Cisco Secure Network Analytics

Information Elements 7.5.1

Information Elements for Secure Network Analytics v7.5.1

The following is a list of NetFlow/IPFIX Information Elements handled by the Flow Collector:

For more information on Information Elements, refer to https://www.iana.org/assignments/ipfix/ipfix.xhtml.

Element ID	Name	Description
1	octetDeltaCount	The number of octets since the previous report (if any) in incoming packets for this Flow at the Observation Point. The number of octets includes IP header(s) and IP payload.
2	packetDeltaCount	The number of incoming packets since the previous report (if any) for this Flow at the Observation Point.
4	protocolIdentifier	The value of the protocol number in the IP packet header. The protocol number identifies the IP packet payload type. Protocol numbers are defined in the IANA Protocol Numbers registry. In Internet Protocol version 4 (IPv4), this is carried in the Protocol field. In Internet Protocol version 6 (IPv6), this is carried in the Next Header field in the last extension header of

Element ID	Name	Description
		the packet.
5	ipClassOfService	For IPv4 packets, this is the value of the TOS field in the IPv4 packet header. For IPv6 packets, this is the value of the Traffic Class field in the IPv6 packet header.
6	tcpControlBits	TCP control bits observed for the packets of this Flow. This information is encoded as a bit field; for each TCP control bit, there is a bit in this set. The bit is set to 1 if any observed packet of this Flow has the corresponding TCP control bit set to 1. The bit is cleared to 0 otherwise.
7	sourceTransportPort	The source port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the source port number given in the respective header. This field MAY also be used for future transport protocols that have 16-bit source port identifiers.
8	sourceIPv4Address	The IPv4 source address in the IP packet header.
10	ingressInterface	The index of the IP interface where packets of this Flow are being received.

Element ID	Name	Description
11	destinationTransportPort	The destination port identifier in the transport header. For the transport protocols UDP, TCP, and SCTP, this is the destination port number given in the respective header. This field MAY also be used for future transport protocols that have 16-bit destination port identifiers.
12	destinationIPv4Address	The IPv4 destination address in the IP packet header.
14	egressInterface	The index of the IP interface where packets of this Flow are being sent.
15	ipNextHopIPv4Address	The IPv4 address of the next IPv4 hop.
16	bgpSourceAsNumber	The autonomous system (AS) number of the source IP address. If AS path information for this Flow is only available as an unordered AS set (and not as an ordered AS sequence), then the value of this Information Element is 0.
17	bgpDestinationAsNumber	The autonomous system (AS) number of the destination IP address. If AS path information for this Flow is only available as an unordered AS set (and not as an ordered AS sequence), then

Element ID	Name	Description
		the value of this Information Element is 0.
18	bgpNextHopIPv4Address	The IPv4 address of the next (adjacent) BGP hop.
21	flowEndSysUpTime	The relative timestamp of the last packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.
22	flowStartSysUpTime	The relative timestamp of the first packet of this Flow. It indicates the number of milliseconds since the last (re-)initialization of the IPFIX Device (sysUpTime). sysUpTime can be calculated from systemInitTimeMilliseconds.
27	sourceIPv6Address	The IPv6 source address in the IP packet header.
28	destinationIPv6Address	The IPv6 destination address in the IP packet header.
32	icmpTypeCodeIPv4	Type and Code of the IPv4 ICMP message. The combination of both values is reported as (ICMP type * 256) +

Element ID	Name	Description
		ICMP code.
34	samplingInterval	When using sampled NetFlow, the rate at which packets are sampled -- e.g., a value of 100 indicates that one of every 100 packets is sampled.
48	samplerId	The unique identifier associated with samplerName.
50	samplerRandomInterval	Packet interval at which to sample -- in case of random sampling. Used in connection with the samplerMode 0x02 (random sampling) value.
52	minimumTTL	Minimum TTL value observed for any packet in this Flow.
53	maximumTTL	Maximum TTL value observed for any packet in this Flow.
56	sourceMacAddress	The IEEE 802 source MAC address field.
57	postDestinationMacAddress	The definition of this Information Element is identical to the definition of Information Element 'destinationMacAddress', except that it reports a potentially modified value caused by a middlebox function after the packet passed the Observation Point.

Element ID	Name	Description
58	vlanId	Virtual LAN identifier associated with ingress interface.

