FloCon 2024

20th Annual Open Forum for Large-Scale Data Analytics

Using Data to Defend

Fusing AWS VPC Flow Logs and Traditional Netflow

JANUARY 9TH, 2024

Dan Ruef
NetSA Technical Manager

Document Markings

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

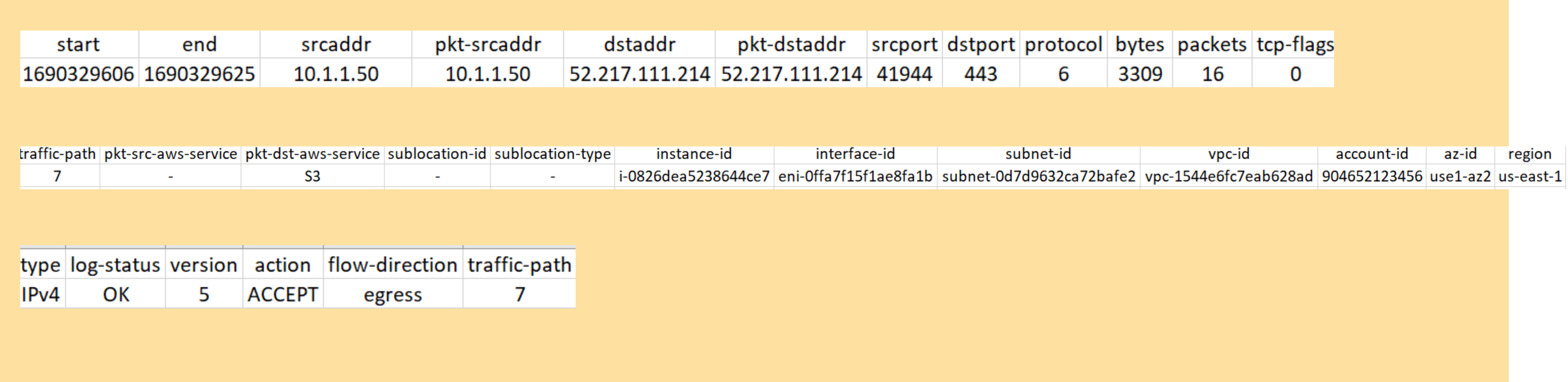
DM24-0002

Agenda

- AWS VPC Flow Logs vs. Traditional Flow Sensor
- Collection Opportunities
- Fusion into Single Repository
- Future Implementation and Next Steps

AWS VPC Flow Logs Intro

- AWS VPC flow logs come from AWS
  - Collection at interfaces, instances, vpc-wide
- Text based Comma Separated Values
- ~200 bytes per record
- Broken into flow, cloud, and metadata fields

