Network layer attacks

- List of endpoints
  - Timeseries
    - Example: hourly percentage breakdown by attack method
  - Summary
    - Example: Russia - overall percentage breakdown by network protocol
- Next steps

Network layer attacks show DDoS attack trends at the network layer. These attacks can be split by the network protocol they use: ICMP, TCP, UDP and others.

:::note

Unlike what happens in Application Layer Attacks, in network layer attacks location attribution does not use the location associated with the client's IP address. Instead, it uses the location of the data center itself. This is due to IP spoofing. :::

When filtering by location or autonomous system (AS), we are filtering by the source location/AS of the attack — which can be very different to the location of the human orchestrator of the attack. Refer to botnets for more information.

List of endpoints

Timeseries

Example: hourly percentage breakdown by attack method

In the following example, we will examine the worldwide versus Singapore distribution of mitigated attacks by network protocol:

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer3/timeseries_groups?name=global&dateR
ange=1d&location=&name=singapore&location=SG&dateRange=1d&aggInterval=1h&format=json" \
--header "Authorization: Bearer <API_TOKEN>"
```

If we inspect the abbreviated response below, we can conclude that globally, at those timestamps, `UDP` and `TCP` attacks were mostly evenly split.


```
{
  "success": true,
  "errors": [],
  "result": {
    "global": {
      "timestamps": ["2022-11-06T13:00:00Z", "2022-11-06T14:00:00Z", "..."],
      "udp": ["50.784034", "51.055221", "..."],
      "tcp": ["49.213944", "48.943769", "..."],
      "icmp": ["0.002023", "0.001009", "..."],
      "gre": ["0.0", "0.0", "0.0", "..."]
    },
    "singapore": {
      "timestamps": ["2022-11-06T13:00:00Z", "2022-11-06T14:00:00Z", "..."],
      "tcp": ["79.605287", "83.943885", "..."],
      "udp": ["20.394594", "16.056115", "..."],
      "icmp": ["0.000119", "0.0", "..."],
      "gre": ["0.0", "0.0", "..."]
    },
    "meta": {
      "dateRange": {
        "startTime": "2022-11-06T13:00:00Z",
        "endTime": "2022-11-07T13:00:00Z"
      },
      "normalization": "PERCENTAGE",
□□□// ...
    }
  }
}
```


We can also conclude that the distribution of network layer attacks coming from Singapore — or, more accurately, reaching Cloudflare's data center located in Singapore — differs quite a bit from the worldwide distribution. At those times, the distribution of network layer attacks clearly favors

TCP.

For more information refer to the API reference for this endpoint.

Summary

Example: Russia - overall percentage breakdown by network protocol

We can also filter by source location and examine attacks coming from Russia:

```
curl
"https://api.cloudflare.com/client/v4/radar/attacks/layer3/summary?location=RU&name=attacks_ru
&dateRange=1d&format=json" \
--header "Authorization: Bearer <API_TOKEN>"
```


```
{
  "success": true,
  "errors": [],
  "result": {
    "attacks_ru": {
      "udp": "86.682356",
      "tcp": "11.928664",
      "gre": "1.381015",
      "icmp": "0.007965"
    },
    "meta": {
      "dateRange": {
        "startTime": "2022-11-06T15:00:00Z",
        "endTime": "2022-11-07T15:00:00Z"
      },
      "normalization": "PERCENTAGE",
□□□// ...
    }
  }
}
```


The response shows that the attacks coming from Russia to other locations tended to use the UDP network protocol at those timestamps.

For more information refer to the API reference for this endpoint.

Next steps

Refer to DNS to learn more about the aggregated and anonymized DNS queries to Cloudflare's 1.1.1.1 public resolver service.

□□□ #2
□ □□□ □□□ 2026-11-01 03:12:22 UTC
□ □□□ □□□ 2026-11-01 03:12:24 UTC