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

Copyright 2024 Carnegie Mellon University.

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.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

CERT®, Carnegie Mellon® and FloCon® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

DM24-0002

Agenda

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

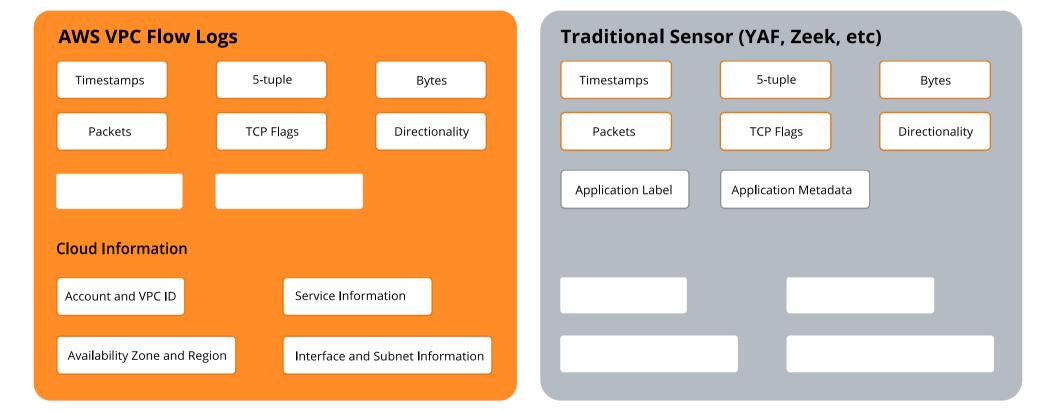
AWS VPC Flow Logs Intro

- 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

S	start end srcaddr pk		-srcaddr	caddr ds		pkt-d	staddr	srcport	dstport	protocol	bytes	packets	tcp-flags					
1690	329606 16	9032962	25 10.	1.1.50 1).1.1.50	52.21	7.111.214	52.217	.111.214	41944	443	6	3309	16	0			
traffic-	path pkt-src-a	ws-service	pkt-dst-aws	s-service sublocatio	n-id sublocatio	on-type	instance	e-id	interfa	ce-id	su	ıbnet-id		vpc-id		account-id	az-id	region
7		-	\$3	-	-		i-0826dea523	8644ce7 e	eni-Offa7f15	f1ae8fa1b	subnet-0d7	d9632ca72b	afe2 vpc	:-1544e6fc7e	ab628ad 9	04652123456	use1-az2	us-east-1
type	log-status	version	action	flow-direction	traffic-pat	h												
IPv4	OK	5	ACCEPT	egress	7													

AWS VPC Flow Logs vs Traditional Sensor



FloCon 2024 © 2024

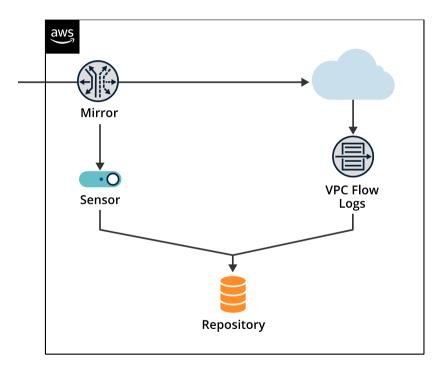
AWS VPC Flow Logs "Cloud Fields" - At Least 137 Bytes