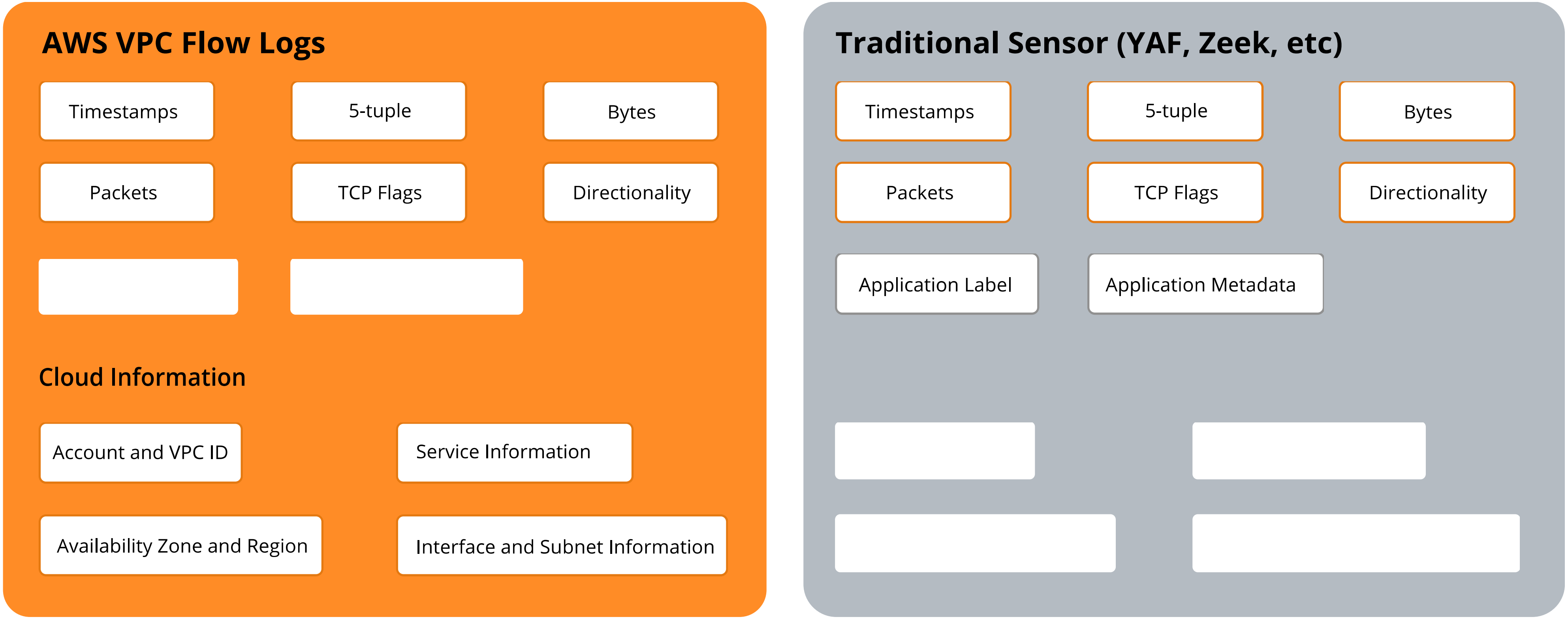


start	end	srcaddr	pkt-srcaddr	dstaddr	pkt-dstaddr	srcport	dstport	protocol	bytes	packets	tcp-flags
1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.111.214	52.217.111.214	41944	443	6	3309	16	0

traffic-path	pkt-src-aws-service	pkt-dst-aws-service	sublocation-id	sublocation-type	instance-id	interface-id	subnet-id	vpc-id	account-id	az-id	region
7	-	S3	-	-	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	subnet-0d7d9632ca72bafe2	vpc-1544e6fc7eab628ad	904652123456	use1-az2	us-east-1

type	log-status	version	action	flow-direction	traffic-path
IPv4	OK	5	ACCEPT	egress	7

AWS VPC Flow Logs vs Traditional Sensor



AWS VPC Flow Logs

- Timestamps
- 5-tuple
- Bytes
- Packets
- TCP Flags
- Directionality

Cloud Information

- Account and VPC ID
- Service Information
- Availability Zone and Region
- Interface and Subnet Information

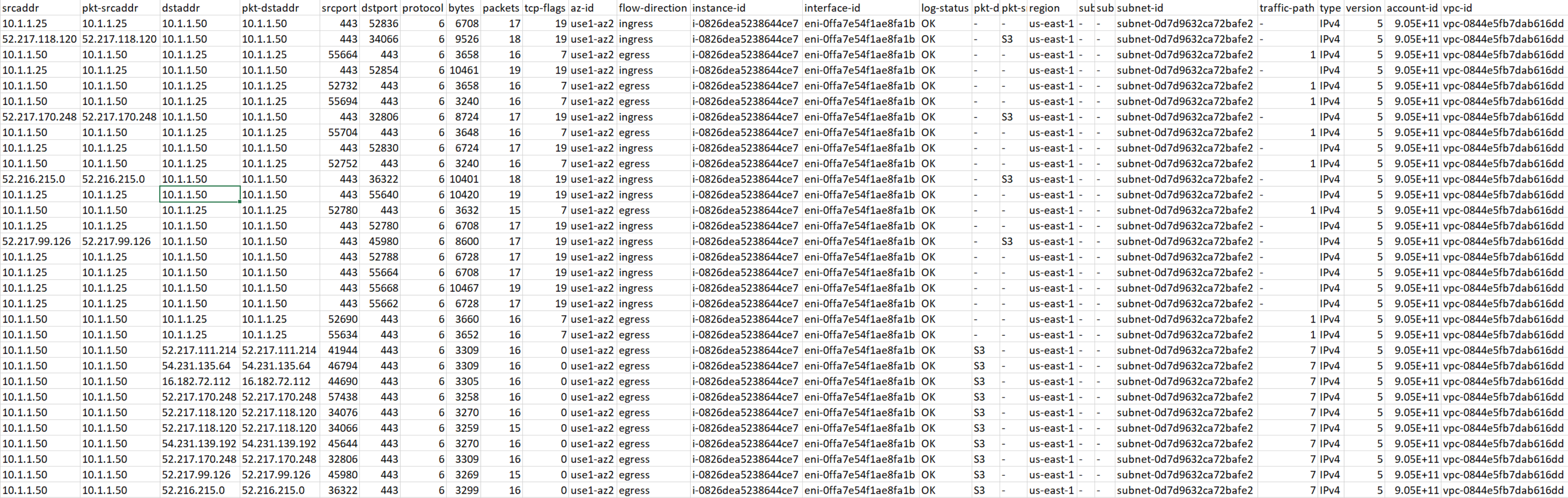
Traditional Sensor (YAF, Zeek, etc)

- Timestamps
- 5-tuple
- Bytes
- Packets
- TCP Flags
- Directionality
- Application Label
- Application Metadata

