Flow Enrichment How to

View latest version

How do I enrich flow data with…

Tip: Any configuration keys that begin with “EF” are configured in /etc/elastiflow/flowcoll.yml or docker compose yml.

Tip: Whenever adding or modifying enrichment features or data elements, it’s best to restart the ElastiFlow flow collector / flowcoll service. Optionally, you can just wait for the refresh timeouts to expire.

NetIntel App Identification

NetIntel App identification identifies SaaS applications using ElastiFlow's own database.

Instructions:

—

Any keys that begin with "EF_" are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

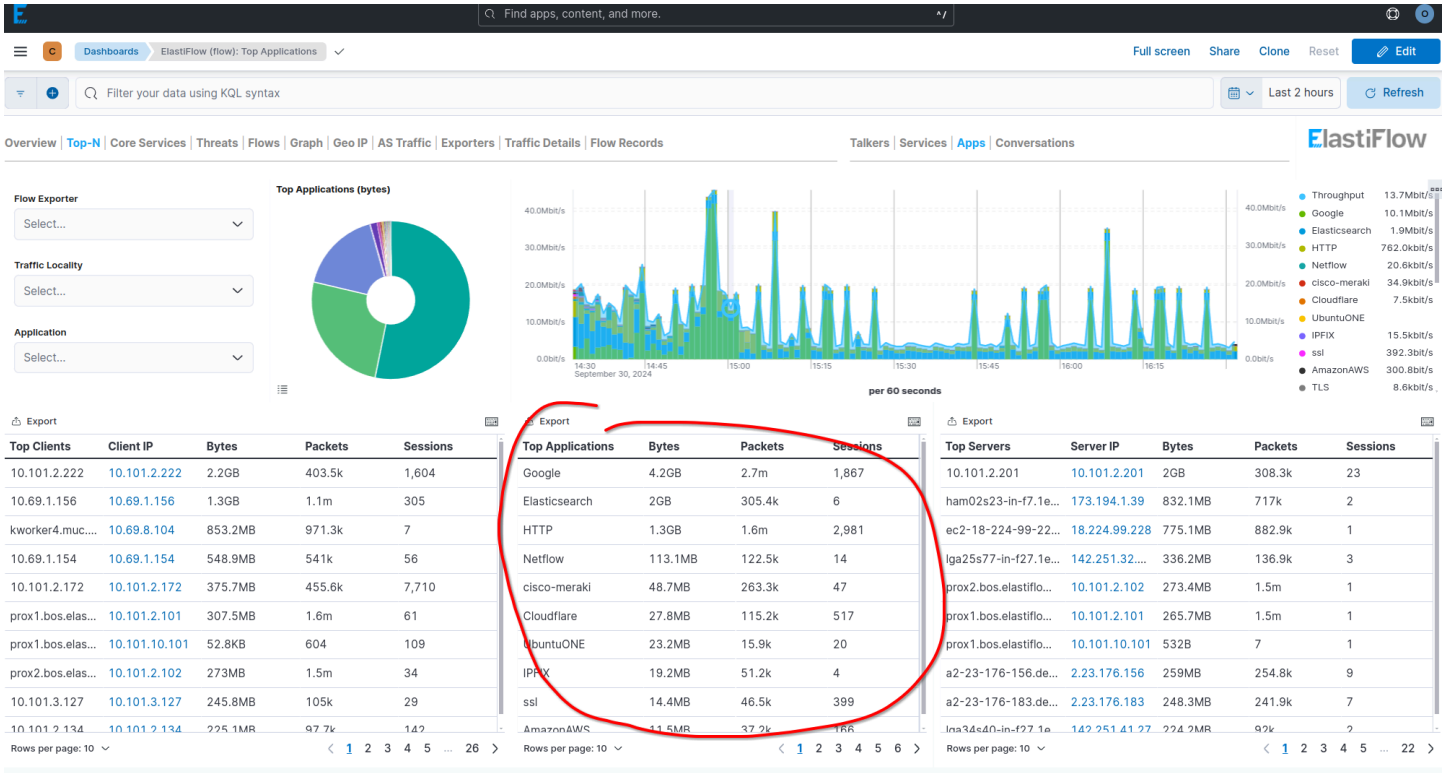
1. Ensure you have a Community Edition or higher account ID and ElastiFlow flow license key
2. Add your account ID and license key to your `/etc/elastiflow/flowcoll.yml` or docker compose yml.

```
EF_LICENSE_ACCEPTED: 'true'
EF_ACCOUNT_ID: '234sfdaq43'
EF_FLOW_LICENSE_KEY: 'fj58fjs03d9gh68'
```

3. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:
   Note: NetIntel is enabled by default.

```
EF_PROCESSOR_ENRICH_IPADDR_NETINTEL_ENABLE: 'true'
```

ElastiFlow



NetIntel Threat Detection

NetIntel Threat Detection can add threat information to any flow records containing IP addresses that NetIntel cloud service has detected as being malicious.

