Cisco Telemetry Broker

Agenda

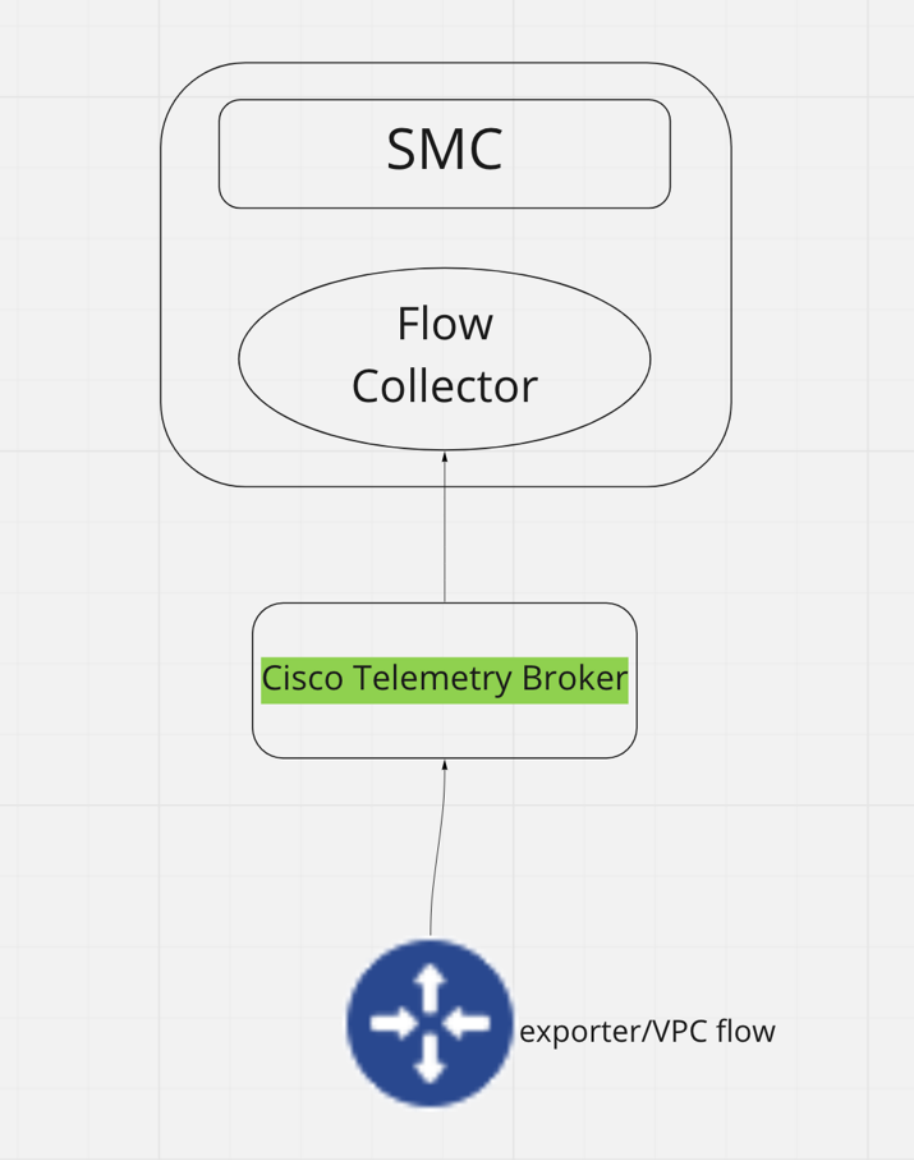
- Introduction
- Installation
- Demo
- Cloud VPC Logs in CTB

Cisco Telemetry Broker allows you to ingest network telemetry from many sources, transform the data format, and forward that telemetry to one or multiple destinations.

- On-premises network telemetry, including NetFlow, syslog, and IPFIX
- Cloud-based telemetry sources, such as AWS VPC Flow Logs