AWS VPC Flow Logs “Cloud Fields” - At Least 137 Bytes

Field Name	Bytes/Characters in CSV*	Level	Example
version	1	2	1,2,3,4,5
interface-id	21	2	eni-0a7d978d39bba1620
account-id	12	2	123456789123
Action	6	2	“ACCEPT” or “REJECT”
log-status	Typically 2	2	“OK”, “NODATA”, or “SKIPDATA”
vpc-id	21	3	vpc-0dd4fd42a389a5a79
subnet-id	24	3	subnet-0a5397bcdecc7e2cc
type	4	3	“IPv4”, “IPv6”, or “EFA”
region	9	4	us-east-1
az-id	7	4	use1-az2
sublocation-type	Usually 1	4	Usually “-”
sublocation-id	Usually 1	4	Usually “-”
pkt-src-aws-service	Usually 1; 3-10	5	“-” |CLOUD9 |DYNAMODB|EC2 | KINESIS_VIDEO_STREAMS | ROUTE53 | S3
pkt-dst-aws-service	Usually 1; 3-10	5	“-” |CLOUD9 |DYNAMODB|EC2 | KINESIS_VIDEO_STREAMS | ROUTE53 | S3
flow-direction	6 or 7	5	“ingress” or “egress”
traffic-path	1	5	1,2,3,4,5,6,7 or 8

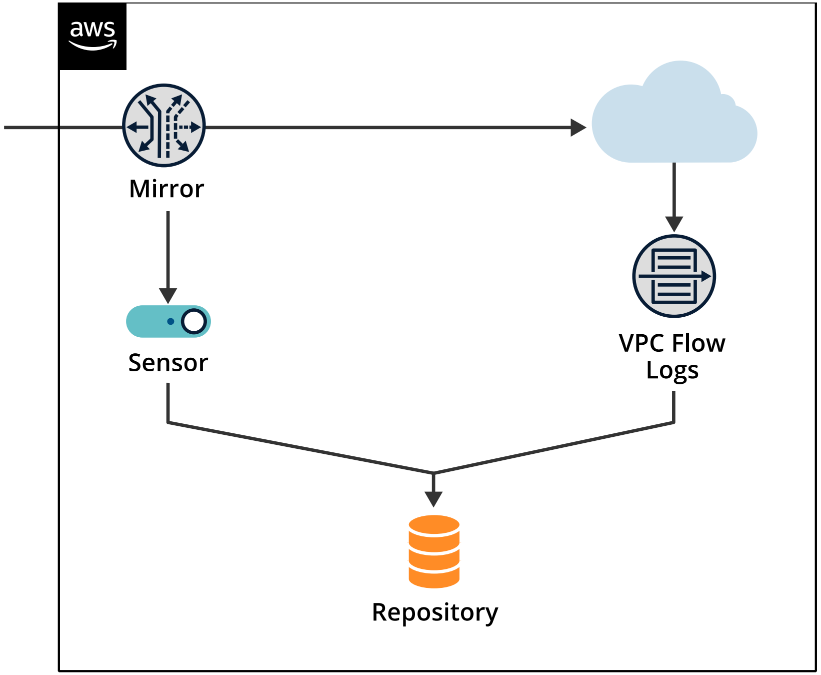
Snapshot of AWS VPC Flow Logs



srcaddr	pkt-srcaddr	dstaddr	pkt-dstaddr	srcport	dstport	protocol	bytes	packets	tcp-flags	az-id	flow-direction	instance-id	interface-id	log-status	pkt-d	pkt-s	region	sub	sub	subnet-id	traffic-path	type	version	account-id	vpc-id
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52836	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
52.217.118.120	52.217.118.120	10.1.1.50	10.1.1.50	443	34066	6	9526	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55664	443	6	3658	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52854	6	10461	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52732	443	6	3658	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55694	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
52.217.170.248	52.217.170.248	10.1.1.50	10.1.1.50	443	32806	6	8724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55704	443	6	3648	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52830	6	6724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52752	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
52.216.215.0	52.216.215.0	10.1.1.50	10.1.1.50	443	36322	6	10401	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55640	6	10420	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52780	443	6	3632	15	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52780	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
52.217.99.126	52.217.99.126	10.1.1.50	10.1.1.50	443	45980	6	8600	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52788	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55664	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55668	6	10467	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55662	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52690	443	6	3660	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55634	443	6	3652	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.111.214	52.217.111.214	41944	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	54.231.135.64	54.231.135.64	46794	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	16.182.72.112	16.182.72.112	44690	443	6	3305	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	57438	443	6	3258	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34076	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34066	443	6	3259	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	54.231.139.192	54.231.139.192	45644	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	32806	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.217.99.126	52.217.99.126	45980	443	6	3269	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd
10.1.1.50	10.1.1.50	52.216.215.0	52.216.215.0	36322	443	6	3299	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.05E+11	vpc-0844e5fb7dab616dd

