypass GeoIP?

SUNY ITEC Information Technology Exchange Center


A Defenders Perspective
Objective: Protect the business!

Source: TheGuardian.com

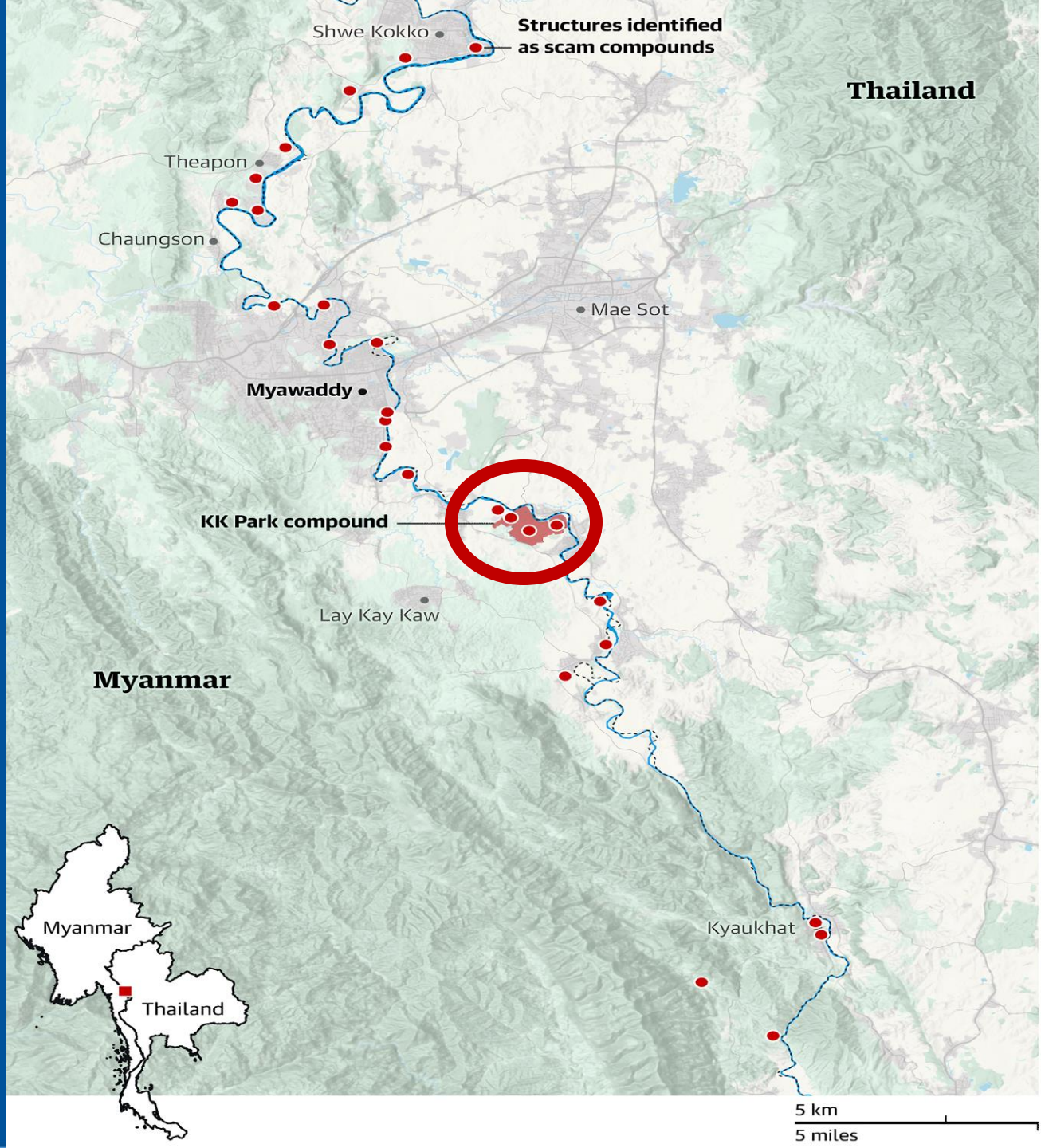
Expansion of KK Park compound

Nov 2019

Source: TheGuardian.com

Operating at Scale

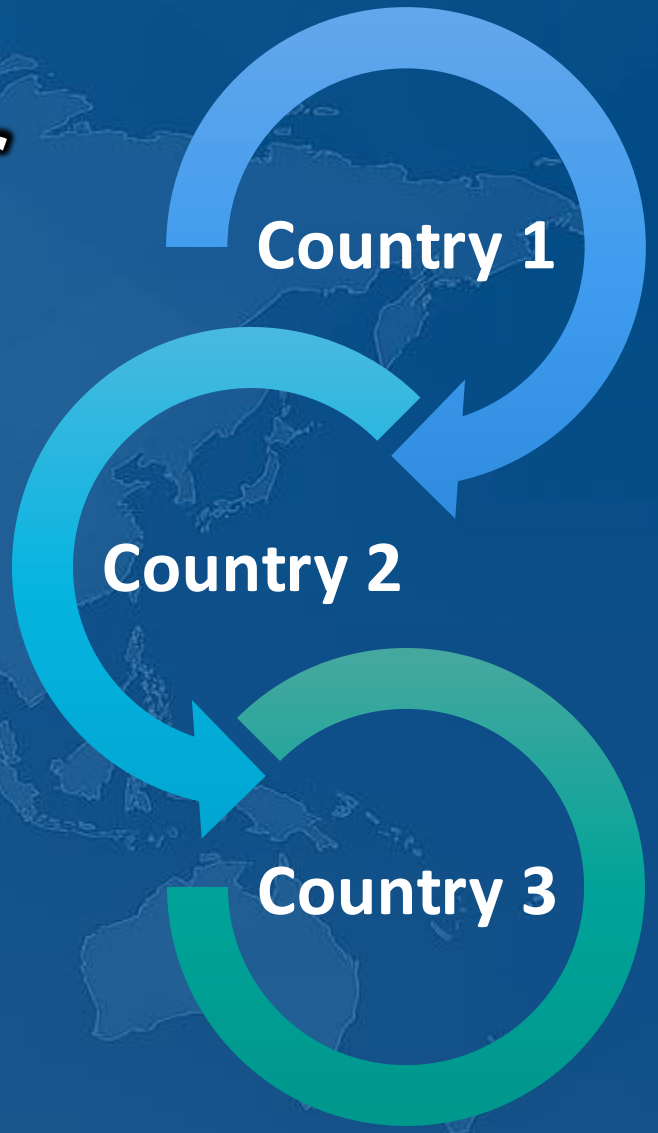
1. This is just one part of the world!
2. We are being outpaced.
3. Device to IT Admin Estimates
    1. EDU: 500:1 to over 2000:1
    2. Private Sector: 70:1 to 100:1
4. Being proactive and implementing GeoIP blocking is crucial.



Implementation Challenges & Considerations

Scenario Consideration: Local Attacker

1. Our Data – The attacker is not next door.
2. Block low-effort, opportunistic attacks.
3. Reduces noise on defenses at the perimeter.
4. Removes "easy access" from APTs.



Scenario Consideration: Student Population

Smart GeoIP Logical Controls for Inclusive Campus Security

1. Allow/Block Lists with Exceptions
2. Create Granular Policies by Application
3. Leverage IP Range Exclusions
4. Combine GeoIP with Identity Controls for Remote Access