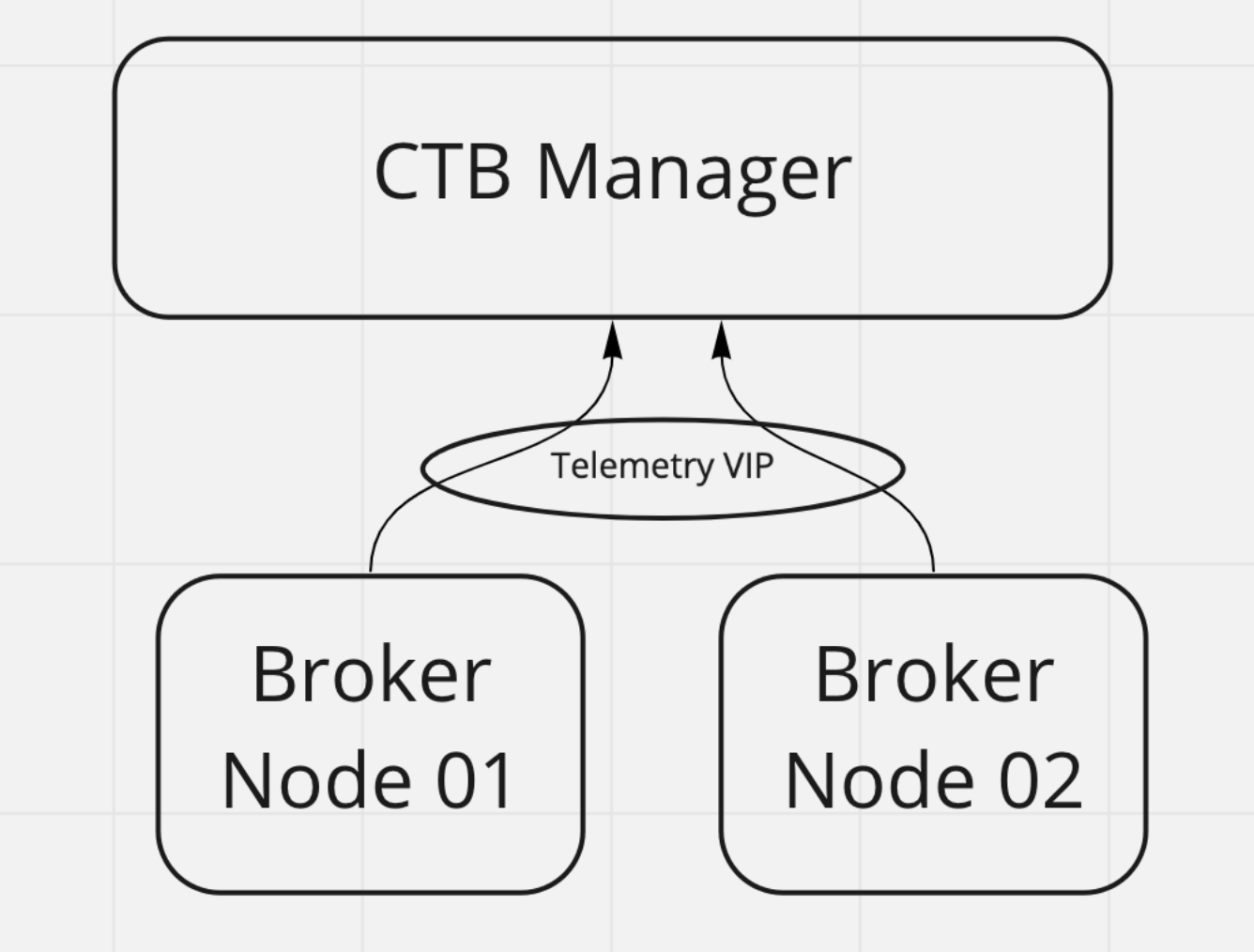
Ingested Data Format	Forwarded Data Format
Netflow	Netflow
VPC Flow Logs	IPFIX
NSG Flow Logs	IPFIX

Solution High level overview



CTB Architecture

Consists of CTB manager and Brokers. Your broker nodes are all managed by one Cisco Telemetry Broker manager. You can log in to this manager's web interface and perform various configuration tasks, including managing the broker nodes, setting up the forwarding rules, creating users, and reviewing the dashboard for usage.



Pre-Requisite

Networks

Management Network: Every node (manager or broker) in your deployment must have one IPv4 network interface connected to the Management Network to provide for administration over SSH and HTTPS (if the node is running the management functions).

Telemetry Network: The broker node must have a second interface (IPv4 or IPv6) that must be connected to the Telemetry Network. On this network the node will receive telemetry from sources and forward it to destinations.

The Management Network and the Telemetry Network can be the same network.

Management Network	Telemetry Network
IPv4 address	IPv4 address

IPv4 mask	IPv4 mask
IPv4 default gateway	IPv4 default gateway
IPv4 DNS nameserver	IPv4 default gateway
NA	IPv6 Network

Hardware Config

Configuration	Manager	Broker
CPU	4	1 Gbit/s: 2 10 Gbit/s: 5 Transformation Capable: 8
Memory	8GB	1 GBit/s: 4GB 10 GBit/s: 8GB
Storage	80GB	70 GB

CTB MANAGER Installation from OVA

You deploy these broker nodes and manager as virtual appliances to a hypervisor.