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

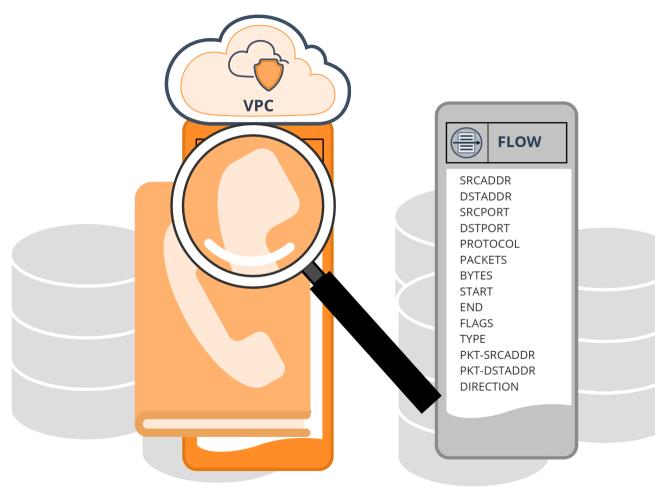
t-srcaddr d	dstaddr	pkt-dstaddr	srcport o	astport proto	ocol bytes pa	ckets tcp-fla	ags az-id	flow-directio	on instance-id	interface-id	og-status pkt	-d pkt-:	region	sutsut	subnet-id	traffic-path type ve	rsion a	ccount-id vp	c-id
.1.1.25	10.1.1.50	10.1.1.50	443	52836	6 6708	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.217.118.120	10.1.1.50	10.1.1.50	443	34066	6 9526	18	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	S3	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	55664	443	6 3658	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	52854	6 10461	19	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	52732	443	6 3658	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	55694	443	6 3240	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.217.170.248	10.1.1.50	10.1.1.50	443	32806	6 8724	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	S3	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	55704	443	6 3648	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	52830	6 6724	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	52752	443	6 3240	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.216.215.0	10.1.1.50	10.1.1.50	443	36322	6 10401	18	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	S3	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	55640	6 10420	19	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	52780	443	6 3632	15	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	52780	6 6708	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.217.99.126	10.1.1.50	10.1.1.50	443	45980	6 8600	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	S3	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	52788	6 6728	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	55664	6 6708	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	55668	6 10467	19	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.25	10.1.1.50	10.1.1.50	443	55662	6 6728	17	19 use1-az2	ingress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	- IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	52690	443	6 3660	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	10.1.1.25	10.1.1.25	55634	443	6 3652	16	7 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK -	-	us-east-1		subnet-0d7d9632ca72bafe2	1 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50 !	52.217.111.214	52.217.111.214	41944	443	6 3309	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50 !	54.231.135.64	54.231.135.64	46794	443	6 3309	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	16.182.72.112	16.182.72.112	44690	443	6 3305	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50 !	52.217.170.248	52.217.170.248	57438	443	6 3258	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	52.217.118.120	52.217.118.120	34076	443	6 3270	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	52.217.118.120	52.217.118.120	34066	443	6 3259	15	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	54.231.139.192	54.231.139.192	45644	443	6 3270	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	52.217.170.248	52.217.170.248	32806	443	6 3309	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	DK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	52.217.99.126	52.217.99.126	45980	443	6 3269	15	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.1.1.50	52.216.215.0	52.216.215.0	36322	443	6 3299	16	0 use1-az2	egress	i-0826dea5238644ce7	eni-Offa7e54f1ae8fa1b	OK S3	-	us-east-1		subnet-0d7d9632ca72bafe2	7 IPv4	5	9.05E+11 vp	c-0844e5fb7dab616d