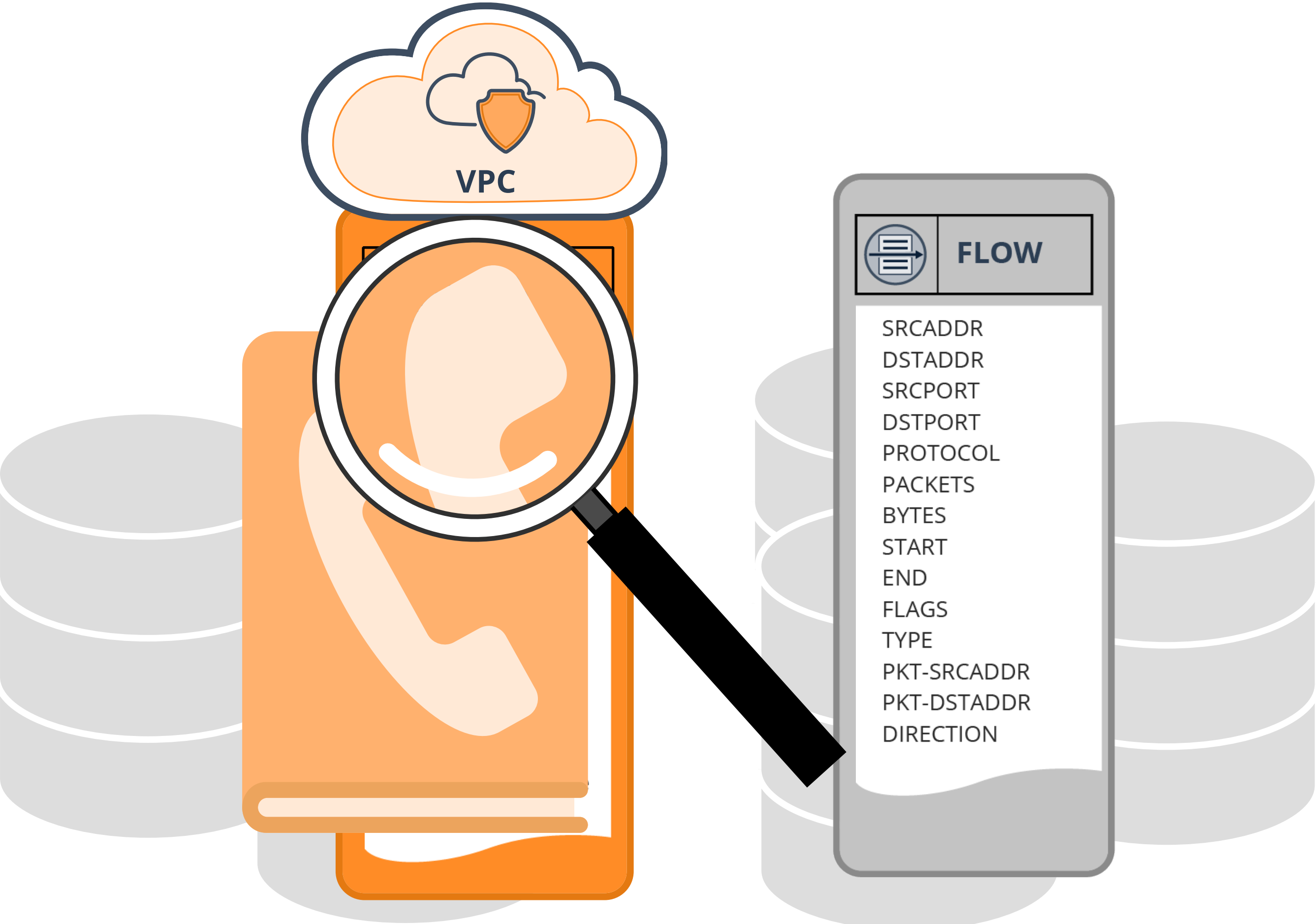
[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Ultimate Goal



- Single repository
- Retain all information
- Remove redundancy
- Conserve Storage
- Present one view to analysts
- Utilize single set of analysis tools