High-Level Roadmap

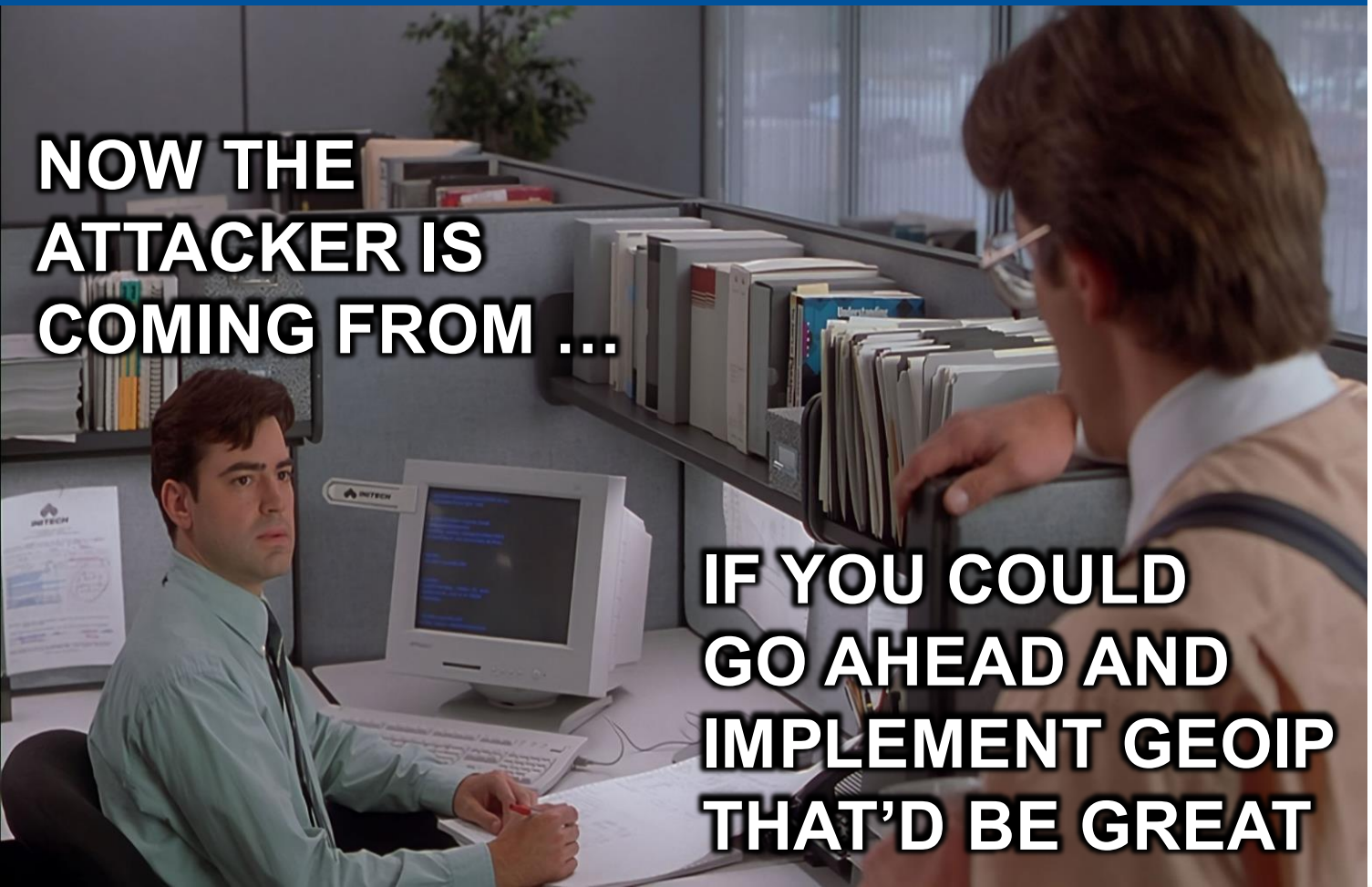
1. Approval (Research)
2. Inventory
3. Capabilities
4. Recommend
5. Approval (Pilot)
6. Report Findings
7. Approval (Implement)
8. Implement
9. Monitor Change