Steps:

1. Download Manager node OVA from software.cisco.com
2. Deploy ova from VMWare vsphere using ova.
3. Once deployed power ON the VM
4. From VM web console, login with username – "install" no password required.
5. Run "sudo ctb-install" and follow the prompt to set up admin password and Network as capture above.
6. After applying network config, browse to **Error! Hyperlink reference not valid.**>
7. You will land to fist time setup page, create a web UI user(different than admin) and set the password.

CTB BROKER Installation from OVA

You deploy these broker nodes and manager as virtual appliances to a hypervisor.

Steps:

1. Download Manager node OVA from software.cisco.com

2. Deploy ova from VMWare vsphere using ova.
3. Once deployed power ON the VM
4. From VM web console, login with username – "install" no password required.
5. Run "sudo ctb-install" and follow the prompt to set up admin password and Network as capture above.

After applying network setting connect broker with Manager. To do so –

1. Run "sudo ctb-manage" command
2. Enter ip address of manager node and authenticate with username/password. Use CTB manager admin username and password.
3. Now CTB broker added to CTB manager.

Instance	CLI	UI
Manager	Admin/password	Webadmin/password
Broker	Admin/password	NA

CTB Manager UI walkthrough: Demo

1. Sources
2. Destination
3. Broker Node
4. Licensing
5. VPC flow log
6. Broker HA

CTB Part - II

CTB Manager VPC flow log Integration

The Cisco Telemetry Broker Integrations shows information about your VPC Flow Logs. You can configure your AWS deployment to export Virtual Private Cloud (VPC) Flow Logs to Cisco Telemetry Broker, then configure Cisco Telemetry Broker to transform the VPC Flow Logs to IPFIX for ingestion by destinations.

AWS side of work (Part - I)

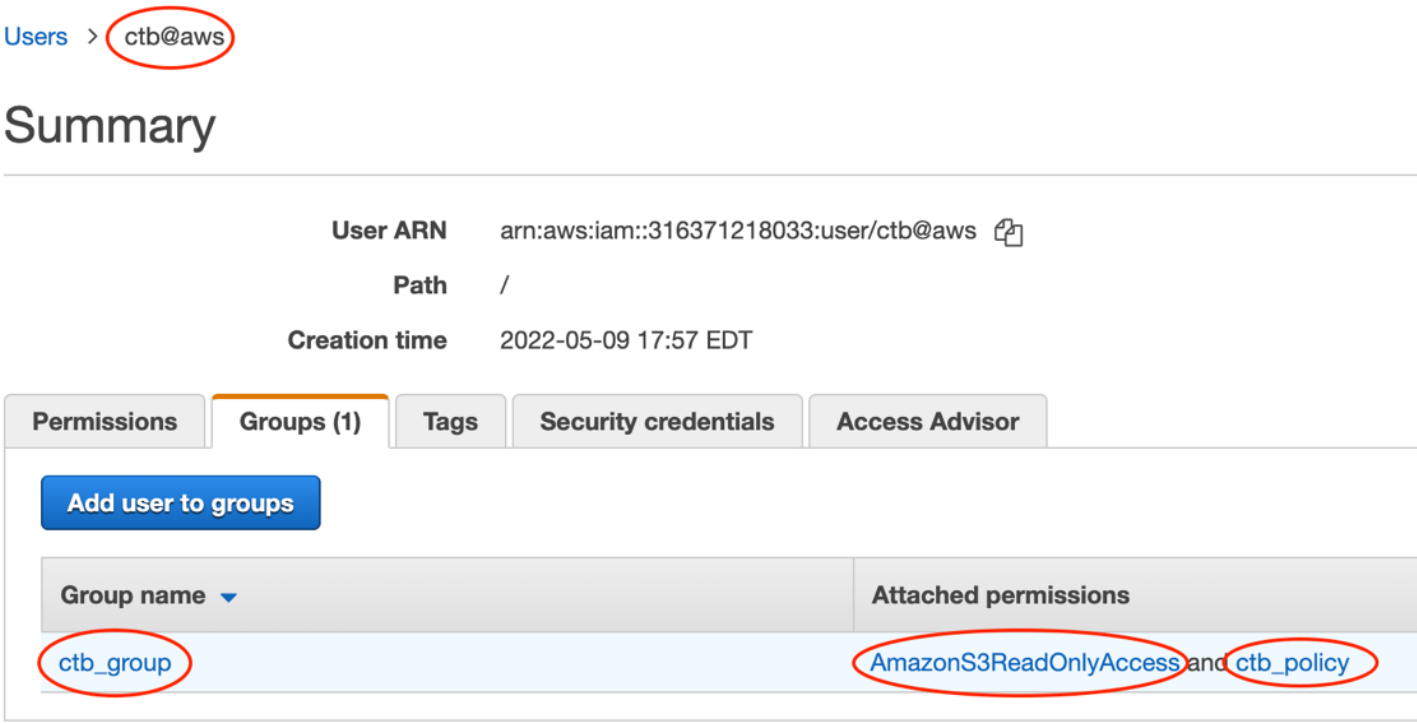
1. Create flow log for VPC and send it to a S3 bucket
2. Create IAM user and download access key and secret. This will be uploaded to CTB.