SiLK on the scene



SRCADDR
DSTADDR
SRCPORT
DSTPORT
PROTOCOL
PACKETS
BYTES
START
END
FLAGS
TYPE
PKT-SRCADDR
PKT-DSTADDR
DIRECTION

Map from Flow to Cloud fields

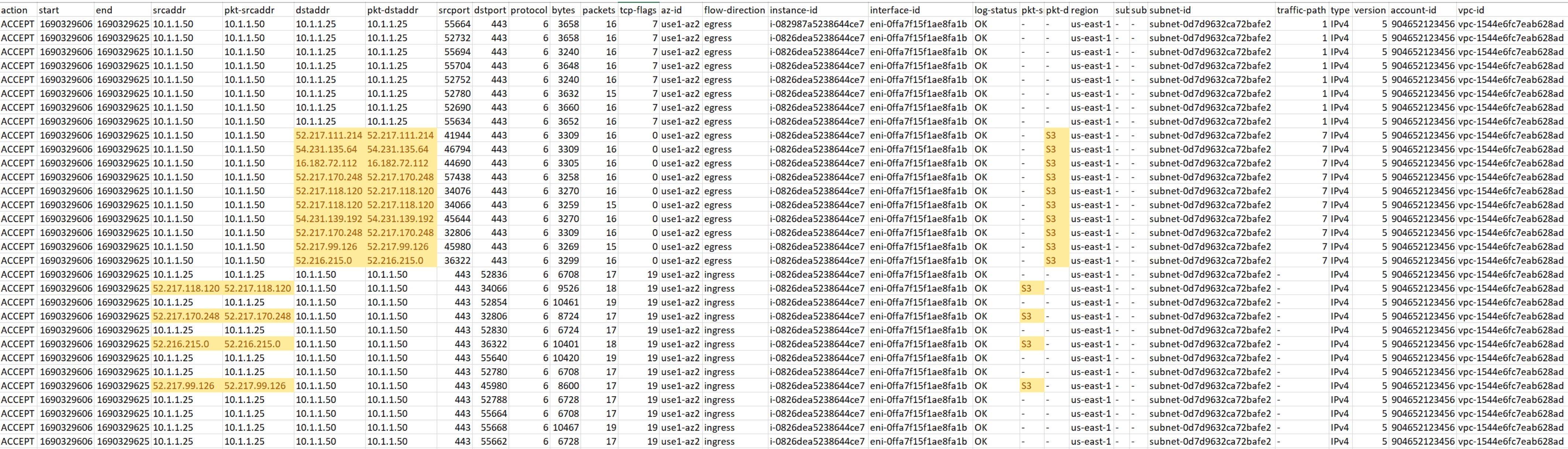
Cloud fields are typically at least **137** bytes per record

- Used in **filtering**: “Look at all traffic to and from S3”
- Used in **enrichment**: “Add cloud information to these flows of interest”