.11 .12 .11 .11 .11 .11 .11 .11 .11 .11	1.25 17.118.120 1.150 1.150 1.150 17.170.248 1.50 1.25 1.25 1.25 1.25 1.25 1.25 1.25 1.25	1.1.25 10.1.1.50 117.118.120 10.1.1.50 1.1.25 10.1.1.50 1.1.25 10.1.1.50 1.1.25 10.1.1.25 1.1.50 10.1.1.25 1.1.50 10.1.1.25 1.1.50 10.1.1.25 1.1.50 10.1.1.25 1.1.50 10.1.1.25 1.1.50 10.1.1.50 1.1.50 10.1.1.50 1.1.50 10.1.1.50 1.1.50 10.1.1.50 1.1.50 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.25 10.1.1.50 1.50 10.1.1.25 1.50 10.1.1.25 1.50 52.217.112.24 1.50 52.217.113.264 1.50 52.217.113.20 1.50 52.217.113.20 1.50 52.217.113.20	1.25 10.1.1.50 10.1.1.50 17.118.120 10.1.1.50 10.1.1.50 1.50 10.1.1.25 10.1.1.50 1.52 10.1.1.25 10.1.1.50 1.50 10.1.1.25 10.1.1.25 1.50 10.1.1.25 10.1.1.25 1.50 10.1.1.25 10.1.1.25 1.50 10.1.1.25 10.1.1.25 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.1.50 1.50 10.1.1.50 10.1.50 1.50 10.1.1.50 10.1.50 1.50 10.1.1.50 10.1.50 1.52 10.1.1.50 10.1.50 1.52 10.1.1.50 10.1.50 1.52 10.1.1.50 10.1.50 1.52 10.1.1.50 10.1.50 1.50 10.1.50	1.25 10.1.1.50 10.1.1.50 443 17.118.120 10.1.1.50 10.1.1.50 443 1.1.50 10.1.1.50 10.1.1.50 443 1.1.50 10.1.1.50 10.1.1.50 443 1.1.50 10.1.1.50 10.1.1.50 443 1.1.50 10.1.1.50 10.1.1.50 55694 1.1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.1.50 443 1.50 10.1.1.50 10.1.50 443 1.50 10.1.1.50 10.1.50 443 1.50 10.1.1.50 10.1.50 443 1.50 10.1.1.50 10.1.50 443 1.50 10.1.1.50 10.1.50 443 1.50 10.1.50	1.125 10.1.1.50 10.1.1.50 443 52836 17.118.120 10.1.1.50 10.1.1.50 443 34066 1.1.50 10.1.1.50 10.1.1.50 443 34066 1.1.50 10.1.1.50 10.1.1.50 443 52836 1.1.50 10.1.1.50 10.1.1.50 55664 443 1.1.50 10.1.1.25 52732 443 1.1.50 10.1.1.50 10.1.1.55 55694 443 1.1.50 10.1.1.50 10.1.1.50 443 52830 1.1.50 10.1.1.50 10.1.1.50 443 52830 1.1.50 10.1.1.50 10.1.50 443 52830 1.50 10.1.1.50 10.1.50 443 52830 1.50 10.1.1.50 10.1.50 443 52830 1.50 10.1.1.50 10.1.50 443 52830 1.50 10.1.1.50 10.1.50 443 52830 1.50 10.1.1.50 10.1.50 443	1.2510.1.1.5010.1.1.50443528366670817.118.12010.1.1.5010.1.1.5044334066695261.5010.1.1.2510.1.1.5044354066695261.5010.1.1.2510.1.1.50443528546104611.5010.1.1.5010.1.1.50443528546104611.5010.1.1.5010.1.1.50443528546324017.70.24810.1.1.5010.1.1.5044352830667241.5010.1.1.5010.1.1.5044352830667241.5010.1.1.5010.1.1.5044352830667241.5010.1.1.5010.1.1.5044352830667241.5010.1.1.5010.1.1.5044352830667241.5010.1.1.5010.1.1.5044355664667241.5010.1.1.5010.1.1.5044355664667081.5010.1.1.5010.1.1.5044355664667081.2510.1.1.5010.1.1.5044355664667081.2510.1.1.5010.1.1.5044355662667281.5010.1.1.5010.1.1.5044355662667281.5010.1.1.5010.1.1.5044355664667081.5010.1.1.5010.1.1.504435566266728<	1.2510.1.1.5010.1.1.5014.4352836667081717.118.12010.1.1.5010.1.1.504433406669526181.5010.1.1.2510.1.1.504435486610461191.2510.1.1.5010.1.1.555566444363588161.5010.1.1.5010.1.1.555573244363658161.5010.1.1.5010.1.1.504435283668724171.5010.1.1.5010.1.1.504435283066724171.5010.1.1.5010.1.1.504435283066724171.5010.1.1.5010.1.1.5044353232610401181.5010.1.1.5010.1.1.504435564066708171.5010.1.1.5010.1.1.504435278066708171.5010.1.1.5010.1.1.504435278066708171.5010.1.1.5010.1.1.504435566466708171.2510.1.1.5010.1.1.504435566466708171.2510.1.1.5010.1.1.504435566466708171.2510.1.1.5010.1.1.504435566466708171.2510.1.1.5010.1.1.504435566466708171.251	1.1.25 10.1.1.50 10.1.1.50 143 52836 6 6708 17 19 use1-az2 1.1.7.118.120 10.1.1.50 10.1.1.50 443 34066 6 9526 18 19 use1-az2 1.1.50 10.1.1.25 10.1.1.50 443 5284 6 10461 19 use1-az2 1.1.50 10.1.1.25 10.1.1.25 52732 443 6 3658 16 7 use1-az2 1.1.50 10.1.1.25 10.1.1.25 55764 443 6 3648 16 7 use1-az2 1.50 10.1.1.50 10.1.1.50 443 52830 6 6724 17 19 use1-az2 1.50 10.1.1.50 10.1.1.50 443 5632 6 7 use1-az2 1.50 10.1.1.50 10.1.1.50 443 5640 6 10401 18 19 use1-az2 1.50 10.1.1.50 10.1.1.50 443 5540 6 6708 17 19 use1-az2 1.50 10.1.	1.1.25 10.1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-az2 ingress 1.1.1.1.50 10.1.1.50 443 34066 6 9526 18 19 use1-az2 ingress 1.1.50 10.1.1.25 10.1.1.50 443 52854 6 10461 19 19 use1-az2 egress 1.1.50 10.1.1.50 443 52854 6 10461 19 use1-az2 egress 1.1.50 10.1.1.50 443 528546 6 6558 16 7 use1-az2 egress 1.1.50 10.1.1.50 443 52836 6 6724 17 19 use1-az2 ingress 1.1.50 10.1.1.50 443 52830 6 6724 17 19 use1-az2 ingress 1.1.50 10.1.1.50 443 5632 6 10401 18 19 use1-az2 ingress 1.50 10.1.1.50 443 55780 443 6 3632 15 7	1.1.25 10.1.1.50 143 52836 6 6708 17 19 use1-a22 ingress 1-0826dea5238644ce7 17.118.120 10.1.1.50 10.1.1.50 443 34066 6 9526 18 19 use1-a22 ingress 1-0826dea5238644ce7 1.1.50 10.1.1.50 10.1.1.50 443 52854 6 10461 19 19 use1-a22 ingress 1-0826dea5238644ce7 1.1.50 10.1.1.25 10.1.1.25 52732 443 6 3658 16 7 use1-a22 ingress 1-0826dea5238644ce7 1.50 10.1.1.25 10.1.1.25 55694 443 6 3648 16 7 use1-a22 ingress 1-0826dea5238644ce7 1.50 10.1.1.50 443 5280 6 6724 17 19 use1-a22 ingress 1-0826dea5238644ce7 1.50 10.1.1.50 