

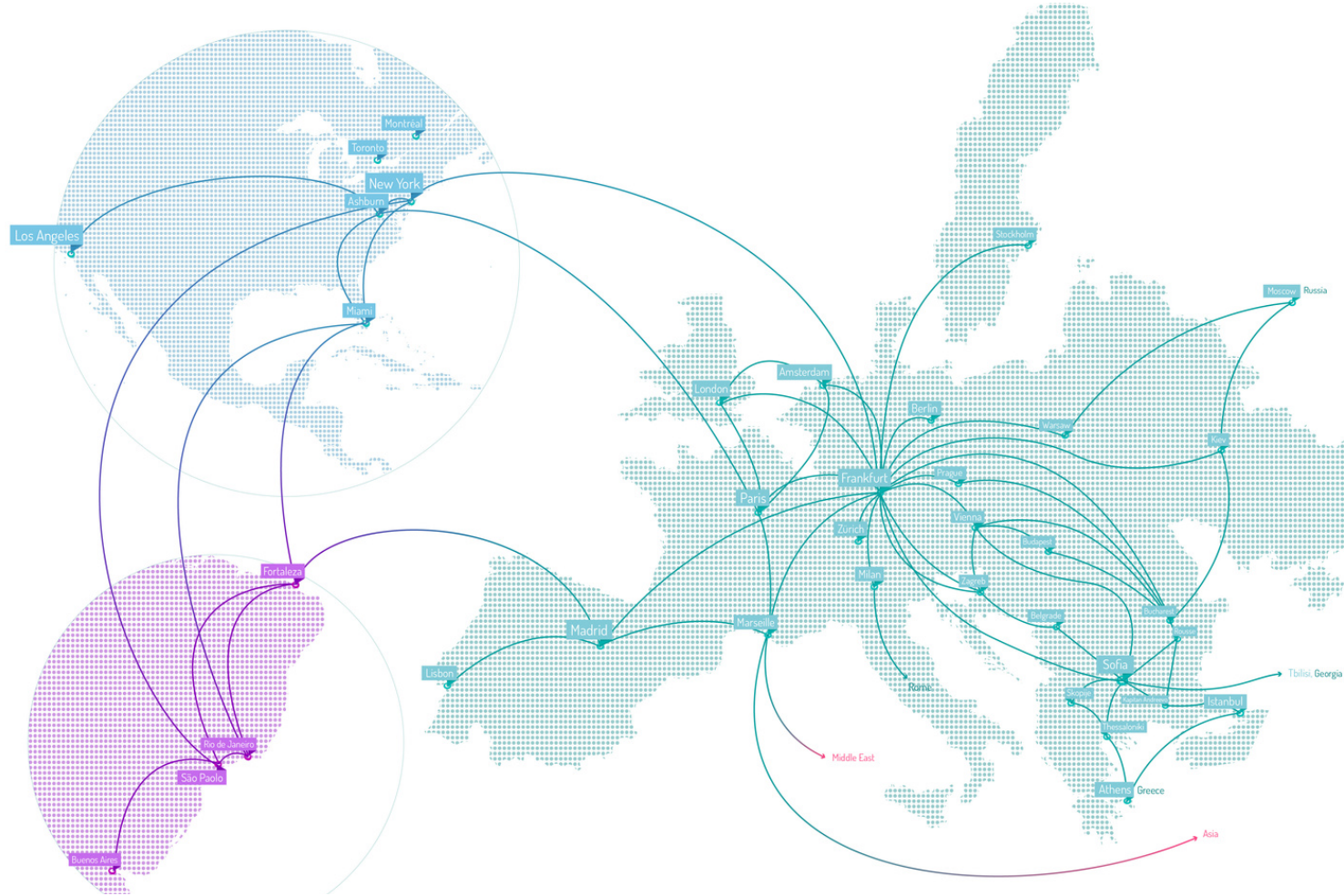
```
$distArray = array();  
$row = mysqli_fetch_assoc($result);  
$correctAnswer = $row['Correct'];  
$distArray['A'] = $row['Anum'];  
$distArray['B'] = $row['Bnum'];  
$distArray['C'] = $row['Cnum'];  
$distArray['D'] = $row['Dnum'];  
$distArray['Correct'] = $correctAnswer;  
$distArray['Answer'] = rtrim($row[$correctAnswer], ".");  
$distArray['Query'] = "SELECT * FROM TechTerms WHERE Date='$date'";  
return $distArray;  
else {  
    $distArray['Error'] = 'Quiz load query failed';  
    return $distArray;  
}
```



Защита от DDoS атаки

NETERRA

Защо Neterra ?