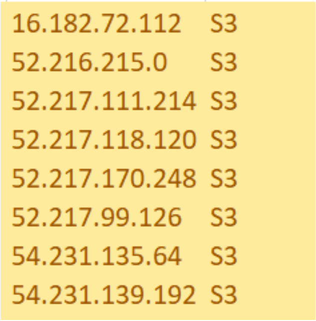
Convert to two-way lookup

- Use IP as the key and cloud field +timestamp as value

Sorted For Directionality – S3 Labeling

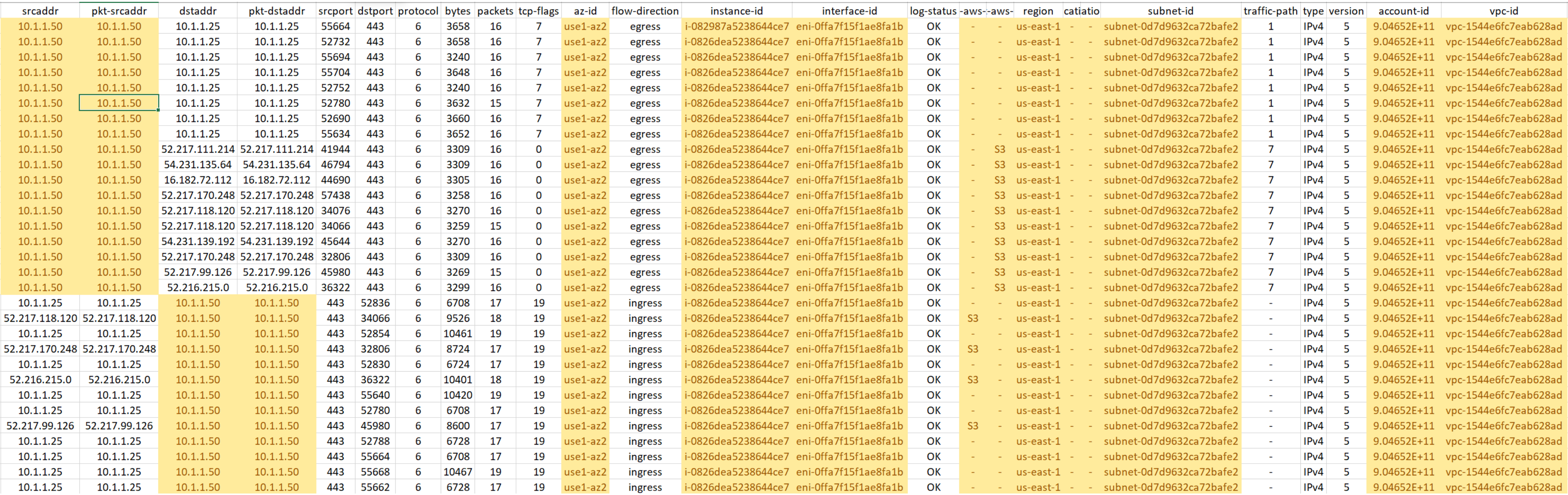


action	start	end	srcaddr	pkt-srcaddr	dstaddr	pkt-dstaddr	srcport	dstport	protocol	bytes	packets	tcp-flags	az-id	flow-direction	instance-id	interface-id	log-status	pkt-s	pkt-d	region	sub	sub	subnet-id	traffic-path	type	version	account-id	vpc-id
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55664	443	6	3658	16	7	use1-az2	egress	i-082987a5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52732	443	6	3658	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55694	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55704	443	6	3648	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52752	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52780	443	6	3632	15	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52690	443	6	3660	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55634	443	6	3652	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.111.214	52.217.111.214	41944	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	54.231.135.64	54.231.135.64	46794	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	16.182.72.112	16.182.72.112	44690	443	6	3305	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	57438	443	6	3258	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34076	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34066	443	6	3259	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	54.231.139.192	54.231.139.192	45644	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	32806	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.217.99.126	52.217.99.126	45980	443	6	3269	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.50	10.1.1.50	52.216.215.0	52.216.215.0	36322	443	6	3299	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52836	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	52.217.118.120	52.217.118.120	10.1.1.50	10.1.1.50	443	34066	6	9526	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52854	6	10461	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	52.217.170.248	52.217.170.248	10.1.1.50	10.1.1.50	443	32806	6	8724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52830	6	6724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	52.216.215.0	52.216.215.0	10.1.1.50	10.1.1.50	443	36322	6	10401	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55640	6	10420	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52780	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	52.217.99.126	52.217.99.126	10.1.1.50	10.1.1.50	443	45980	6	8600	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52788	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55664	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55668	6	10467	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad
ACCEPT	1690329606	1690329625	10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55662	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	904652123456	vpc-1544e6fc7eab628ad



16.182.72.112	S3
52.216.215.0	S3
52.217.111.214	S3
52.217.118.120	S3
52.217.170.248	S3
52.217.99.126	S3
54.231.135.64	S3
54.231.139.192	S3