443 5626 6 10401 18 19 use1-a22 ingress 1-0826dea5238644ce7 1.6215.0 10.1.1.50 443 55640 6 </td <td>1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.1.50 10.1.1.50 413 34066 6 5526 18 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55664 443 6 3658 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55694 443 6 3658 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55694 443 6 3648 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.50 10.1.1.50 443 36320 6 6724 17 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.52 10.1.1.50 10.1.1.50 443 36322 6 10401 18 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 16.25 10.1.1.50 <td< td=""><td>1.1.50 10.1.1.50 143 52836 6 6708 17 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 17.118.10 10.1.1.50 143 34066 6 9526 18 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.1.50 143 52854 6 1041 19 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 52732 443 6 3586 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 52752 443 6 3632 15 7 use1-az2 ingress +0826dea5238644c7</td><td>1.1.50 10.1.1.50 14.1.50 443 52836 6 6708 17 19 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - 53 1.1.50 10.1.1.50 443 34066 6 9526 18 10 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 53 1.50 10.1.1.50 10.1.55 52732 443 6 3588 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 1.50 10.1.125 10.1.125 5504 443 6 3548 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - <td< td=""><td>1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - useast1 17.118.120 10.1.1.25 5064 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.150 10.1.125 5564 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55694 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55794 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 57574 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54</td><td>1.1.150 10.1.150 143 52836 6 6708 17 19 usel-az2 logges 10826des233644ce7 en-0fa7e54f1ae8fa1b OK - useart - - 17.118.120 10.1.150 10.1.150 443 34066 6 9526 18 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3658 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3624 17 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 55704 443 6 3648 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.55 1.50 10.1.125 55704 443 6 3624 17 19 usel-az2 logges538644ce7</td><td>1.1.50 10.1.1.50 441 5238 6 6708 17 19 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - use-ast-1 - submet-0d7d9632ca72bafe2 17.118.120 10.1.1.50 10.1.1.50 443 5264 443 6 658 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5232 443 6 3688 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 55964 443 6 3688 16 7 usel-ar2 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5233 6 6724 17 19 usel-ar2 legress +0026des523864ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50</td><td>1.1.50 10.1.50 443 52836 6 6708 17 9 9 9 9826de322864de7 0 0 9 u-east1 4 subert-0d76952ar2bafe2 1PM4 17.181.20 10.1.125 5564 443 6 3658 16 7 uetat2 gress 10826de322864de7 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5273 443 6 358 16 7 uetat2 gress 10826de523864de7 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5564 443 6 3246 16 7 uetat2 gress 10826de323864de7 n-0787541ae81ab 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 16 7 uetat2 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 17 9 <</td><td>1.15 10.11.50 10.</td><td>1.150 10.11.50 443 5330 6 67.88 17 10 ucl+az lgeres 1002debc32864ar2 end/frác4flasfta DK 5 uweetat - uwher0d7d953227bal2 IPA 5 0.511 vp 1111 101.125 101.125 5564 443 6 358 10</td></td<></td></td<></td>	1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.1.50 10.1.1.50 413 34066 6 5526 18 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55664 443 6 3658 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55694 443 6 3658 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.25 10.1.1.25 55694 443 6 3648 16 7 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.50 10.1.1.50 10.1.1.50 443 36320 6 6724 17 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 1.52 10.1.1.50 10.1.1.50 443 36322 6 10401 18 19 use1-az2 ingress i-0826dea5238644ce7 eni-Offa7e54flae8falb 16.25 10.1.1.50 <td< td=""><td>1.1.50 10.1.1.50 143 52836 6 6708 17 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 17.118.10 10.1.1.50 143 34066 6 9526 18 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.1.50 143 52854 6 1041 19 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 52732 443 6 3586 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 52752 443 6 3632 15 7 use1-az2 ingress +0826dea5238644c7</td><td>1.1.50 10.1.1.50 14.1.50 443 52836 6 6708 17 19 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - 53 1.1.50 10.1.1.50 443 34066 6 9526 18 10 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 53 1.50 10.1.1.50 10.1.55 52732 443 6 3588 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 1.50 10.1.125 10.1.125 5504 443 6 3548 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - <td< td=""><td>1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - useast1 17.118.120 10.1.1.25 5064 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.150 10.1.125 5564 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55694 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55794 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 57574 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54</td><td>1.1.150 10.1.150 143 52836 6 6708 17 19 usel-az2 logges 10826des233644ce7 en-0fa7e54f1ae8fa1b OK - useart - - 17.118.120 10.1.150 10.1.150 443 34066 6 9526 18 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3658 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3624 17 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 55704 443 6 3648 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.55 1.50 10.1.125 55704 443 6 3624 17 19 usel-az2 logges538644ce7</td><td>1.1.50 10.1.1.50 441 5238 6 6708 17 19 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - use-ast-1 - submet-0d7d9632ca72bafe2 17.118.120 10.1.1.50 10.1.1.50 443 5264 443 6 658 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5232 443 6 3688 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 55964 443 6 3688 16 7 usel-ar2 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5233 6 6724 17 19 usel-ar2 legress +0026des523864ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50</td><td>1.1.50 10.1.50 443 52836 6 6708 17 9 9 9 9826de322864de7 0 0 9 u-east1 4 subert-0d76952ar2bafe2 1PM4 17.181.20 10.1.125 5564 443 6 3658 16 7 uetat2 gress 10826de322864de7 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5273 443 6 358 16 7 uetat2 gress 10826de523864de7 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5564 443 6 3246 16 7 uetat2 gress 10826de323864de7 n-0787541ae81ab 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 16 7 uetat2 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 17 9 <</td><td>1.15 10.11.50 10.</td><td>1.150 10.11.50 443 5330 6 67.88 17 10 ucl+az lgeres 1002debc32864ar2 end/frác4flasfta DK 5 uweetat - uwher0d7d953227bal2 IPA 5 0.511 vp 1111 101.125 101.125 5564 443 6 358 10</td></td<></td></td<>	1.1.50 10.1.1.50 143 52836 6 6708 17 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 17.118.10 10.1.1.50 143 34066 6 9526 18 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.1.50 143 52854 6 1041 19 19 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 52732 443 6 3586 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 55704 443 6 3648 16 7 use1-az2 ingress +0826dea5238644c7 eni-Offa7e541ae8fa1b OK - 1.50 10.1.125 10.1.125 52752 443 6 3632 15 7 use1-az2 ingress +0826dea5238644c7	1.1.50 10.1.1.50 14.1.50 443 52836 6 6708 17 19 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - 53 1.1.50 10.1.1.50 443 34066 6 9526 18 10 use1-az ingress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 53 1.50 10.1.1.50 10.1.55 52732 443 6 3588 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - - 1.50 10.1.125 10.1.125 5504 443 6 3548 16 7 use1-az egress i>0826dea5238644ce7 eni-0ffa7e54flae8fa1b OK - <td< td=""><td>1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - useast1 17.118.120 10.1.1.25 5064 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.150 10.1.125 5564 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55694 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55794 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 