Instructions:

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

—

1. Ensure you have a Community Edition or higher account ID and ElastiFlow flow license key
2. Add your account ID and license key to your `/etc/elastiflow/flowcoll.yml` or docker compose yml.

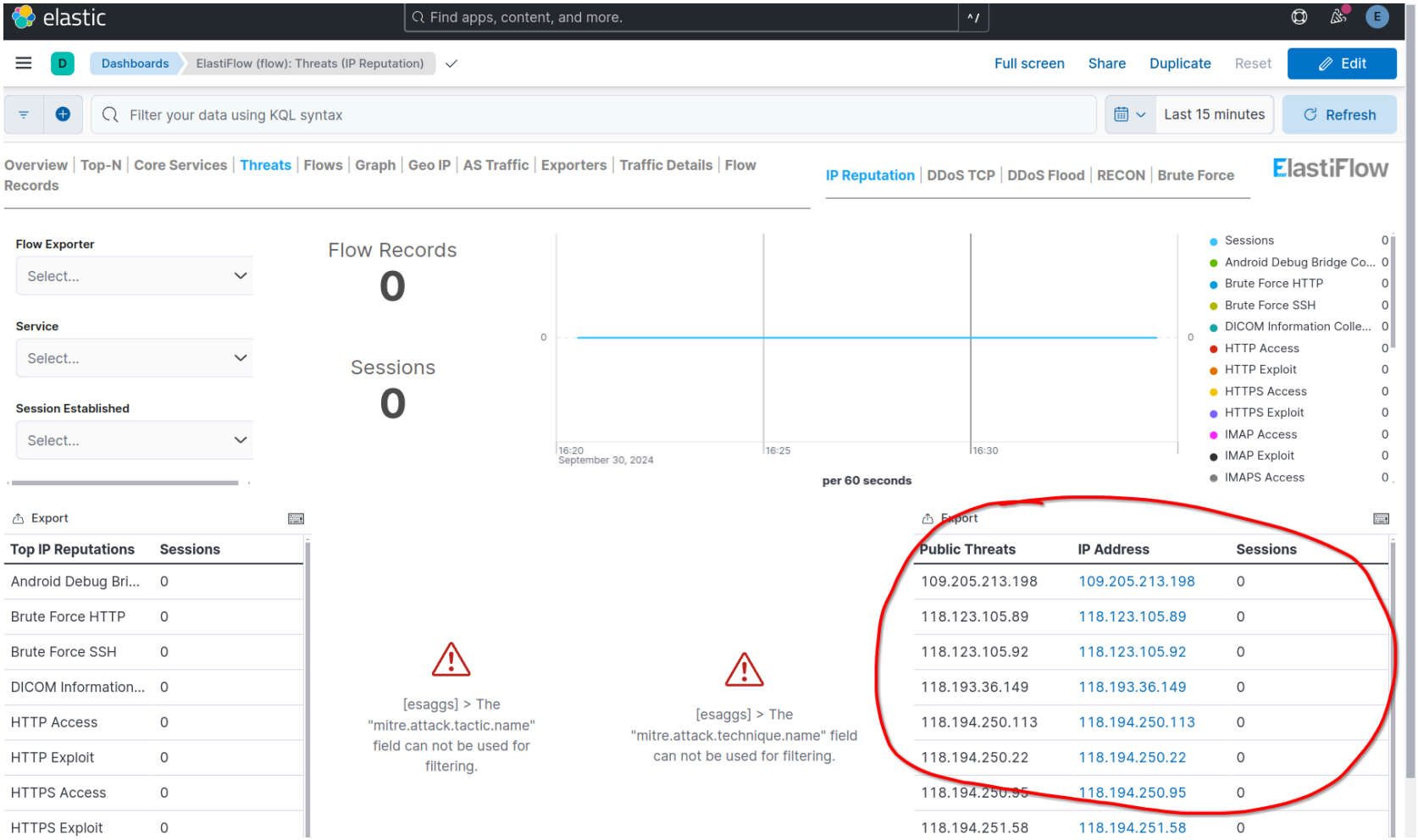
```
EF_LICENSE_ACCEPTED: 'true'
EF_ACCOUNT_ID: '234sfdaq43'
```