CTB side of work (Part - I)

1. Upload AWS user credential in CTB. Integration > Add AWS credentials.
2. In CTB source > vpc flow log > add flow
3. Enter S3 bucket path, your AWS region and saved creds.
4. Expand Policy to use and copy the json file, this permission should be attached to AWS CTB user.

AWS side of work (Part - II)

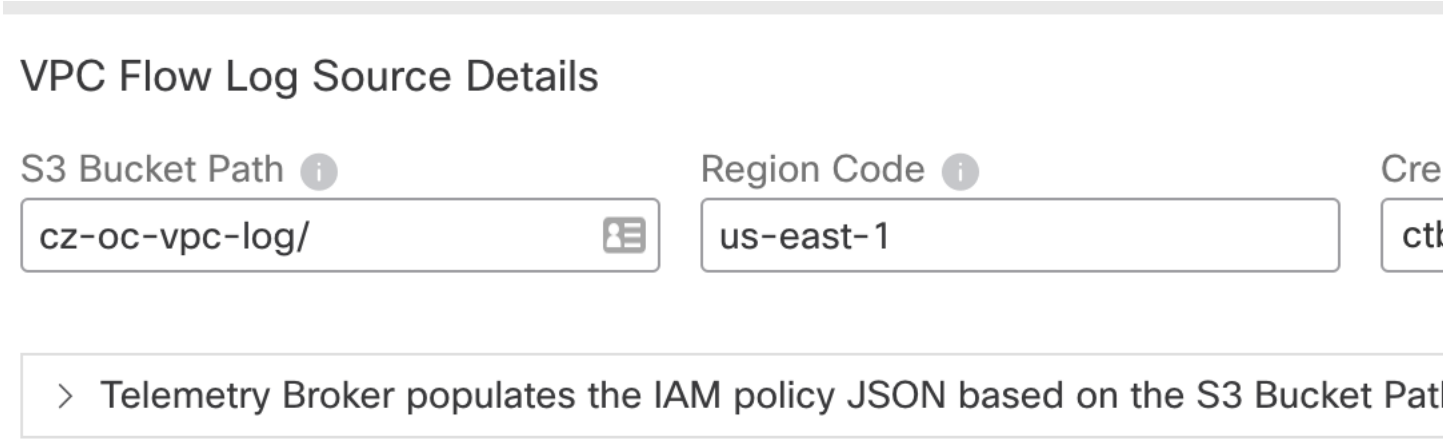
1. AWS console IAM – policies – Create policy. Create a new CTB policy with json copied earlier.
2. Now with in 'IAM'create a user Group and assign the user to the group.
3. Attach the policy to the group. Also add AWSS3READonly per-defined policy to the group.