61	flowDirection	The direction of the Flow observed at the Observation Point. There are only two values defined:
		`0x00: ingress flow`
		`0x01: egress flow`

70	mplsTopLabelStackSection	The Label, Exp, and S fields from the top MPLS label stack entry, i.e., from the last label that was pushed.
71	mplsLabelStackSection2	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsTopLabelStackSection.
72	mplsLabelStackSection3	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection2.
73	mplsLabelStackSection4	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection3.

Element ID	Name	Description
74	mplsLabelStackSection5	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection4.
75	mplsLabelStackSection6	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection5.
76	mplsLabelStackSection7	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection6.
77	mplsLabelStackSection8	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection7.
78	mplsLabelStackSection9	The Label, Exp, and S fields from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection8.
79	mplsLabelStackSection10	The Label, Exp, and S fields

Element ID	Name	Description
		from the label stack entry that was pushed immediately before the label stack entry that would be reported by mplsLabelStackSection9.
85	octetTotalCount	The total number of octets in incoming packets for this Flow at the Observation Point since the Metering Process (re-)initialization for this Observation Point. The number of octets includes IP header(s) and IP payload.
95	applicationId	Specifies an Application ID per Cisco Systems Export of Application Information in IPFIX.
139	icmpTypeCodeIPv6	Type and Code of the IPv6 ICMP message. The combination of both values is reported as (ICMP type * 256) + ICMP code.
148	flowID	An identifier of a Flow that is unique within an Observation Domain. This Information Element can be used to distinguish between different Flows if Flow Keys such as IP addresses and port numbers are not reported or are reported in separate records.
150	flowStartSeconds	The absolute timestamp of the

Element ID	Name	Description
		first packet of this Flow.
151	flowEndSeconds	The absolute timestamp of the last packet of this Flow.
152	flowStartMilliseconds	The absolute timestamp of the first packet of this Flow.
153	flowEndMilliseconds	The absolute timestamp of the last packet of this Flow.
154	flowStartMicroseconds	The absolute timestamp of the first packet of this Flow.
155	flowEndMicroseconds	The absolute timestamp of the last packet of this Flow.
156	flowStartNanoseconds	The absolute timestamp of the first packet of this Flow.
157	flowEndNanoseconds	The absolute timestamp of the last packet of this Flow.
158	flowStartDeltaMicroseconds	This is a relative timestamp only valid within the scope of a single IPFIX Message. It contains the negative time offset of the first observed packet of this Flow relative to the export time specified in the IPFIX Message Header.
159	flowEndDeltaMicroseconds	This is a relative timestamp only valid within the scope of a single IPFIX Message. It contains the negative time offset of the last observed

Element ID	Name	Description
		packet of this Flow relative to the export time specified in the IPFIX Message Header.
160	systemInitTimeMilliseconds	The absolute timestamp of the last (re-)initialization of the IPFIX Device.
176	icmpTypeIPv4	Type of the IPv4 ICMP message.
177	icmpCodeIPv4	Code of the IPv4 ICMP message.
178	icmpTypeIPv6	Type of the IPv6 ICMP message.
179	icmpCodeIPv6	Code of the IPv6 ICMP message.
180	udpSourcePort	The source port identifier in the UDP header.
181	udpDestinationPort	The destination port identifier in the UDP header.
182	tcpSourcePort	The source port identifier in the TCP header.
183	tcpDestinationPort	The destination port identifier in the TCP header.
192	ipTTL	For IPv4, the value of the Information Element matches the value of the Time to Live (TTL) field in the IPv4 packet header. For IPv6, the value of

Element ID	Name	Description
		the Information Element matches the value of the Hop Limit field in the IPv6 packet header.
195	ipDiffServCodePoint	The value of a Differentiated Services Code Point (DSCP) encoded in the Differentiated Services field. The Differentiated Services field spans the most significant 6 bits of the IPv4 TOS field or the IPv6 Traffic Class field, respectively. This element encodes only the 6 bits of the Differentiated Services field. Therefore, its value may range from 0 to 63.
218	tcpSynTotalCount	The total number of packets of this Flow with TCP "Synchronize sequence numbers" (SYN) flag set.
219	tcpFinTotalCount	The total number of packets of this Flow with TCP "No more data from sender" (FIN) flag set.
220	tcpRstTotalCount	The total number of packets of this Flow with TCP "Reset the connection" (RST) flag set.
222	tcpAckTotalCount	The total number of packets of this Flow with TCP "Acknowledgment field significant" (ACK) flag set.