Sorted For Directionality – Internal IP Labeling

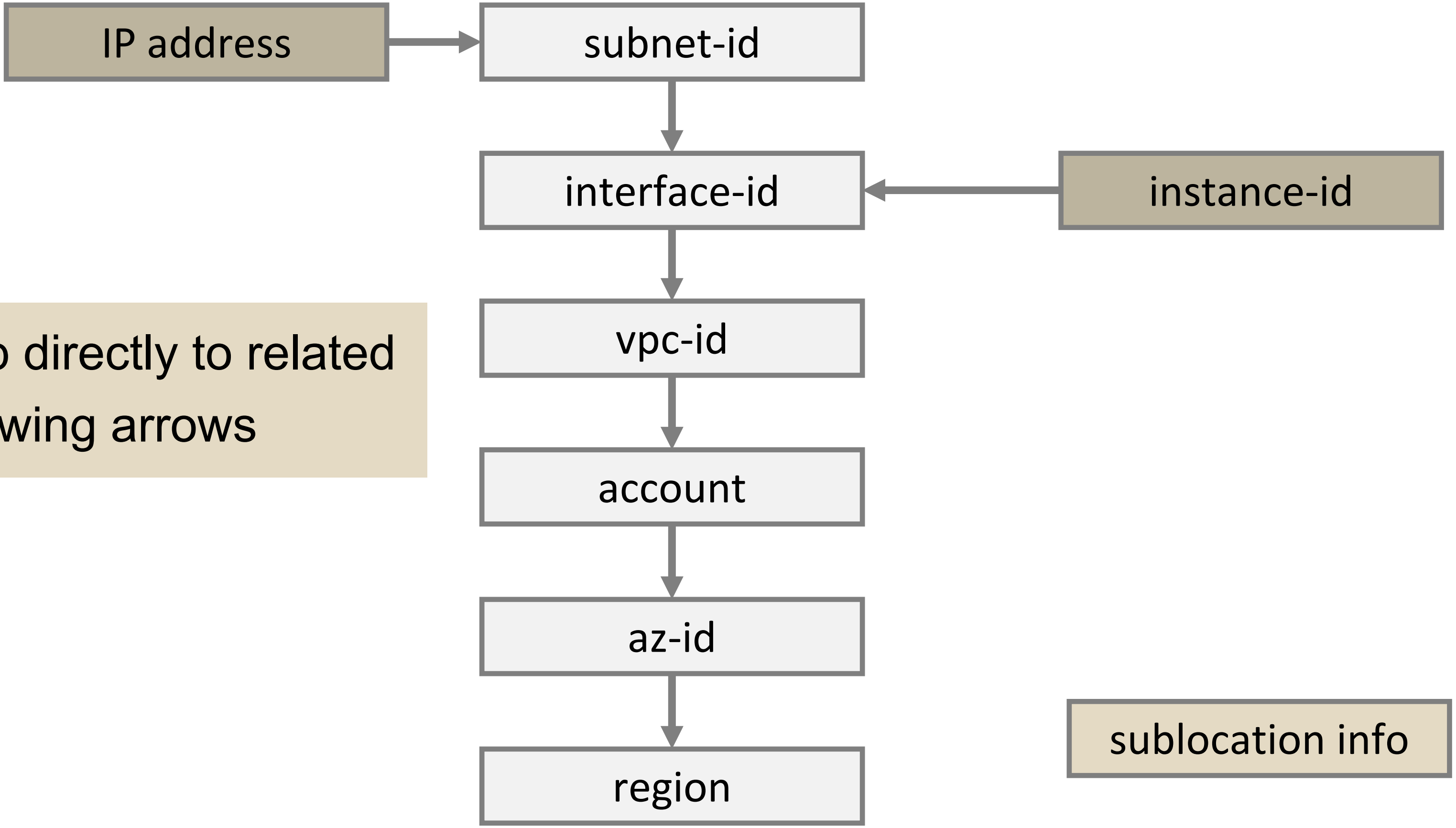


srcaddr	pkt-srcaddr	dstaddr	pkt-dstaddr	srcport	dstport	protocol	bytes	packets	tcp-flags	az-id	flow-direction	instance-id	interface-id	log-status	-aws-	-aws-	region	cati	atio	subnet-id	traffic-path	type	version	account-id	vpc-id
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55664	443	6	3658	16	7	use1-az2	egress	i-082987a5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52732	443	6	3658	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55694	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55704	443	6	3648	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52752	443	6	3240	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52780	443	6	3632	15	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	52690	443	6	3660	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	10.1.1.25	10.1.1.25	55634	443	6	3652	16	7	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	1	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.111.214	52.217.111.214	41944	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	54.231.135.64	54.231.135.64	46794	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	16.182.72.112	16.182.72.112	44690	443	6	3305	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	57438	443	6	3258	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34076	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.118.120	52.217.118.120	34066	443	6	3259	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	54.231.139.192	54.231.139.192	45644	443	6	3270	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.170.248	52.217.170.248	32806	443	6	3309	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.217.99.126	52.217.99.126	45980	443	6	3269	15	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.216.215.0	52.216.215.0	36322	443	6	3299	16	0	use1-az2	egress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	S3	us-east-1	-	-	subnet-0d7d9632ca72bafe2	7	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52836	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
52.217.118.120	52.217.118.120	10.1.1.50	10.1.1.50	443	34066	6	9526	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52854	6	10461	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
52.217.170.248	52.217.170.248	10.1.1.50	10.1.1.50	443	32806	6	8724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52830	6	6724	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
52.216.215.0	52.216.215.0	10.1.1.50	10.1.1.50	443	36322	6	10401	18	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55640	6	10420	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52780	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
52.217.99.126	52.217.99.126	10.1.1.50	10.1.1.50	443	45980	6	8600	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	S3	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52788	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55664	6	6708	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55668	6	10467	19	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55662	6	6728	17	19	use1-az2	ingress	i-0826dea5238644ce7	eni-0ffa7f15f1ae8fa1b	OK	-	-	us-east-1	-	-	subnet-0d7d9632ca72bafe2	-	IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad

IP Address	First Seen	Last Seen	Availability Zone	Instance-ID	Interface-id	Service	Region	Subnet-ID	Account-ID	VPC-ID	Sublocation
10.1.1.50	1690329000	1690330000	use1-az2	i-0826dea5238644ce7	eni-0ffa7e54f1ae8fa1b		us-east-1	subnet- 0d7d9632ca72bafe2	904652123456	vpc- 0844e5fd7dab616dd	

[DISTRIBUTION STATEMENT A] Approved for public release and unlimited distribution.

Further Cloud Field Reduction



Values map directly to related values following arrows

Fields we can remove or reduce

Action

- accept and reject accounted for in SiLK class/type

Flow-direction

- accounted for in SiLK class/type

Log-status

- used for processing, but not analyzing

Interface-id

- can either become silk sensor

Type

- dropped as SiLK combines v4 and v6

Version

- used for processing, but not analyzing

Convert non-mirrored flows

Convert what doesn’t come out of sensor to that format, such as SiLK, IPFIX, Zeek.

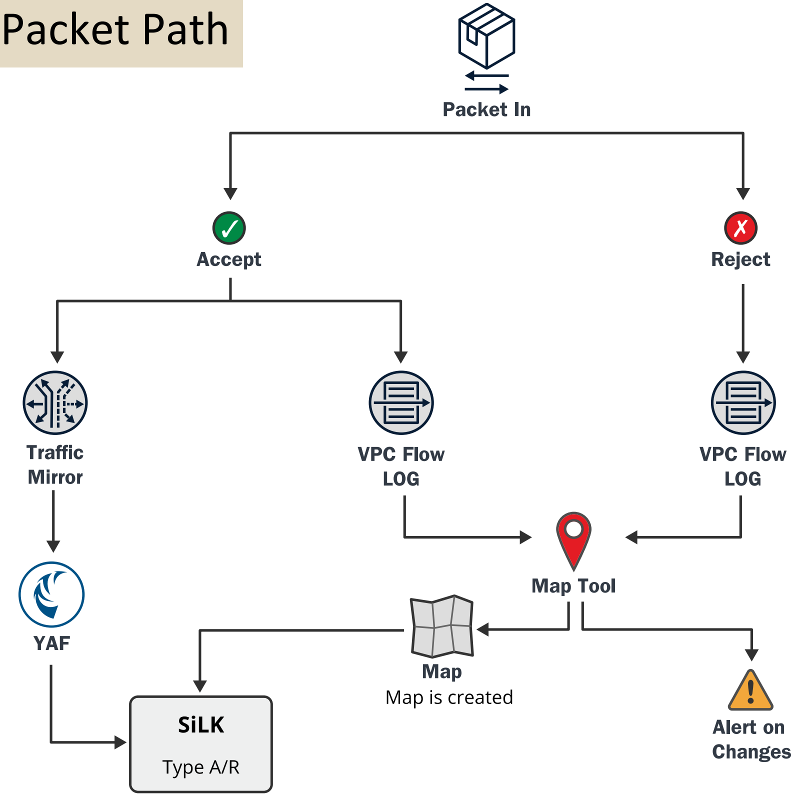
Primarily “REJECT” packets

Choose proper IP addresses from flow logs from a NAT

PKT-SRCADDR and PKT-DSTADDR

Architecture

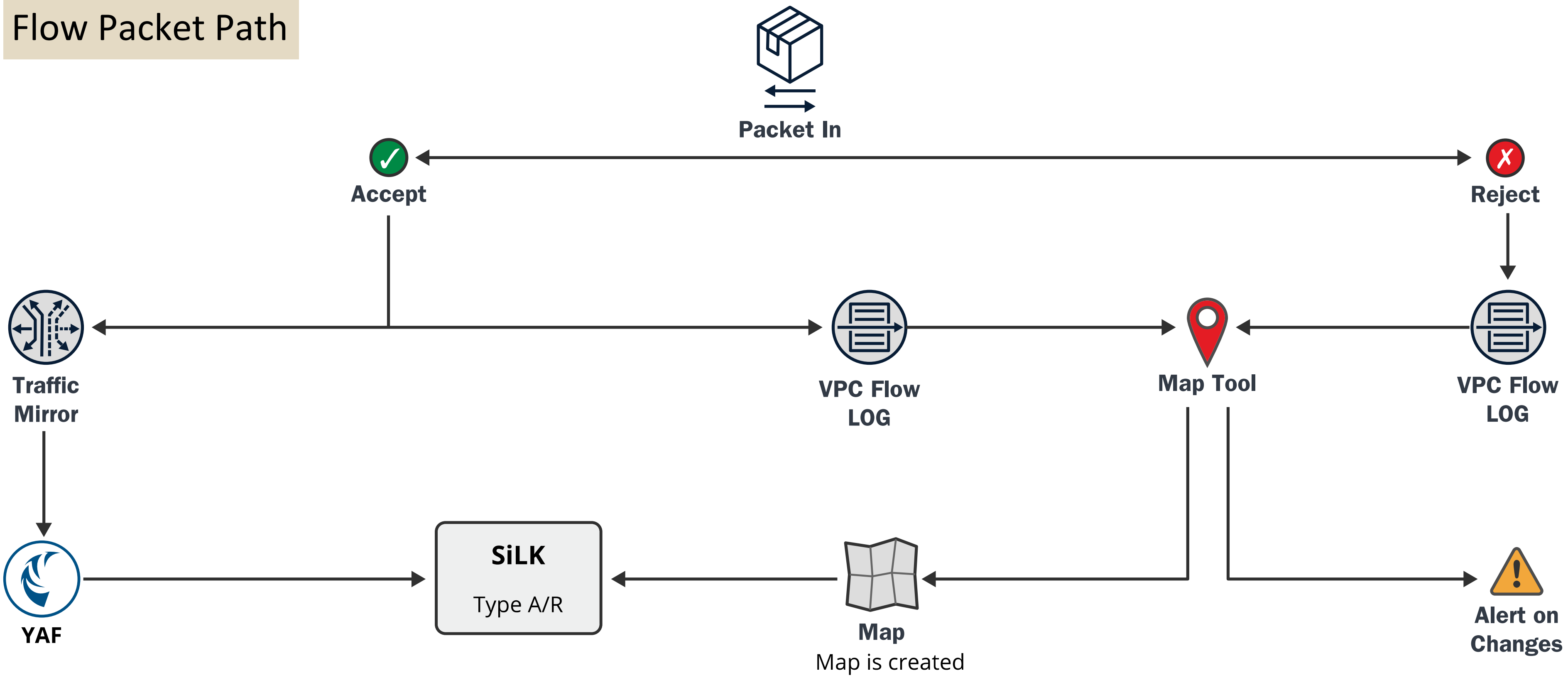
Flow Packet Path



- **Accept** flows in both. Extract for map
- **Reject** flows added to SiLK repository
- Map referenced by SiLK tools.
- Map can also alert on changes

Full Architecture

Flow Packet Path



Next Steps

- How to handle multiple interfaces meaningfully to create an “**inside**” and “**outside**”
- Define additional class-type labels:

  int2aws

  aws2int
- Investigate AWS API calls for context
- Handle multi-VPC collection efficiently
- Additional architectures
- AWS VPC Flow Log to SiLK

Contact

Dan Ruef
Network Situational Awareness Technical Manager

Email: druef@cert.org

Email: netsa-help@cert.org

Email: info@sei.cmu.edu