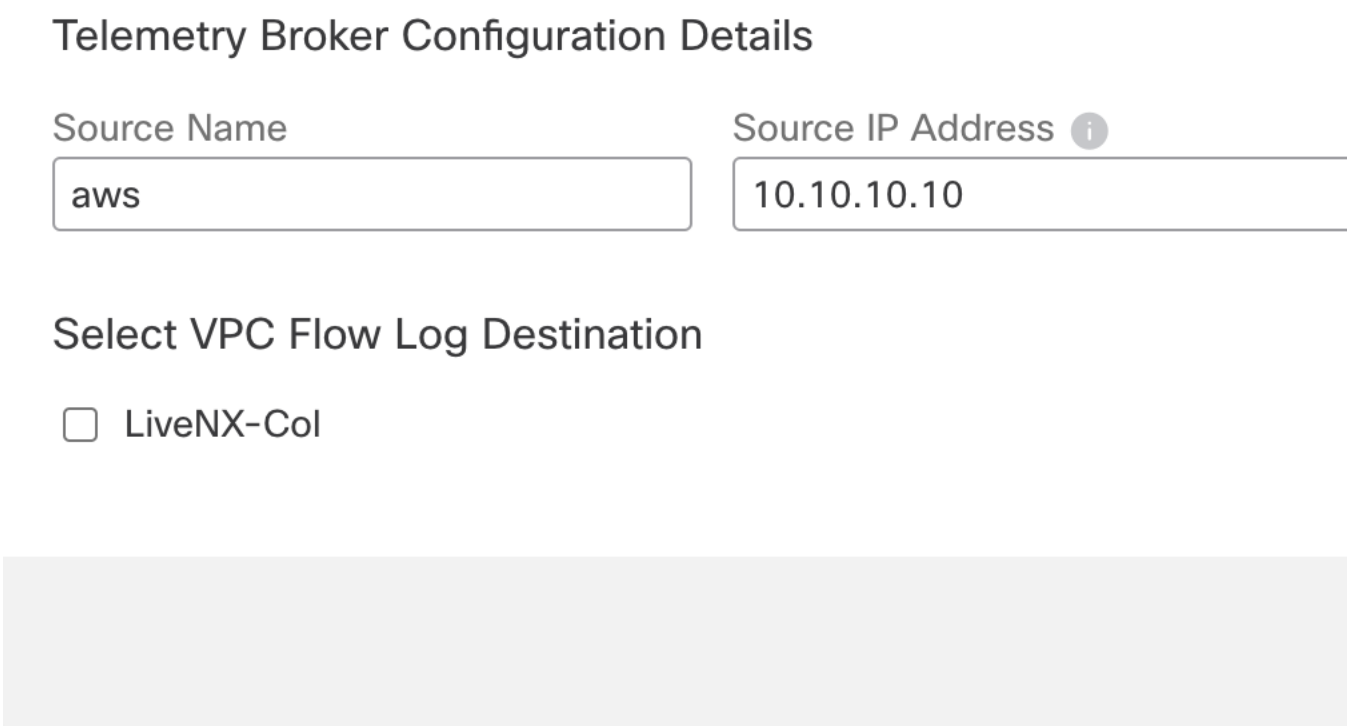


CTB side of work (Part - II)

To configure Cisco Telemetry Broker to process the VPC Flow Log data and transform it into IPFIX, complete the following steps.

1. In CTB add vpc flow log > source name
2. Enter source IP address. This is the IP address CTB will use as VPC flow log source address.
3. Assigned a Broker node, choose telemetry interface.
4. Assign a destination to ingest the flow log data. Note that Cisco Telemetry Broker transforms VPC Flow Logs to IPFIX.
5. Fields shown below -