Element ID	Name	Description
223	tcpUrgTotalCount	The total number of packets of this Flow with TCP "Urgent Pointer field significant" (URG) flag set.
225	postNATSourceIPv4Address	The definition of this Information Element is identical to the definition of Information Element 'sourceIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
226	postNATDestinationIPv4Address	The definition of this Information Element is identical to the definition of Information Element 'destinationIPv4Address', except that it reports a modified value caused by a NAT middlebox function after the packet passed the Observation Point.
227	postNAPTSourceTransportPort	The definition of this Information Element is identical to the definition of Information Element 'sourceTransportPort', except that it reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.

Element ID	Name	Description
228	postNAPTDestinationTransportPort	The definition of this Information Element is identical to the definition of Information Element 'destinationTransportPort', except that it reports a modified value caused by a Network Address Port Translation (NAPT) middlebox function after the packet passed the Observation Point.
230	natEvent	This Information Element identifies a NAT event. This IE identifies the type of a NAT event. Examples of NAT events include, but are not limited to, NAT translation create, NAT translation delete, Threshold Reached, or Threshold Exceeded, etc. Values for this Information Element are listed in the NAT Event Type registry.
231	initiatorOctets	The total number of layer 4 payload bytes in a flow from the initiator since the previous report. The initiator is the device which triggered the session creation, and remains the same for the life of the session.
232	responderOctets	The total number of layer 4 payload bytes in a flow from the responder since the previous

Element ID	Name	Description
		report. The responder is the device which replies to the initiator, and remains the same for the life of the session.
233	firewallEvent	Indicates a firewall event. The allowed values are: 0 - Ignore (invalid) 1 - Flow Created 2 - Flow Deleted 3 - Flow Denied 4 - Flow Alert 5 - Flow Update
239	biflowDirection	A description of the direction assignment method used to assign the Biflow Source and Destination. This Information Element MAY be present in a Flow Data Record, or applied to all flows exported from an Exporting Process or Observation Domain using IPFIX Options. If this Information Element is not present in a Flow Record or associated with a Biflow via scope, it is assumed that the configuration of the direction assignment method is done out-of-band. Note that when using IPFIX Options to apply this Information Element to all flows within an

Element ID	Name	Description
		Observation Domain or from an Exporting Process, the Option SHOULD be sent reliably. If reliable transport is not available (i.e., when using UDP), this Information Element SHOULD appear in each Flow Record.
281	postNATSourceIPv6Address	The definition of this Information Element is identical to the definition of Information Element 'sourceIPv6Address', except that it reports a modified value caused by a NAT64 middlebox function after the packet passed the Observation Point.
282	postNATDestinationIPv6Address	The definition of this Information Element is identical to the definition of Information Element 'destinationIPv6Address', except that it reports a modified value caused by a NAT64 middlebox function after the packet passed the Observation Point.
313	ipHeaderPacketSection	This Information Element carries a series of n octets from the IP header of a sampled packet, starting sectionOffset octets into the IP header.

Element ID	Name	Description
314	ipPayloadPacketSection	This Information Element carries a series of n octets from the IP payload of a sampled packet, starting sectionOffset octets into the IP payload.
323	observationTimeMilliseconds	This Information Element specifies the absolute time in milliseconds of an observation.
346	privateEnterpriseNumber	A private enterprise number, as assigned by IANA. Within the context of an Information Element Type record, this element can be used along with the informationElementId element to scope properties to a specific Information Element. To export type information about an IANA-assigned Information Element, set the privateEnterpriseNumber to 0, or do not export the privateEnterpriseNumber in the type record. To export type information about an enterprise-specific Information Element, export the enterprise number in privateEnterpriseNumber, and export the Information Element number with the Enterprise bit cleared in informationElementId. The Enterprise bit in the associated informationElementId

Element ID	Name	Description
		Information Element MUST be ignored by the Collecting Process.
371	userName	User name associated with the flow.
1232	TrustSecSourceIdentifierIPFIX PEN(9)	Cisco PEN (PrivateEnterpriseNumber) field containing the TrustSec Identifier of the source host.
1233	TrustSecDestinationIdentifierIPFIX PEN(9)	Cisco PEN field containing the TrustSec Identifier of the destination host.
9292	AVCResponsesCountDeltaIPFIX	AVC (Application Visibility and Control) Responses Count Delta field for IPFIX. Used in determining RTT and SRT.
9303	AVCSummaryResponseTimeIPFIX	AVC Summary Response Time field for IPFIX. SRT field. Dividing this field by the AVCResponsesCountDeltaIPFIX field yields RTT.
9306	AVCSummaryServerResponseTime	AVC Summary Server Response Time field for IPFIX. Dividing this field by the AVCResponsesCountDeltaIPFIX field yields SRT.
12235	AVCSubApplicationValueIPFIX PEN(9)	Cisco NBAR2 field that identifies the application used with the flow. It can also contain