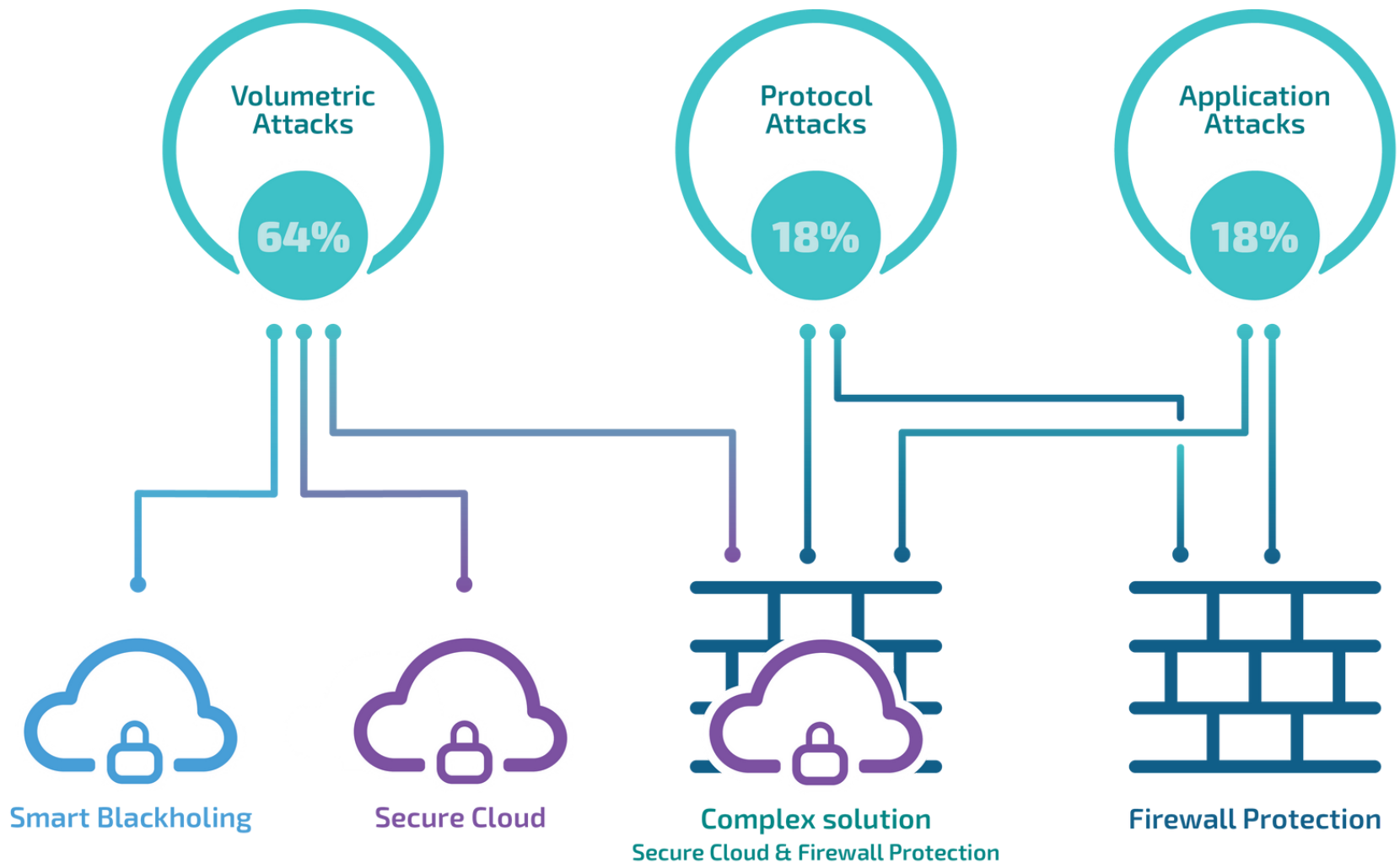
- 200+ точки на присъствие на 6 континента
- 65 града
- 55 държави
- 6 континента
- 10 000+ директно видими ASN
- 30+ свързани IXP-та
- ~50% от всички IPv4 префикси

DDoS атаките влият на вашия бизнес!