ElastiFlow

```
EF_FLOW_LICENSE_KEY: 'sdfadfadfasdfsdf'
```

3. Ensure that the following key / value pair is present. Note: NetIntel is enabled by default.

```
EF_PROCESSOR_ENRICH_IPADDR_NETINTEL_ENABLE: 'true'
```



NetIntel Threat Detection with Mitre Mapping + Scoring

Instructions:

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

—

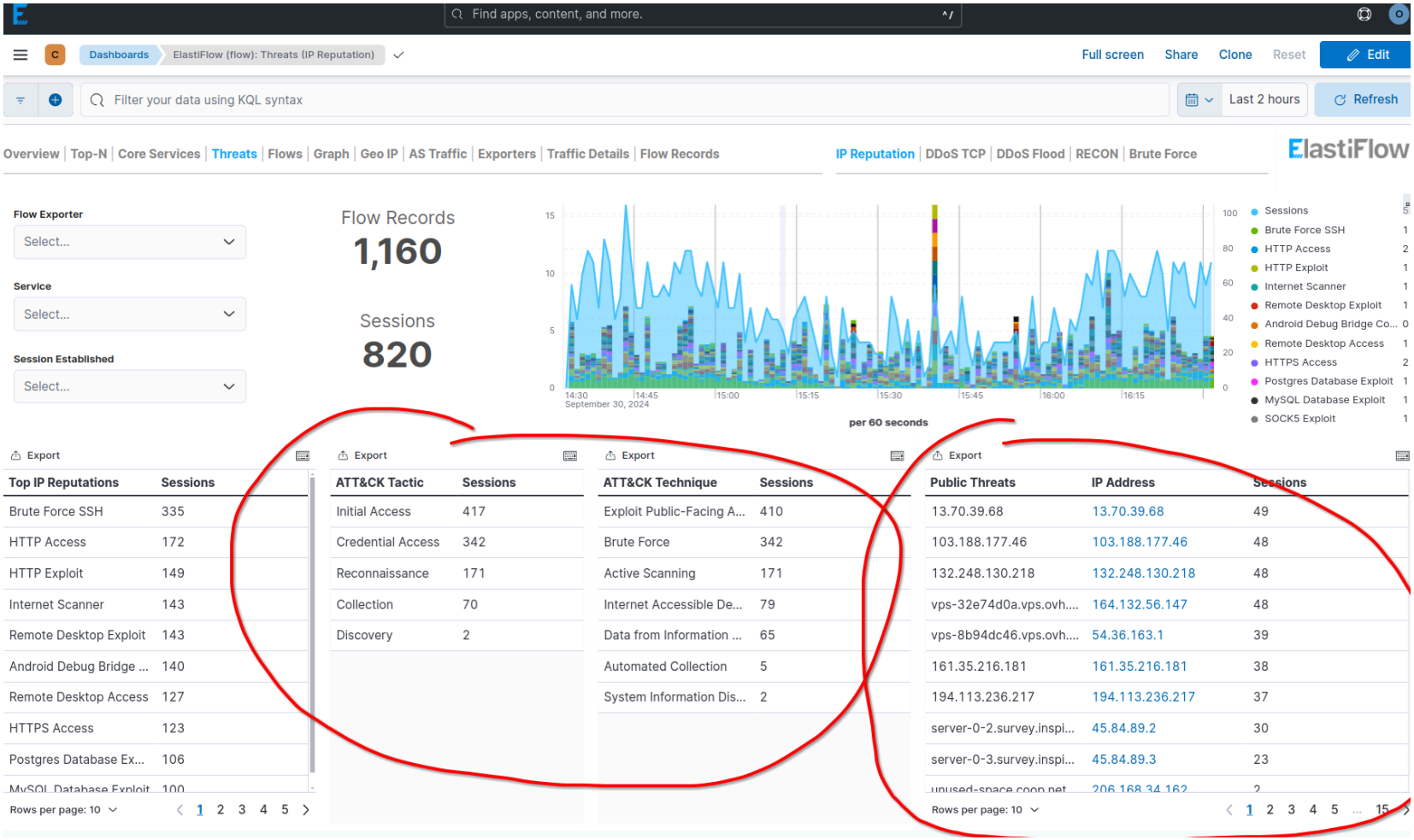
1. Ensure you have a Premium license account ID and ElastiFlow flow license key
2. Add your account ID and license key to your `/etc/elastiflow/flowcoll.yml` or docker compose yml.

```
EF_LICENSE_ACCEPTED: 'true'
EF_ACCOUNT_ID: '234sfdaq43'
EF_FLOW_LICENSE_KEY: 'sdfadfadfasdfsdf’
```