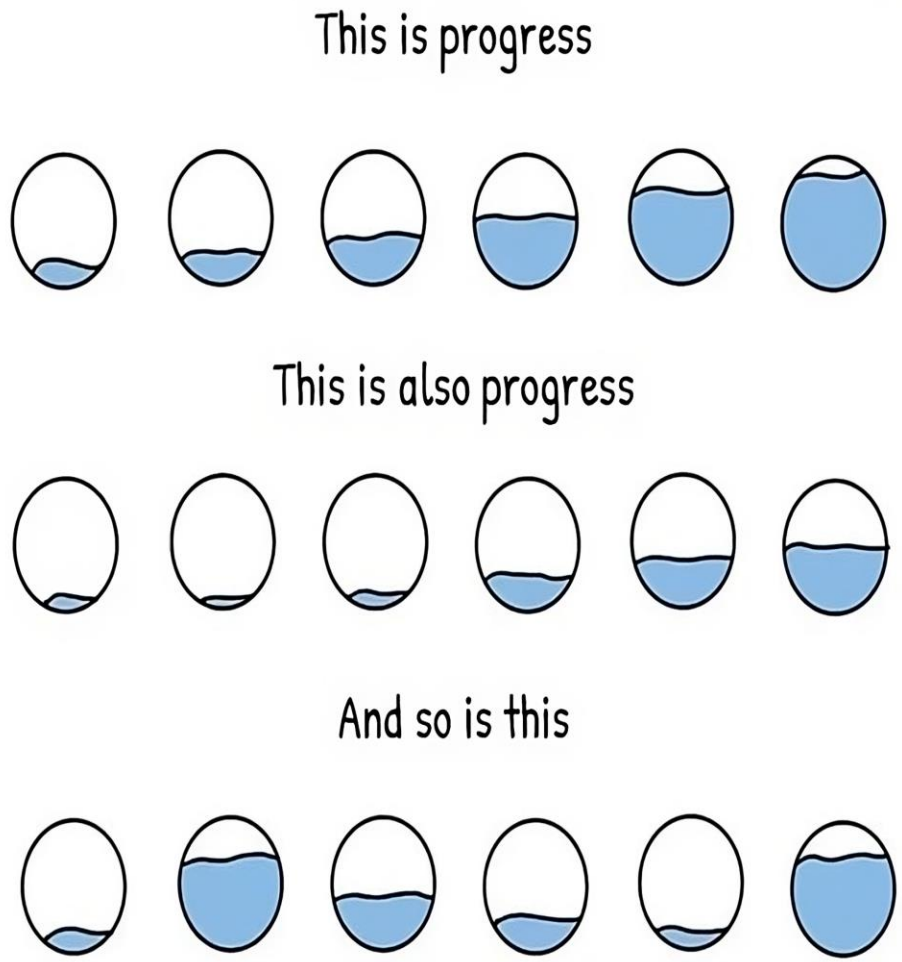
Learning The Hard Way

Risk-Based Prioritization

1. Firewalls
2. Remote Access
3. Web App Firewall (WAF)
4. Load Balancers
5. Cloud Services
6. Identity and Access Management Platforms
7. Security Gateways (DNS/Content Filtering)
8. Email Servers

Progress over Perfection





Rationale for Implementation

1. Reduces Risk
2. Low-Cost / No-Cost
3. Due Care (Proactive Efforts)
4. Recommended by U.S. Government & Industry Leaders

Block banned countries

Government Regulations:
EAR (Export Administration Regulations)
OFAC (Office of Foreign Assets Control)
ITAR (International Traffic in Arms Regulations)

You can implement policies to block websites hosted in countries categorized as high risk. The designation of such countries may result from your organization's customers or through the implementation of regulations including EAR ↗, OFAC ↗, and ITAR ↗.

Guidance from Cloudflare

Block banned countries

You can implement policies to block websites hosted in countries categorized as high risk. The designation of such countries may result from your organization's customers or through the implementation of regulations including EAR ↗, OFAC ↗, and ITAR ↗.

Government Regulations:
EAR (Export Administration Regulations)
OFAC (Office of Foreign Assets Control)
ITAR (International Traffic in Arms Regulations)

Dashboard API

Selector	Operator	Value	Action
Resolved Country IP Geolocation	in	*Afghanistan, Belarus, Congo (Kinshasa), Cuba, Iran, Iraq, Korea, North, Myanmar, Russian Federation, Sudan, Syria, Ukraine, Zimbabwe*	Block

DNS Security Risk Blocking

7	Threat Intel Feeds	BLOCK	✓
8	GeoIP Restrictions	BLOCK	✓
9	Block Top-Level Domains	BLOCK	✓
10	Block Content Categories	BLOCK	✓
11	Block Security Threats	BLOCK	✓
12	Block Malicious Domains	BLOCK	✓
13	Block Malicious IPs	BLOCK	✓
14	Hide Explicit Search Results	SAFE SEARCH	✓

Traffic: Resolved Country IP Geolocation
OR Traffic: Source Country IP Geolocation

HTTP Security Risk Blocking

33	HTTP Block Security Threats	BLOCK	✓
34	HTTP Block Top-Level Domains	BLOCK	✓
35	HTTP Block Malicious Domains	BLOCK	✓
36	HTTP Block Malicious IPs	BLOCK	✓
37	HTTP GeoIP Restrictions	BLOCK	✓

Traffic: Resolved Country IP Geolocation
OR Traffic: Source Country IP Geolocation

Doing More With Less

- Attack volume keeps increasing.
- Staffing and budgets do not.
- Exposure must be reduced before unnecessary work is created.
- GeoIP controls can be applied in:
  - Firewalls
  - Load Balancers
  - Application Gateways
  - Web Application Firewalls (WAF)
  - Applications

Questions or Feedback

Hitesh Upadhyay – hitesh.upadhyay@itec.suny.edu
Michael Kozlowski – michael.kozlowski@itec.suny.edu
Travis G. Kench, CISSP – travis.kench@itec.suny.edu

SUNY ITEC Information Technology Exchange Center