- Преки финансови загуби
- Кражба на данни
- Загуба на клиентско доверие
- Спад на продажбите
- Загуба на време и пари за справяне с проблема
- Спад в класирането в търсачките

Видове атаки



Нетера е вашият най-добър избор



- близо 30 опит в предоставянето на надеждни услуги
- Пълен набор от телеком услуги
- Незабавно филтриране на DDoS атаки
- Онлайн портал - DDoS защита
- 24x7 наблюдение и поддръжка
- Известяване при проблем

NETERRA

Клауд решения

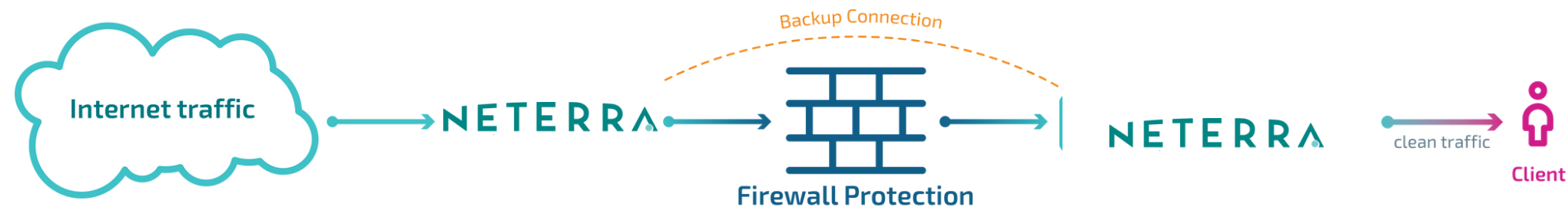
Сигурна клауд защита



- защита от L3-L7 атаки
- защита от атаки с голям капацитет
- Сигурен клауд - местен и международен
- без добавено допълнително RTD

Appliance решение

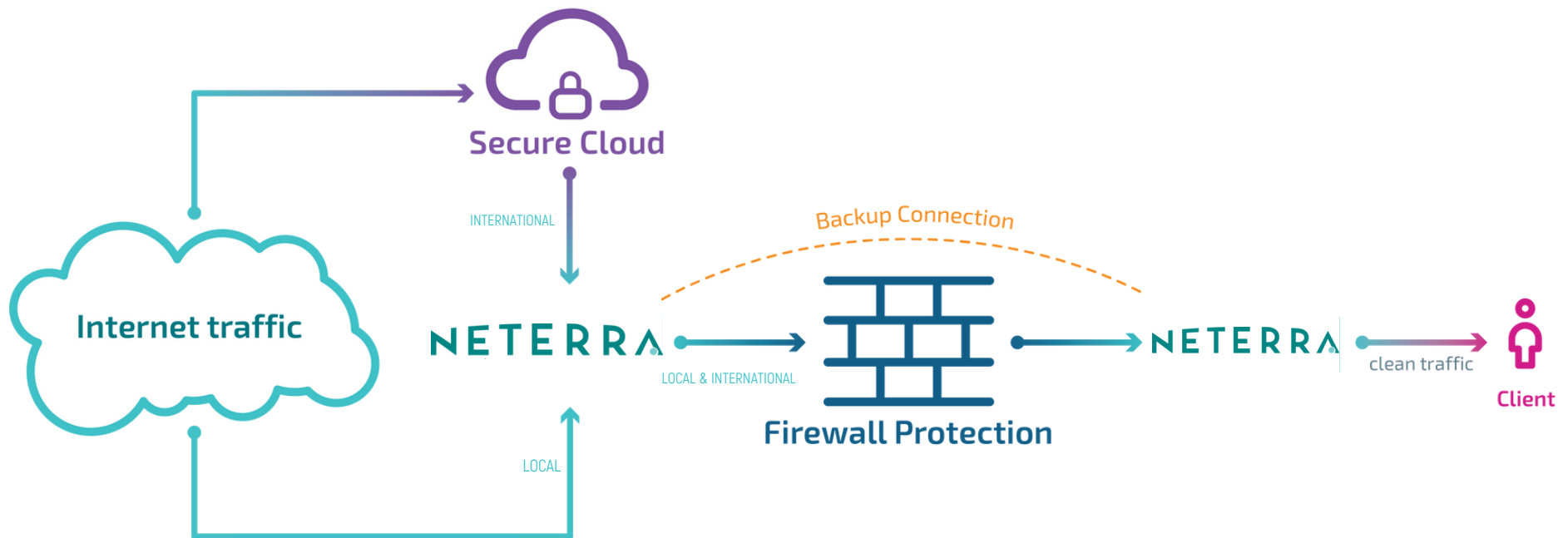
Firewall защита



- защита от L3-L7 атаки
- атаки с малък и голям капацитет
- двойна защитеност на услугите
- без добавяне на RTD