57574 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54</td><td>1.1.150 10.1.150 143 52836 6 6708 17 19 usel-az2 logges 10826des233644ce7 en-0fa7e54f1ae8fa1b OK - useart - - 17.118.120 10.1.150 10.1.150 443 34066 6 9526 18 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3658 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3624 17 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 55704 443 6 3648 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.55 1.50 10.1.125 55704 443 6 3624 17 19 usel-az2 logges538644ce7</td><td>1.1.50 10.1.1.50 441 5238 6 6708 17 19 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - use-ast-1 - submet-0d7d9632ca72bafe2 17.118.120 10.1.1.50 10.1.1.50 443 5264 443 6 658 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5232 443 6 3688 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 55964 443 6 3688 16 7 usel-ar2 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5233 6 6724 17 19 usel-ar2 legress +0026des523864ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50</td><td>1.1.50 10.1.50 443 52836 6 6708 17 9 9 9 9826de322864de7 0 0 9 u-east1 4 subert-0d76952ar2bafe2 1PM4 17.181.20 10.1.125 5564 443 6 3658 16 7 uetat2 gress 10826de322864de7 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5273 443 6 358 16 7 uetat2 gress 10826de523864de7 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5564 443 6 3246 16 7 uetat2 gress 10826de323864de7 n-0787541ae81ab 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 16 7 uetat2 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 17 9 <</td><td>1.15 10.11.50 10.</td><td>1.150 10.11.50 443 5330 6 67.88 17 10 ucl+az lgeres 1002debc32864ar2 end/frác4flasfta DK 5 uweetat - uwher0d7d953227bal2 IPA 5 0.511 vp 1111 101.125 101.125 5564 443 6 358 10</td></td<>	1.1.50 10.1.1.50 443 52836 6 6708 17 19 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - useast1 17.118.120 10.1.1.25 5064 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.150 10.1.125 5564 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55694 443 6 3658 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 55794 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54f1ae8fa1b OK - us-east1 1.50 10.1.125 10.1.125 57574 443 6 3240 16 7 use1-as2 ingress 1-0826dea5238644cer ni-0ffa7e54	1.1.150 10.1.150 143 52836 6 6708 17 19 usel-az2 logges 10826des233644ce7 en-0fa7e54f1ae8fa1b OK - useart - - 17.118.120 10.1.150 10.1.150 443 34066 6 9526 18 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3658 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 10.1.125 5564 443 6 3624 17 19 usel-az2 logges 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.50 10.1.125 55704 443 6 3648 7 us-east - 10826des2338644ce7 en-0fa7e54f1ae8fa1b OK - us-east - - 1.55 1.50 10.1.125 55704 443 6 3624 17 19 usel-az2 logges538644ce7	1.1.50 10.1.1.50 441 5238 6 6708 17 19 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - use-ast-1 - submet-0d7d9632ca72bafe2 17.118.120 10.1.1.50 10.1.1.50 443 5264 443 6 658 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b 0K - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5232 443 6 3688 16 7 usel-ar21 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 55964 443 6 3688 16 7 usel-ar2 legress +0026des5238644ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50 10.1.125 10.1.125 5233 6 6724 17 19 usel-ar2 legress +0026des523864ce7 enioffa7c54flaeffa1b CK - us-east-1 - submet-0d7d9632ca72bafe2 1.50	1.1.50 10.1.50 443 52836 6 6708 17 9 9 9 9826de322864de7 0 0 9 u-east1 4 subert-0d76952ar2bafe2 1PM4 17.181.20 10.1.125 5564 443 6 3658 16 7 uetat2 gress 10826de322864de7 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5273 443 6 358 16 7 uetat2 gress 10826de523864de7 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 5564 443 6 3246 16 7 uetat2 gress 10826de323864de7 n-0787541ae81ab 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 16 7 uetat2 0 0 u-east1 4 subert-0d76952ar2bafe2 1PM4 1.50 10.1.125 10.1.125 5704 443 6 324 17 9 <	1.15 10.11.50 10.	1.150 10.11.50 443 5330 6 67.88 17 10 ucl+az lgeres 1002debc32864ar2 end/frác4flasfta DK 5 uweetat - uwher0d7d953227bal2 IPA 5 0.511 vp 1111 101.125 101.125 5564 443 6 358 10

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



FloCon 2024 © 2024

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		dstport proto	ocol bytes	packets tcp-fl	ags az-id	flow-direction	instance-id	interface-id	log-status pkt-s	pkt-d reg	gion subs	sub subnet-id	traffic-pa	ath type version	n 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-az	2 egress	i-082987a5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2	1 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	S3 us-	east-1 -	subnet-0d7d9632	ca72bafe2	7 IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK S3	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK S3	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK S3	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	oOK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1	o OK S3	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	o OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad
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-az	2 ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK -	- us-	east-1 -	subnet-0d7d9632	ca72bafe2 -	IPv4	5 9046521234	6 vpc-1544e6fc7e	ab628ad

16.182.72.112	S3
52.216.215.0	S 3
52.217.111.214	S 3
52.217.118.120	S 3
52.217.170.248	S 3
52.217.99.126	S 3
54.231.135.64	S 3
54.231.139.192	S 3

Mellon

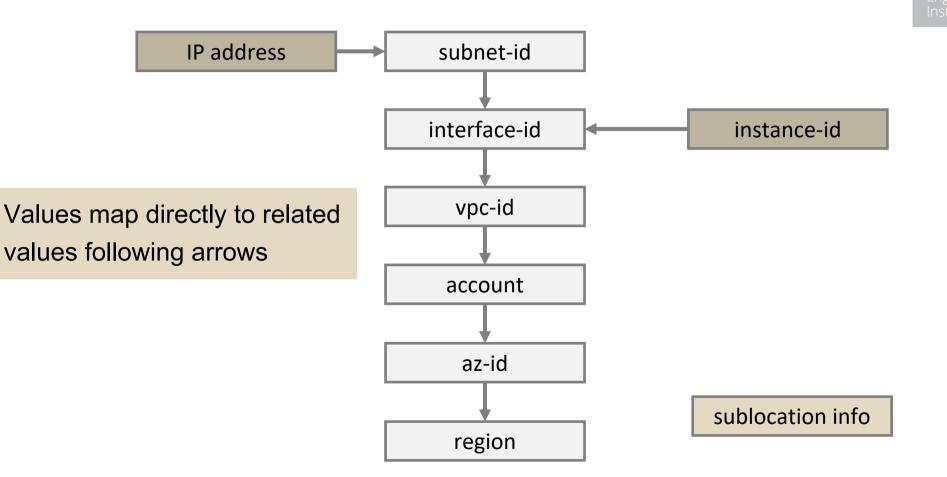
Sorted For Directionality – Internal IP Labeling

Carnegie Mellon
University

srcaddr	pkt-srcaddr	dstaddr	pkt-dstaddr	srcport	dstport	protocol	bytes	packets tcp	flags	az-id	flow-direction	instance-id	interface-id	log-status	s -awsaws-	region	catiatio	subnet-id	traffic-pat	h type v	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 u	se1-az2	egress	i-082987a5238644ce7	eni-Offa7f15f1ae8fa1b	ОК		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	ОК		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	ОК		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	ОК		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK		us-east-1	SU	ubnet-0d7d9632ca72bafe	2 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 <mark>u</mark> :	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK		us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK	- S3	us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	ОК	- S3	us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress		eni-Offa7f15f1ae8fa1b		- S3	us-east-1	su	ubnet-0d7d9632ca72bafe	2 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 u:	se1-az2	egress		eni-Offa7f15f1ae8fa1b		- S3	us-east-1	SU	ubnet-0d7d9632ca72bafe	2 7	IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.50		52.217.118.120				6	3270	16	0 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK	- S3	us-east-1	SU	ubnet-0d7d9632ca72bafe	2 7	IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.50		52.217.118.120			443	6	3259	15	0 u:	se1-az2	egress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK	- S3	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5	9.04652E+11	vpc-1544e6fc7eab628ad
10.1.1.50		54.231.139.192			443	6	3270	16	0 u:	se1-az2	egress		eni-Offa7f15f1ae8fa1b	OK	- S3	us-east-1	SU	ubnet-0d7d9632ca72bafe	2 7	IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.50		52.217.170.248				6	3309	16	0 u:	se1-az2	egress		eni-Offa7f15f1ae8fa1b	OK	- S3	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.50		52.217.99.126				6	3269	15	0 u:	se1-az2	egress		eni-Offa7f15f1ae8fa1b	OK		us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.50	10.1.1.50	52.216.215.0	52.216.215.0	36322		6	3299			se1-az2	egress		eni-Offa7f15f1ae8fa1b		- S3			ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52836	6	6708			se1-az2	ingress		eni-Offa7f15f1ae8fa1b			us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
52.217.118.120		10.1.1.50	10.1.1.50		34066	6	9526			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK	S3 -	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52854	6	10461			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK		us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
52.217.170.248		10.1.1.50	10.1.1.50	443	32806	6	8724			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK	S3 -	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52830	6	6724			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK		us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
52.216.215.0	52.216.215.0	10.1.1.50	10.1.1.50		36322	6	10401			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK	S3 -	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55640	6	10420			se1-az2	ingress		eni-Offa7f15f1ae8fa1b			us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	52780	6	6708			se1-az2	ingress		eni-Offa7f15f1ae8fa1b			us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
	52.217.99.126	10.1.1.50	10.1.1.50	443	45980	6	8600			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK	S3 -	us-east-1		ubnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50		52788	6	6728			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK	1.1	us-east-1		Ibnet-0d7d9632ca72bafe		IPv4	5		vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55664	6	6708			se1-az2	ingress		eni-Offa7f15f1ae8fa1b	OK				Ibnet-0d7d9632ca72bafe		IPv4			vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55668	6	10467			se1-az2	ingress		eni-Offa7f15f1ae8fa1b			us-east-1		ibnet-0d7d9632ca72bafe		IPv4			vpc-1544e6fc7eab628ad
10.1.1.25	10.1.1.25	10.1.1.50	10.1.1.50	443	55662	6	6728	17	L9 u:	se1-az2	ingress	i-0826dea5238644ce7	eni-Offa7f15f1ae8fa1b	OK	1.1	us-east-1	SL	ubnet-0d7d9632ca72bafe	2 -	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	