3. Ensure that the following key / value pair is present. Note: NetIntel is enabled by default.

```
EF_PROCESSOR_ENRICH_IPADDR_NETINTEL_ENABLE: 'true'
```

ElastiFlow


Find apps, content, and more.
Dashboards
ElastiFlow (flow): Threats (IP Reputation)
Full screen
Share
Clone
Reset
Edit
Filter your data using KQL syntax
Last 2 hours
Refresh
Overview | Top-N | Core Services | Threats | Flows | Graph | Geo IP | AS Traffic | Exporters | Traffic Details | Flow Records
IP Reputation | DDoS TCP | DDoS Flood | RECON | Brute Force
ElastiFlow
Flow Exporter
Select...
Service
Select...
Session Established
Select...
Flow Records
1,160
Sessions
820
14:30
September 30, 2024
14:45
15:00
15:15
15:30
15:45
16:00
16:15
per 60 seconds
Sessions
Brute Force SSH 1
HTTP Access 2
HTTP Exploit 1
Internet Scanner 1
Remote Desktop Exploit 1
Android Debug Bridge Co... 0
Remote Desktop Access 1
HTTPS Access 2
Postgres Database Exploit 1
MySQL Database Exploit 1
SOCK5 Exploit 1
Export
Top IP Reputations | Sessions
Brute Force SSH 335
HTTP Access 172
HTTP Exploit 149
Internet Scanner 143
Remote Desktop Exploit 143
Android Debug Bridge ... 140
Remote Desktop Access 127
HTTPS Access 123
Postgres Database Ex... 106
Rows per page: 10
1 2 3 4 5
Export
ATT&CK Tactic | Sessions
Initial Access 417
Credential Access 342
Reconnaissance 171
Collection 70
Discovery 2
Export
ATT&CK Technique | Sessions
Exploit Public-Facing A... 410
Brute Force 342
Active Scanning 171
Internet Accessible De... 79
Data from Information ... 65
Automated Collection 5
System Information Dis... 2
Export
Public Threats | IP Address | Sessions
13.70.39.68 | 13.70.39.68 | 49
103.188.177.46 | 103.188.177.46 | 48
132.248.130.218 | 132.248.130.218 | 48
vps-32e74d0a.vps.ovh.... | 164.132.56.147 | 48
vps-8b94dc46.vps.ovh.... | 54.36.163.1 | 39
161.35.216.181 | 161.35.216.181 | 38
194.113.236.217 | 194.113.236.217 | 37
server-0-2.survey.inspi... | 45.84.89.2 | 30
server-0-3.survey.inspi... | 45.84.89.3 | 23
Rows per page: 10
1 2 3 4 5 ... 15

ElastiFlow

Hostnames

This section describes how you can enable the enrichment of flow records with the hostnames of IP addresses in the flow records.

Instructions:

—

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

- Enable hostname enrichment
  - `EF_PROCESSOR_ENRICH_IPADDR_DNS_ENABLE: "true"`
- Specify a DNS server for DNS lookups
  - `EF_PROCESSOR_ENRICH_IPADDR_DNS_NAMESERVER_IP`
- Set DNS server timeouts
  - `EF_PROCESSOR_ENRICH_IPADDR_DNS_NAMESERVER_TIMEOUT`
- Exclude / include IPs from DNS lookups
  - "`EF_PROCESSOR_ENRICH_IPADDR_DNS_INCLEXCL_PATH`: '/etc/elastiflow/hostname/incl_excl.yml'
  - Change refresh rate for include / exclude definition file
    `EF_PROCESSOR_ENRICH_IPADDR_DNS_INCLEXCL_REFRESH_RATE`
- Specify your own IP-to-DNS hostname mappings
  - `"EF_PROCESSOR_ENRICH_IPADDR_DNS_USERDEF_PATH: '/etc/elastiflow/hostname/user_defined.yml`
  - Change refresh rate
    `EF_PROCESSOR_ENRICH_IPADDR_DNS_USERDEF_REFRESH_RATE`
- Enable / disable resolving public / private IP spaces
  - `EF_PROCESSOR_ENRICH_IPADDR_DNS_RESOLVE_PRIVATE`
  - `EF_PROCESSOR_ENRICH_IPADDR_DNS_RESOLVE_PUBLIC`

AS Name, ASNs, and Geolocation

Enrich flow records with with AS name, ASNs, and geolocations

Instructions:

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.
—

1. Create a free account here: https://www.maxmind.com/en/geolite2/signup
2. Download Maxmind Geolite databases to your ElastiFlow host:
   `/etc/elastiflow/maxmind/GeoLite2-ASN.mmdb`
   `/etc/elastiflow/maxmind/GeoLite2-City.mmdb`

   Tip: You easily download and copy the database files you can use the following command snippets on your ElastiFlow server. Be sure to replace “YOUR_MAXMIND_LICENSE_KEY” with your MaxMind license key.

Unset

```
sudo wget -O ./GeoLite2-ASN.tar.gz
"https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-ASN&license_key=YOUR_MAXMIND_LICENSE_KEY
&suffix=tar.gz"
sudo wget -O ./GeoLite2-City.tar.gz
"https://download.maxmind.com/app/geoip_download?edition_id=GeoLite2-City&license_key=YOUR_MAXMIND_LICENSE_KE
Y&suffix=tar.gz"
sudo tar -xvzf GeoLite2-ASN.tar.gz --strip-components 1 -C /etc/elastiflow/maxmind/
sudo tar -xvzf GeoLite2-City.tar.gz  --strip-components 1 -C /etc/elastiflow/maxmind/
```

3. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:
   `EF_PROCESSOR_ENRICH_IPADDR_MAXMIND_ASN_ENABLE: “true”`
   `EF_PROCESSOR_ENRICH_IPADDR_MAXMIND_GEOIP_ENABLE: ”true”`

Flow Exporter

Select...

Client

Select...

Server

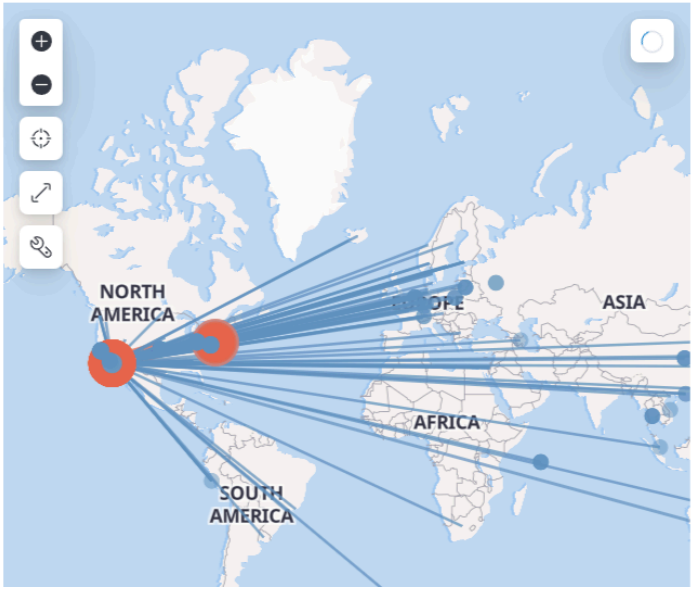
Select...

Client Countries (flow recor...

- United States
- China
- Germany
- Lithuania
- Russia
- Seychelles
- Thailand
- The Netherl...

Client Cities (flow records)

- San Marcos
- Wilmington
- San Jose
- Ashburn
- Columbus
- Amsterdam
- Bangkok
- Vilnius



Server Countries (flow reco...

- United States
- The Netherl...
- Sweden
- Germany
- United King...
- Australia
- Hong Kong
- Brazil

Server Cities (flow records)

- Los Angeles
- Ashburn
- Boardman
- Kansas City
- Santa Clara
- El Segundo
- San Francis...
- San Marcos

Flow Exporter

Select...

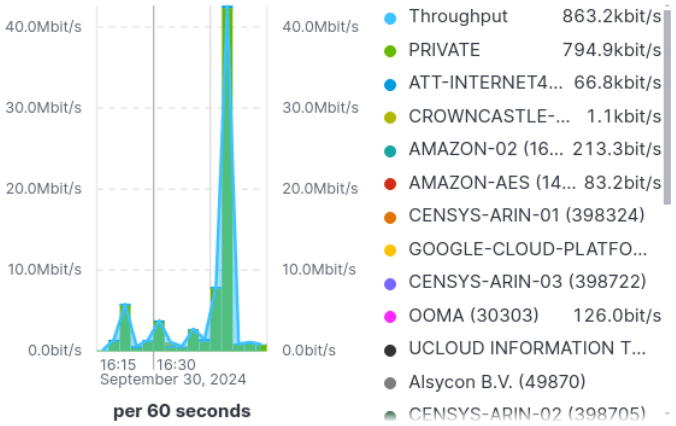
Client AS

Select...

Server AS

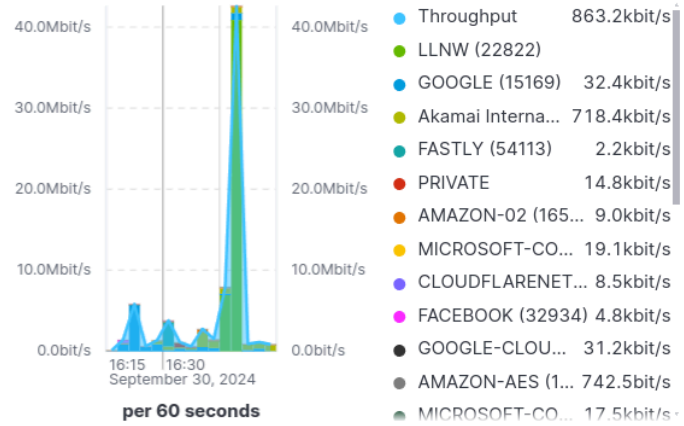
Select...

Client AS (bits/s)



- Throughput 863.2kbit/s
- PRIVATE 794.9kbit/s
- ATT-INTERNET4... 66.8kbit/s
- CROWNCASTLE-... 1.1kbit/s
- AMAZON-02 (16... 213.3bit/s
- AMAZON-AES (14... 83.2bit/s
- CENSYS-ARIN-01 (398324)
- GOOGLE-CLOUD-PLATFO...
- CENSYS-ARIN-03 (398722)
- OOMA (30303) 126.0bit/s
- UCLOUD INFORMATION T...
- Alsycon B.V. (49870)
- CENSYS-ARIN-02 (398705)

Server AS (bits/s)



- Throughput 863.2kbit/s
- LLNW (22822)
- GOOGLE (15169) 32.4kbit/s
- Akamai Interna... 718.4kbit/s
- FASTLY (54113) 2.2kbit/s
- PRIVATE 14.8kbit/s
- AMAZON-02 (165... 9.0kbit/s
- MICROSOFT-CO... 19.1kbit/s
- CLOUDFLARENET... 8.5kbit/s
- FACEBOOK (32934) 4.8kbit/s
- GOOGLE-CLOU... 31.2kbit/s
- AMAZON-AES (1... 742.5bit/s
- MICROSOFT-CO... 17.5kbit/s

ElastiFlow

Enrich private / RFC1918 IP space with geolocation

Instructions:

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

—

1. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:

   ```
   EF_PROCESSOR_ENRICH_IPADDR_METADATA_ENABLE: “true”
   EF_PROCESSOR_ENRICH_IPADDR_METADATA_USERDEF_PATH: “/etc/elastiflow/metadata/ipaddrs.yml"
   ```

2. Edit `/etc/elastiflow/metadata/ipaddrs.yml`, adding the enrichment information you’d like to add to flow records.

   Example `ipaddrs.yml` content:

   ```
   192.168.0.0/16:
     metadata:
       .geo.loc.coord: 48.167106,11.486918
       .geo.city.name: Munich
       .geo.country.code: DE
       .geo.country.name: Germany
       .geo.tz.name: Europe/Berlin
   ```

Application Identities

Note: ElastiFlow fully supports application identification arriving in flow records from your infrastructure.