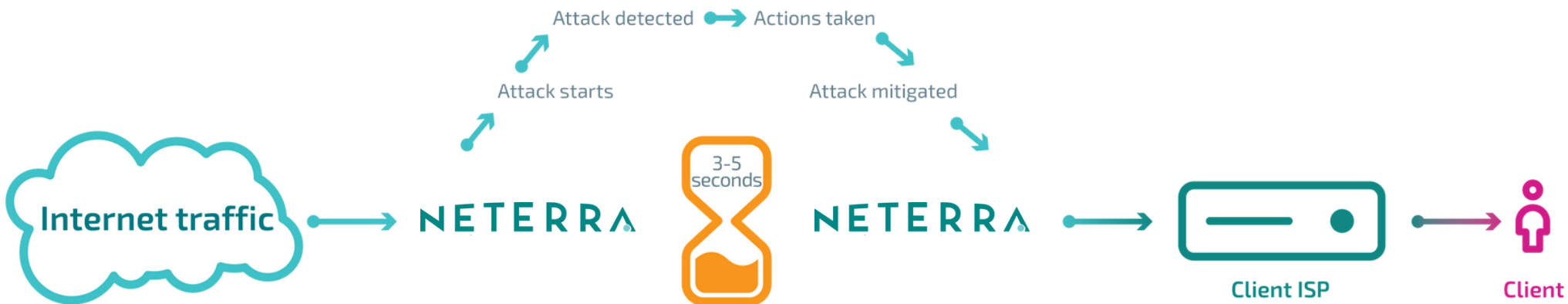
Комбинирано решение

Сигурна Cloud + Firewall защита



- защита от L3-L7 атаки
- двойна защитеност на услугите
- атаки с малък или голям капацитет
- без добавяне на RTD

Neterra Smart Blackholing



- Автоматично откриване и справяне с атаките
- Автоматично възстановяване на услугата
- Клиентски портал (активиране/промяна)
- SMS и имейл известия
- Система за мониторинг и подробна статистика
- 24/7 проактивна професионална поддръжка

Ползи

- Спира всички видове атаки - и близко до източника, и до атакувания
- White label портал за клиенти
- Спира големи атаки (>3Tbps)
- Не внася допълнително времезакъснение
- Възможност за комбиниране с други услуги за защита
- Доказано работещо решение
- 24/7 проактивна експертна поддръжка
- Система за онлайн наблюдение
- SMS и имейл известяване
- Подробен анализ/статистика и история на атаките





Контролен панел

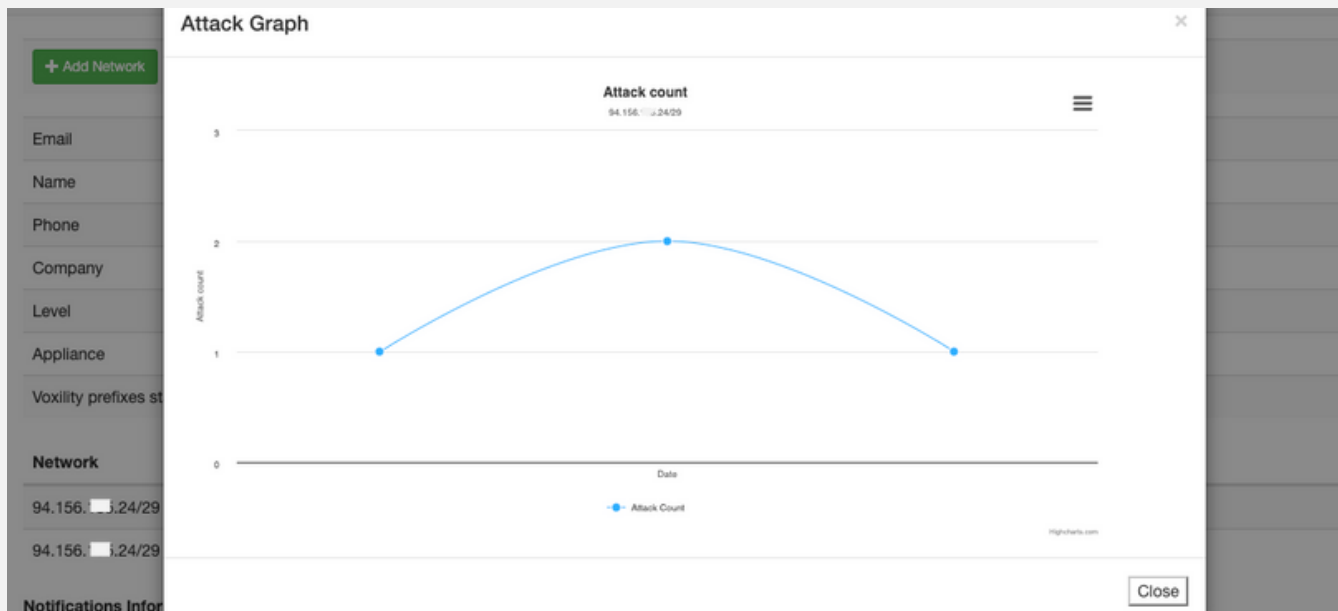
Dashboard Ongoing Users Statistics Settings Info SecureCloud Settings Change log