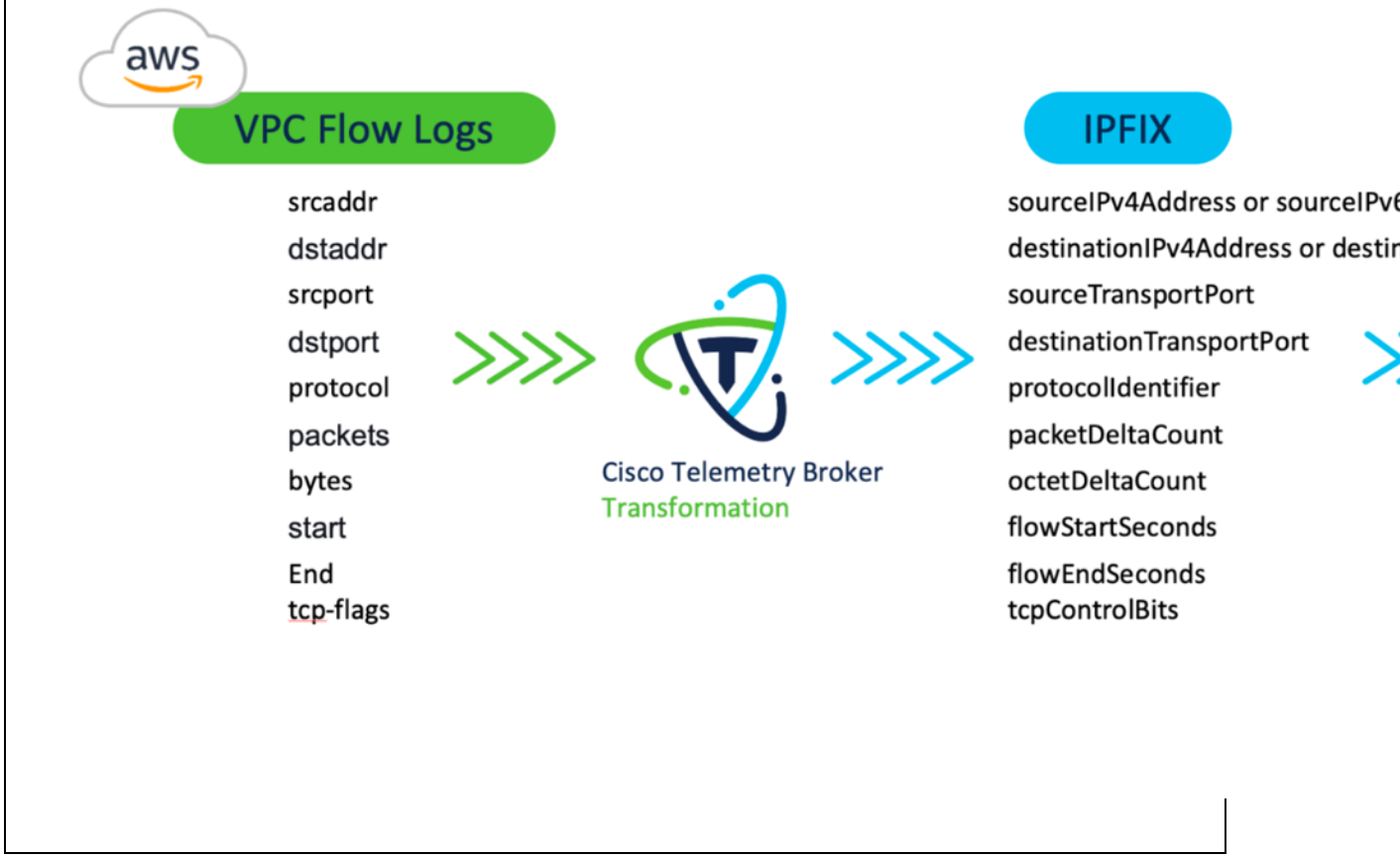


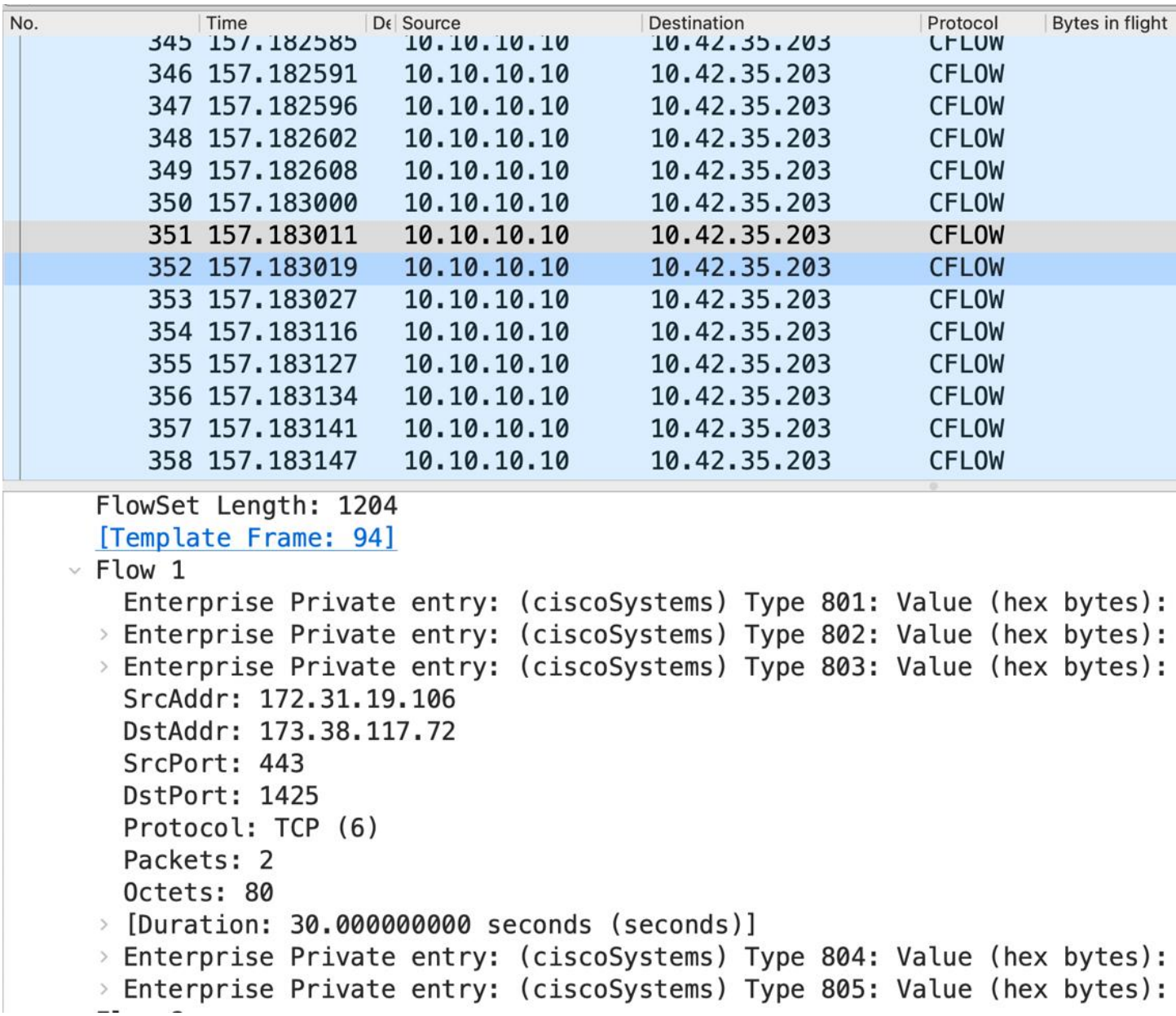


CTB VPC Flow log Validation:

1. Open the Netflow collector of your choice(destination) and search for VPC interface/flows.