NetIntel AppID

Please see this.

Define custom applications and servers

Instructions:

—

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

1. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:
   ```
   EF_PROCESSOR_ENRICH_APP_IPPORT_ENABLE: "true"
   EF_PROCESSOR_ENRICH_APP_IPPORT_PATH" "EF_PROCESSOR_ENRICH_APP_IPPORT_PATH:
   '/etc/elastiflow/app/ipport.yml'
   ```
2. Edit `/etc/elastiflow/app/ipport.yml`, adding the enrichment information you’d like to add to flow records.

Enable app identifications that arrive in option records

This is required for devices from the following vendors that are sending app IDs: Cisco, Fortinet, Velocloud, Versa, and Viptela

Instructions:

—

Any keys that begin with “EF_” are configured in /etc/elastiflow/flowcoll.yml or docker compose yml.

1. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:
   ```
   EF_PROCESSOR_ENRICH_APP_ID_ENABLE: "true"
   EF_PROCESSOR_ENRICH_APP_ID_PATH" "EF_PROCESSOR_ENRICH_APP_ID_PATH:
   '/etc/elastiflow/app/appid.yml'
   ```

2. Edit `/etc/elastiflow/app/appid.yml`, adding the IPs and corresponding vendors of your devices.

User-defined Metadata

You can add virtually any kind of textual data to your flow records easily.

Instructions:

—

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

1. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:
   ```
   EF_PROCESSOR_ENRICH_IPADDR_METADATA_ENABLE: "true"
   EF_PROCESSOR_ENRICH_IPADDR_METADATA_USERDEF_PATH: '/etc/elastiflow/metadata/ipaddrs.yml'
   ```
2. Add your enrichment information to `/etc/elastiflow/metadata/ipaddrs.yml`.

Network interface Names

Add metadata to network interfaces.

Instructions:

—

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

1. Ensure that the following key / value pairs are present in `/etc/elastiflow/flowcoll.yml` or docker compose yml:

```
EF_PROCESSOR_ENRICH_NETIF_METADATA_ENABLE: "true"
EF_PROCESSOR_ENRICH_NETIF_METADATA_USERDEF_PATH: '/etc/elastiflow/metadata/netifs.yml'
```

2. Add your enrichment information to `/etc/elastiflow/metadata/netifs.yml`.

Network Interface Names and Descriptions from SNMP

Enrich flow records with proper interface names by polling SNMP

Instructions:

—

Any keys that begin with “EF_” are configured in `/etc/elastiflow/flowcoll.yml` or docker compose yml.

Option 1: If you have one SNMP configuration for all your devices sending flow data to ElastiFlow, configure the following key / value pairs where appropriate:

```
EF_PROCESSOR_ENRICH_NETIF_SNMP_COMMUNITIES: public
EF_PROCESSOR_ENRICH_NETIF_SNMP_ENABLE: "false"
EF_PROCESSOR_ENRICH_NETIF_SNMP_PORT: 161
EF_PROCESSOR_ENRICH_NETIF_SNMP_RETRIES: 1
EF_PROCESSOR_ENRICH_NETIF_SNMP_TIMEOUT: 2
EF_PROCESSOR_ENRICH_NETIF_SNMP_V3_AUTHENTICATION_PASSPHRASE: ""
EF_PROCESSOR_ENRICH_NETIF_SNMP_V3_AUTHENTICATION_PROTOCOL: noauth
EF_PROCESSOR_ENRICH_NETIF_SNMP_V3_PRIVACY_PASSPHRASE: ""
EF_PROCESSOR_ENRICH_NETIF_SNMP_V3_PRIVACY_PROTOCOL: nopriv
EF_PROCESSOR_ENRICH_NETIF_SNMP_V3_USERNAME: ""
EF_PROCESSOR_ENRICH_NETIF_SNMP_VERSION: 2
```

Option 2: If you have different SNMP configurations for each of your devices sending flow data to ElastiFlow, configure the following key / value pairs where appropriate:

```
EF_PROCESSOR_ENRICH_NETIF_SNMP_ACCESS_ENABLE: "true"
EF_PROCESSOR_ENRICH_NETIF_SNMP_ACCESS_PATH: /etc/elastiflow/settings/snmp_access.yml
EF_PROCESSOR_ENRICH_NETIF_SNMP_ACCESS_REFRESH_RATE: 15
```