Summary

This article explains the format behind the traffic summaries logs coming out of the Illumio PCE. The article shows a table with all the relevant interesting fields in alphabetic order that could be present depending on the type of traffic. It also includes the possible values that fields can have and some real life example scenarios from Production PCE. After reading this article, Illumio customers and partners will be able to better understand the values of fields from exported traffic summaries. PCE version = 22.5 The following Traffic Flow Summary scenarios are presented: VEN to VEN VEN to FQDN/UMW UMW to VEN VEN MULTICAST VEN BROADCAST VEN ICMP VEN AUS blocked non-admin user VEN AUS allowed admin user VEN = Virtual Enforcement Node UMW = Unmanaged Workload AUD = Adaptive User Segmentation

Description

The following table shows traffic summaries fields with their possible values and data samples.

After this table, you will find some data samples from real traffic for different scenarios

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
class	Transmission Type	U, M, B U: Unicast B: Broadcast M: Multicast	U
code	This value exists only if protocol is ICMP. The ICMP message code (subtype) associated with the first flow in the summary.	See IANA URL below for all possible values for ICMP codes: https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml	0
count	Count of the number of flows in the flow summary.	Integer	7

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
ddms	Delta flow duration in milliseconds: The duration of the aggregate within the current sampling interval. This field enables you to calculate the bandwidth between two applications in a given sampling interval.	Integer	22300
dir	Direction of the first packet	I=first packet of the flow was heading into the system. I=Observed by Provider. O=first packet of the flow was heading out of the system. O=Observerd by Consumer	I
dst_hostname	Hostname of the destination workload that reported the flow	String	UK-WIN-WPROD-A03
dst_href	HREF of the destination workload that	String	/orgs/1/workloads/17284828-5791-4875-b7ab-64ad36219528

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
	reported the flow		
dst_ip	Destination IP of the flows	String	10.60.34.5
dst_labels	Labels applied to the destination workload.	Object Type Labels Can include MT4L (More than 4 labels)	dst_labels: { app: App3 env: Prod loc: UK role: Web os: Win }
dst_port	Destination Port	Minimum = 0 (ICMP) Maximum = 65535	3389
dst_tbi	Destination Total Bytes In	(Value only exists if Byte Count Premium Feature is enabled on PCE) Total bytes received till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes sent by source.	3536
dst_tbo	Destination Total Bytes Out	(Value only exists if Byte Count Premium Feature is enabled on PCE) Total bytes sent till now by the destination over the flows included in this flow-summary in the latest sampled interval. This is the same as bytes received by source.	13562
dst_dbi	Destination Delta Bytes In	(Value only exists if Byte Count Premium Feature is enabled on PCE)	3536

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
		Number of bytes received by destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes sent by source.	
dst_dbo	Destination Delta Bytes Out	(Value only exists if Byte Count Premium Feature is enabled on PCE) Number of bytes sent by the destination in the latest sampled interval, over the flows included in this flow-summary. This is the same as bytes received by source.	13562
fqdn	Fully qualified domain name	String. This field is often only present on outbound traffic to this FQDN from the VEN.	ctldl.windowsupdate.com
interval_sec	Sample duration in seconds for the flows in the summary. Defa ult duration is approximately 600 seconds (10 minutes) depending on the VEN's ability to report traffic	Normally between 540 and 700 seconds	600

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
network	Network Profile	Corporate or External	Corporate
pce_fqdn	The fully qualified domain name of the PCE	String	scp3.illum.io
pd	Policy decision value, which indicates if the flow was allowed, potentially blocked (but allowed), blocked, or unknown.	Possible values: [0,1,2,3] 0 – Allowed traffic 1 – Potentially blocked. Allowed traffic which will be blocked after enforcement 2 – Blocked traffic 3 – Unknown	0
pd_qualifier	Policy Decision Qualifier. This helps the user determine if a flow is blocked due to boundary or lack of segmentation rule	Possible values: [0,1,2,3] 0 – Flow is blocked/potentially blocked due lack of segmentation rule 1 – Flow blocked/potentially blocked due to boundary 2 – Flow blocked/potentially blocked due to an overiden global deny rule 3 – Flow blocked by deny rule not written by Illumio	0
pn	Program name associated with the first flow in the summary. It is supported on inbound	String	svchost.exe

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
	flows for Linux and Windows VEN and on outbound flows for only Windows VEN. This information might not be available on short-lived processes. Currently flows are aggregated, so this value might represent only the first process that was detected across all aggregated flows		
proto	Protocol number (0-255)	Minimum=0 Maximum=255 See IANA URL below for all possible values for protocol numbers: https://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml	6
src_hostname	Hostname of the source workload that reported the flow	String	US-NIX-DBTEST-A06