2. Run a packet capture at Flow log collector and watch the IPIFX stream in coming.

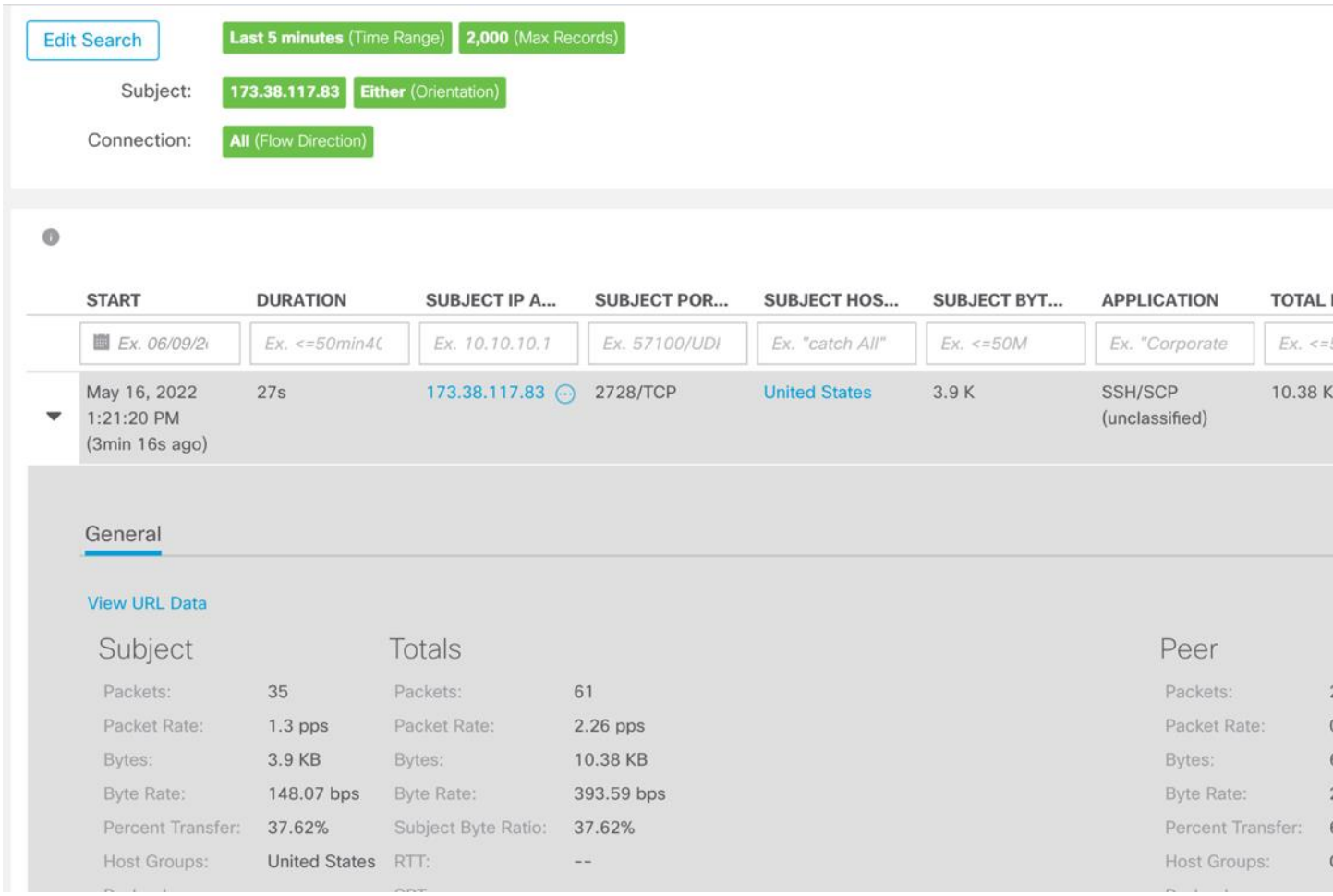
version account-id interface-id srcaddr dstaddr srcport dstport protocol packets bytes start end action log-status