Further Cloud Field Reduction



Mellon

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

Туре

 dropped as SiLK combines v4 and v6

Version

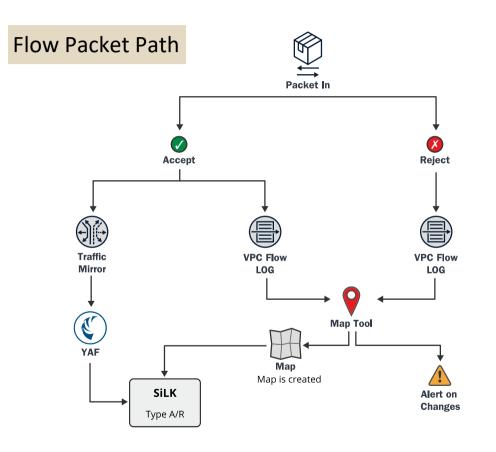
 used for processing, but not analyzing

Convert non-mirrored flows

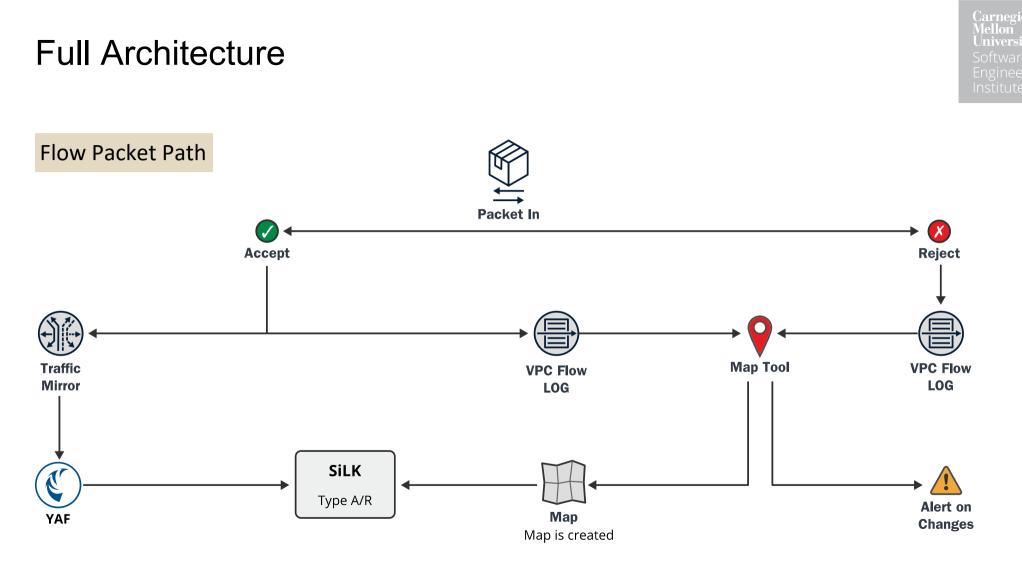
Convert what doesn't come out of sensor to that format, such as SiLK, IPFIX, Zeek.

Primarily "REJECT" packets Choose proper IP addresses from flow logs from a NAT PKT-SRCADDR and PKT-DSTADDR

Architecture



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



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

Carnegie Mellon University Software Engineering Institute

Contact



Dan Ruef Network Situational Awareness Technical Manager

Email: <u>druef@cert.org</u> Email: <u>netsa-help@cert.org</u> Email: <u>info@sei.cmu.edu</u>

FloCon 2024 © 2024