+ Add Network

Edit Account

Email	ibcybercrime
Name	
Phone	
Company	CyberCrime
Level	User
Appliance	Secure Cloud/Firewall

Network	Delete	Attack Graph	Protection Info
94.156. .24/29			
94.156. .24/29			N/A



- Добавете мрежа за защита
- Задайте правила за всяка мрежа
- SMS и имейл известия за всяка мрежа



Контролен панел

Network : [Q Search](#)

From date : To date : #Secure Cloud Firewall Protection

[Export CSV](#)

IP	Start	Duration	Action	Type
31.13.133	2023-05-23 14:10:31 EEST	00:05:43	Filter ON	Abnormally high rate of UDP incoming packets Info
31.13.138	2023-05-23 14:04:28 EEST	00:05:47	Filter ON	Abnormally high rate of UDP incoming packets Info
193.109.202	2023-05-23 14:03:30 EEST	00:05:44	Filter ON	Abnormally high rate of UDP incoming packets Info
91.92.255	2023-05-23 14:00:51 EEST	00:10:23	Filter ON	Abnormally high rate of UDP incoming packets Info
193.109.201	2023-05-23 13:59:39 EEST	00:05:36	Filter C	
31.13.138	2023-05-23 13:50:00 EEST	00:05:15	Filter C	
31.13.141	2023-05-23 13:49:27 EEST	00:05:48	Filter C	
91.92.255	2023-05-23 13:49:25 EEST	00:05:50	Filter a	
31.13.134	2023-05-23 13:45:45 EEST	00:05:29	Filter C	
95.43.4	2023-05-23 13:43:33 EEST	00:05:41	Filter C	
193.109.200	2023-05-23 13:36:45 EEST	00:05:30	Filter C	
87.121.145	2023-05-23 13:36:44 EEST	00:06:31	Filter C	
31.13.138	2023-05-23 13:33:07 EEST	00:05:08	Filter C	
87.121.145	2023-05-23 13:29:16 EEST	00:05:58	Filter C	
31.13.15	2023-05-23 13:25:43 EEST	00:05:32	Filter C	
87.121.145	2023-05-23 13:14:25 EEST	00:43:49	Filter C	
87.121.145	2023-05-23 13:09:29 EEST	00:05:45	Filter C	
193.109.200	2023-05-23 13:07:11 EEST	00:05:04	Filter C	
31.13.141	2023-05-23 13:02:39 EEST	00:05:35	Filter C	
87.121.145	2023-05-23 12:58:48 EEST	00:15:27	Filter C	
87.121.145	2023-05-23 12:53:47 EEST	00:05:27	Filter C	

Network : [Q Search](#)

From date : To date :

[Export CSV](#)

IP

- 31.13.133
- 31.13.138
- 193.109.202
- 91.92.255
- 193.109.201
- 31.13.138
- 31.13.141
- 91.92.255
- 31.13.134
- 95.43.4
- 193.109.200
- 87.121.145
- 31.13.138
- 87.121.145
- 31.13.15
- 87.121.145
- 87.121.145
- 193.109.200

Cloud Attack Info [X](#)

Src IP	Dst IP	Dst Port	Proto	Len IP	Timestamp
173.194. .70	31.13. .133	58381	17	217	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info, 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info, 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info, 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info, 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30
173.194. .70	31.13. info 133	58381	17	1278	2023-05-23 11:10:30

- Подробна статистика на атаки


```
require 'spec_helper'
require 'rspec/rails'

require 'capybara/rspec'
require 'capybara/rails'

Capybara.javascript_driver = :selenium_chrome_headless
Category.delete_all;
Shoulda::Matchers.configure do |config|
  config.integrate_with_test_framework = :rspec
end
end


# Add additional matchers here
# Requires support for :rspec
# spec/support/shoulda_matchers.rb
# run as spec_helper
# in _spec_helper.rb
# run twice
# end with
# option

No results found for 'm'
```



neterra.net 

CONTACT@NETERRA.NET 

+359 2 975 16 16 

 Neterra

 Neterra

NETERRA
telecommunications