aws
VPC Flow Logs
srcaddr
dstaddr
srcport
dstport
protocol
packets
bytes
start
End
tcp-flags
Cisco Telemetry Broker
Transformation
IPFIX
sourceIPv4Address or sourceIPv6
destinationIPv4Address or destin
sourceTransportPort
destinationTransportPort
protocolIdentifier
packetDeltaCount
octetDeltaCount
flowStartSeconds
flowEndSeconds
tcpControlBits



No.	Time	De	Source	Destination	Protocol	Bytes in flight
345	157.182585		10.10.10.10	10.42.35.203	CFLOW	
346	157.182591		10.10.10.10	10.42.35.203	CFLOW	
347	157.182596		10.10.10.10	10.42.35.203	CFLOW	
348	157.182602		10.10.10.10	10.42.35.203	CFLOW	
349	157.182608		10.10.10.10	10.42.35.203	CFLOW	
350	157.183000		10.10.10.10	10.42.35.203	CFLOW	
351	157.183011		10.10.10.10	10.42.35.203	CFLOW	
352	157.183019		10.10.10.10	10.42.35.203	CFLOW	
353	157.183027		10.10.10.10	10.42.35.203	CFLOW	
354	157.183116		10.10.10.10	10.42.35.203	CFLOW	
355	157.183127		10.10.10.10	10.42.35.203	CFLOW	
356	157.183134		10.10.10.10	10.42.35.203	CFLOW	
357	157.183141		10.10.10.10	10.42.35.203	CFLOW	
358	157.183147		10.10.10.10	10.42.35.203	CFLOW	

```
FlowSet Length: 1204
[Template Frame: 94]
Flow 1
  Enterprise Private entry: (ciscoSystems) Type 801: Value (hex bytes):
> Enterprise Private entry: (ciscoSystems) Type 802: Value (hex bytes):
> Enterprise Private entry: (ciscoSystems) Type 803: Value (hex bytes):
  SrcAddr: 172.31.19.106
  DstAddr: 173.38.117.72
  SrcPort: 443
  DstPort: 1425
  Protocol: TCP (6)
  Packets: 2
  Octets: 80
> [Duration: 30.000000000 seconds (seconds)]
> Enterprise Private entry: (ciscoSystems) Type 804: Value (hex bytes):
> Enterprise Private entry: (ciscoSystems) Type 805: Value (hex bytes):
```


Edit Search
Last 5 minutes (Time Range)
2,000 (Max Records)
Subject:
173.38.117.83
Either (Orientation)
Connection:
All (Flow Direction)
START
DURATION
SUBJECT IP A...
SUBJECT POR...
SUBJECT HOS...
SUBJECT BYT...
APPLICATION
TOTAL
Ex. 06/09/2
Ex. <=50min4(
Ex. 10.10.10.1
Ex. 57100/UDI
Ex. "catch All"
Ex. <=50M
Ex. "Corporate
May 16, 2022 1:21:20 PM (3min 16s ago)
27s
173.38.117.83
2728/TCP
United States
3.9 K
SSH/SCP (unclassified)
10.38 K
General
View URL Data
Subject
Packets: 35
Packet Rate: 1.3 pps
Bytes: 3.9 KB
Byte Rate: 148.07 bps
Percent Transfer: 37.62%
Host Groups: United States
Totals
Packets: 61
Packet Rate: 2.26 pps
Bytes: 10.38 KB
Byte Rate: 393.59 bps
Subject Byte Ratio: 37.62%
RTT: --
Peer
Packets:
Packet Rate:
Bytes:
Byte Rate:
Percent Transfer:
Host Groups: