Splunk® Common Information Model Add-on Common Information Model Add-on Manual 5.3.2

Network Traffic

Generated: 6/06/2024 2:30 pm

Network Traffic

The fields and tags in the Network Traffic data model describe flows of data across network infrastructure components.

Note: A **dataset** is a component of a data model. In versions of the Splunk platform prior to version 6.5.0, these were referred to as data model objects.

Difference between Network Traffic and Intrusion Detection data models

Both Network Traffic and Intrusion Detection data models describe the network traffic "allow" and "deny" events.

However the network traffic in the Network Traffic data model is allowed or denied based on simple network connection rules, which are using network parameters such as TCP headers, destination, ports, and so on. These rules are usually triggered when the network connection is being established.

The network traffic in the Intrusion Detection data model is allowed or denied based on more complex traffic patterns. Traffic is continuously monitored by the Intrusion Detection systems and may be denied passage in the middle of an existing connection based on known signatures or bad traffic patterns.

Tags used with Network Traffic event datasets

The following tags act as constraints to identify your events as being relevant to this data model. For more information, see How to use these reference tables.

Dataset name	Tag name
All_Traffic	network
	communicate

Fields for Network Traffic event datasets

The following table lists the extracted and calculated fields for the event datasets in the model. Note that it does not include any inherited fields. For more information, see How to use these reference tables.

The key for using the column titled "Notes" or "Abbreviated list of example values" is as follows:

- **Recommended**: Add-on developers make their best effort attempts to map these event fields. If these fields are not populated, then the event is not very useful.
- **Required**: Add-on developers must map these event fields when using the pytest-splunk-addon to test for CIM compatibility. See pytest-splunk-addon documentation.
- **Prescribed values**: Permitted values that can populate the fields, which Splunk is using for a particular purpose. Other valid values exist, but Splunk is not relying on them.
- **Other values**: Other example values that you might see.

For even more examples, see NetworkTrafficFieldMapping.

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	`action`	string	The action taken by the network device.	• recommended

Dataset name	Field name	Data type	Description	Abbreviated list of example values
				• required for pytest-splunk-addon • prescribed values: `allowed` `blocked`, `teardown`
All_Traffic	`app`	string	The application protocol of the traffic.	required for pytest-splunk-addon
All_Traffic	`bytes`	number	Total count of bytes handled by this device/interface (`bytes_in + bytes_out`).	recommended
All_Traffic	`bytes_in`	number	How many bytes this device/interface received.	recommended
All_Traffic	`bytes_out`	number	How many bytes this device/interface transmitted.	recommended
All_Traffic	`channel`	number	The 802.11 channel used by a wireless network.	
All_Traffic	`dest`	string	The destination of the network traffic (the remote host). You can **alias** this from more specific fields, such as `dest_host`, `dest_ip`, or `dest_name`.	• recommended • required for pytest-splunk-addon
All_Traffic	`dest_bunit`	string	colspan="2" rowspan="2"These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	`dest_category`	string		
All_Traffic	`dest_interface`	string	The interface that is listening remotely or receiving packets locally. Can also be referred to as the "egress interface."	
All_Traffic	`dest_ip`	string	The IP address of the destination.	
All_Traffic	`dest_mac`	string	The destination TCP/IP layer 2 Media Access Control (MAC) address of a packet's destination, such as `06:10:9f:eb:8f:14`. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Traffic	`dest_port`	number	The destination port of the network traffic. **Note:** Do not translate the values of this field to strings (`tcp/80` is `80`, not `http`). You can set up the corresponding string value in a `dest_svc` field by extending the data model.	recommended
All_Traffic	`dest_priority`	string	The destination priority, if applicable. This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	`dest_translated_ip`	string	The NATed IPv4 or IPv6 address to which a packet has been sent.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	dest_translated_port	number	The NATed port to which a packet has been sent. **Note:** Do not translate the values of this field to strings (tcp/80 is 80, not http).	
All_Traffic	dest_zone	string	The network zone of the destination.	required for pytest-splunk-addon
All_Traffic	direction	string	The direction the packet is traveling.	prescribed values: inbound, outbound
All_Traffic	duration	number	The amount of time for the completion of the network event, in seconds.	
All_Traffic	dvc	string	The device that reported the traffic event. You can **alias** this from more specific fields, such as dvc_host, dvc_ip, or dvc_name.	• recommended • required for pytest-splunk-addon
All_Traffic	dvc_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	dvc_category	string		
All_Traffic	dvc_ip	string	The ip address of the device.	
All_Traffic	dvc_mac	string	The device TCP/IP layer 2 Media Access Control (MAC) address of a packet's destination, such as 06:10:9f:eb:8f:14. Note: Always force lower case on this field and use colons instead of dashes, spaces, or no separator.	
All_Traffic	dvc_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	dvc_zone	string	The network zone of the device.	
All_Traffic	flow_id	string	Unique identifier for this traffic stream, such as a netflow, jflow, or cflow.	
All_Traffic	icmp_code	string	The RFC 2780 or RFC 4443 human-readable code value of the traffic, such as Destination Unreachable or Parameter Problem . See the ICMP Type Numbers and the ICMPv6 Type Numbers.	
All_Traffic	icmp_type	number	The RFC 2780 or RFC 4443 numeric value of the traffic. See the ICMP Type Numbers and the ICMPv6 Type Numbers.	prescribed values: 0 to 254
All_Traffic	packets	number	The total count of packets handled by this device/interface (packets_in + packets_out).	
All_Traffic	packets_in	number	The total count of packets received by this device/interface.	
All_Traffic	packets_out	number	The total count of packets transmitted by this device/interface.	
All_Traffic	process_id	string	The numeric identifier of the process (PID) or service generating the network traffic.	

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	protocol	string	The OSI layer 3 (network) protocol of the traffic observed, in lower case. For example, ip, appletalk, ipx.	
All_Traffic	protocol_version	string	Version of the OSI layer 3 protocol.	
All_Traffic	response_time	number	The amount of time it took to receive a response in the network event, if applicable.	
All_Traffic	rule	string	The rule that defines the action that was taken in the network event. **Note:** This is a string value. Use a rule_id field for rule fields that are integer data types. The rule_id field is optional, so it is not included in this table.	recommended
All_Traffic	session_id	string	The session identifier. Multiple transactions build a session.	
All_Traffic	src	string	The source of the network traffic (the client requesting the connection). You can **alias** this from more specific fields, such as src_host, src_ip, or src_name.	• recommended • required for pytest-splunk-addon
All_Traffic	src_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	src_category	string		
All_Traffic	src_interface	string	The interface that is listening locally or sending packets remotely. Can also be referred to as the "ingress interface."	
All_Traffic	src_ip	string	The ip address of the source.	
All_Traffic	src_mac	string	The source TCP/IP layer 2 Media Access Control (MAC) address of a packet's destination, such as 06:10:9f:eb:8f:14. **Note:** Always force lower case on this field. **Note:** Always use colons instead of dashes, spaces, or no separator.	
All_Traffic	src_port	number	The source port of the network traffic. **Note:** Do not translate the values of this field to strings (tcp/80 is 80, not http). You can set up the corresponding string value in the src_svc field.	recommended
All_Traffic	src_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	src_translated_ip	string	The NATed IPv4 or IPv6 address from which a packet has been sent..	required for pytest-splunk-addon
All_Traffic	src_translated_port	number	The NATed port from which a packet has been sent. **Note:** Do not translate the values of this field to strings (tcp/80 is 80, not http).	
All_Traffic	src_zone	string	The network zone of the source.	required for pytest-splunk-addon

Dataset name	Field name	Data type	Description	Abbreviated list of example values
All_Traffic	ssid	string	The 802.11 service set identifier (ssid) assigned to a wireless session.	
All_Traffic	tag	string	This automatically generated field is used to access tags from within data models. Do not define extractions for this field when writing add-ons.	
All_Traffic	tcp_flag	string	The TCP flag(s) specified in the event.	prescribed values: SYN, ACK, FIN, RST, URG, or PSH.
All_Traffic	transport	string	The OSI layer 4 (transport) or internet layer protocol of the traffic observed, in lower case.	• recommended • required for pytest-splunk-addon • prescribed values: icmp, tcp, udp
All_Traffic	tos	string	The combination of source and destination IP ToS (type of service) values in the event.	
All_Traffic	ttl	number	The "time to live" of a packet or diagram.	
All_Traffic	user	string	The user that requested the traffic flow.	recommended
All_Traffic	user_bunit	string	These fields are automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for these fields when writing add-ons.	
All_Traffic	user_category	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	user_priority	string	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.	
All_Traffic	vendor_account	string	The account associated with the network traffic. The account represents the organization, or a Cloud customer or a Cloud account.	
All_Traffic	vendor_product	string	The vendor and product of the device generating the network event. This field can be automatically populated by vendor and product fields in your data.	recommended
All_Traffic	vlan	string	The virtual local area network (VLAN) specified in the record.	
All_Traffic	wifi	string	The wireless standard(s) in use, such as 802.11a, 802.11b, 802.11g, or 802.11n.	