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
src_href	HREF of the source workload that reported the flow	String	/orgs/1/workloads/23284828-5791-3337-b7ab-64ad12399528
src_ip	Source IP of the flows	String	192.168.26.144
src_labels	Labels applied to the source workload.	Object Type Labels Can include MT4L (More than 4 labels)	src_labels: { app: App6 env: Test loc: US role: DB os: Linux }
state	Session state for the traffic flows in the flow summaries.	A, C, T, S, N Active (A): Connection was still open at the time the flow summary was logged. Applies to allowed and potentially blocked flows. Closed (C): (Linux only) Connection closed at the time the flow summary was logged. Applies to allowed and potentially blocked flows Timed out (T): Connection timed out at the time the flow summary was logged. Applies to allowed and potentially blocked flows. Due to a limitation of WFP, a Windows VEN will report "T" even when the connection is closed at the time the flow summary was logged. Snapshot (S): SSnapshot of current	T

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
		connections to and from the VEN, which applies only to workloads whose policy state is set to Idle. Applies to allowed and potentially blocked flows New connection (N): Dropped TCP packet contains a SYN and is associated with a new connection. Applies to blocked TCP flows. The value is empty for blocked UDP flows.	
tdms	Total flow duration in milliseconds (tdms): The duration of the aggregate across all sampling intervals. This field enables you to calculate the average bandwidth of a connection between two applications.	Integer	85921997
timestamp	Indicates the time (RFC3339) when the first flow in the summary was created,	yyyy-MM-dd'T'HH:mm:ssZ	2023-02-10T16:21:38Z

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
	represented in UTC.		
type	This value exists only if protocol is ICMP. The ICMP message type associated with the first flow in the summary	See IANA URL below for all possible values for ICMP types: https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml	8
un	User name associated with the first flow in the summary. It is supported on inbound flows for Linux and Windows VEN and on outbound flows for only Linux VEN. On Windows, it can include the username of the user account that initiated the connection.	String NOTE: This information might not be available on short-lived processes	rdpagentuser
version	Version of the flow summary	Integer	4

Field Name	**Description**	**Possible Values**	**Sample value from production PCE**
	schema.		

Details

VEN to VEN traffic data sample

Allowed DNS request from US-NIX-DBTEST-A06 to UK-WIN-WPROD-A03
Labels from both VENs can be seen below on src_labels and dst_labels fields.

VEN to FQDN/UMW traffic data sample

Blocked HTTP request from US-NIX-DBTEST-A06 to FQDN ctdtl.windows.update.com
Labels from source VEN can be seen below on src_labels field.

UMW to VEN traffic data sample

Allowed HTTPS traffic from source IP 10.100.122.91 to UK-WIN-WPROD-A03
Labels from destination VEN can be seen below on dst_labels field.

VEN MULTICAST traffic data sample

Allowed Multicast DHCP Request from source US-NIX-DBTEST-A06
Labels from source VEN can be seen below on src_labels field.

VEN BROADCAST traffic data sample

Allowed Broadcast NetBIOS Request from source US-NIX-DBTEST-A06
Labels from source VEN can be seen below on src_labels field.

VEN ICMP traffic data sample

Allowed ICMP Request to destination UK-WIN-WPROD-A03
dst_port is 0 because protocol is 1 (ICMP)
Labels from destination VEN can be seen below on dst_labels field.
type=8 and code=0 means that this ICMP traffic contains 7 flows of an Echo ICMP Request

VEN Adaptive User Segmentation traffic data sample
(not admin user is blocked)

Blocked RDP request to WINADFS2016 from user salva-test0 logged in on Win10-Endpoint
Labels from both VENs can be seen below on src_labels and dst_labels fields.
On this Windows VEN, the "un" field includes the username of the user account that initiated the connection.
This is how Adaptive User Segmentation works. Rulesets are implemented based on the User Group ID from AD
As you can see user is not an admin (salva-test0). For that reason, traffic is blocked.

VEN Adaptive User Segmentation traffic data sample
(admin user is allowed)

Allowed RDP request to WINADFS2016 from user salva-admin logged in on Win10-Endpoint
Labels from both VENs can be seen below on src_labels and dst_labels fields.

On this Windows VEN, the "un" field includes the username of the user account that initiated the connection.

This is how Adaptive User Segmentation works. Rulesets are implemented based on the User Group ID from AD

As you can see user is an admin (salva-admin). For that reason, traffic is allowed.