Element ID	Name	Description
		host and URL information which the Flow Collector pulls out and attaches to a Secure Network Analytics flow.
12172	NF_F_ETTA_INITIAL_DATA_PACKET_IPFIX	ETA IDP field containing the payload of the initial data packet sent in a flow. Used to grab URLs and other information prior to the connection becoming encrypted.
12173	NF_F_ETTA_SEQUENCE_OF_PACKET_LENGTHS_AND_TIMES_IPFIX	ETA SPLT field containing packet lengths and times of encrypted sessions.
12174	NF_F_ETTA_SEQUENCE_OF_APPLICATION_LENGTHS_AND_TIMES_IPFIX	ETA SALT field containing application lengths and times of encrypted sessions.
12177	NF_F_ETTA_TLS_RECORDS_IPFIX	ETA TLS records field containing arrays that describe the first N records of a TLS flow.
12178	NF_F_ETTA_TLS_CIPHER_SUITES_IPFIX	ETA TLS cipher suites field containing a list of up to N cipher suites offered by the client or selected by the server in a TLS flow.
12179	NF_F_ETTA_TLS_EXTENSIONS_IPFIX	ETA TLS extensions field describing the TLS extensions observed in the Hello message for a TLS flow.

Element ID	Name	Description
12180	NF_F_ETTA_TLS_VERSION_IPFIX	ETA TLS version field containing the TLS version number observed in the TLS Hello message for a flow
12181	NF_F_ETTA_TLS_KEY_LENGTH_IPFIX	ETA TLS key length field containing the length of the client key observed in the TLS ClientKeyExchange message.
12182	NF_F_ETTA_TLS_SESSION_ID_IPFIX	ETA TLS session ID field containing the session ID value observed (if any) in the TLS Hello message for a flow
12183	NF_F_ETTA_TLS_RANDOM_IPFIX	ETA TLS random field containing the random value observed in the TLS Hello message for this flow.
12192	NF_F_ETTA_TLS_EXTENSION_ LENGTHS_IPFIX	ETA TLS extension lengths field containing a list of extension lengths for up to the first N TLS extensions observed in the TLS Hello message for a flow.
12193	NF_F_ETTA_TLS_EXTENSION_TYPES_ IPFIX	ETA TLS extension types field containing a list of extension types for up to the first N TLS extensions observed in the TLS Hello message for a flow.
16386	ETAInitialDataPacket	ETA (Encrypted Traffic Analysis) IDP (Initial Data Packet) field. Field containing the payload of the initial data packet sent in a

Element ID	Name	Description
		flow. Used to grab URLs and other information prior to the connection becoming encrypted.
16387	ETASequenceofPktLengthsandTimes	ETA SLPT (Sequence of Packet Lengths and Times) field. Packet lengths and times of encrypted sessions.
29794	FlowSensorInitiator PEN(8712:Lancope)	Lancope FlowSensor PEN field that indicates which side of the flow initiated the conversation. 0x00: Initiator Unknown 0x01: Initiator is IP0 0x02: Initiator is IP1
29795	FlowSensorTCPSYNACKTotalCount PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of SYN/ACK packets encountered in the flow
29796	FlowSensorTCPSRSTotalCount PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of soft resets encountered in the flow. These are resets that are used to terminate a session versus the normal FIN approach.
29797	FlowSensorRoundTripTime PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the Round Trip Time computed in the flow.
29798	FlowSensorServerResponseTime PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains Server Response Time computed in the flow.

Element ID	Name	Description
29799	FlowSensorRetransmits PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of retransmits seen in the flow.
29800	FlowSensorTCPBadTotalCount PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of bad flag combinations seen in the flow.
29801	FlowSensorTCPFragTotalCount PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of fragmented packets seen in the flow.
29802	FlowSensorSourceEmailIn PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email addresses received by the source host of the flow.
29803	FlowSensorSourceEmailOut PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email addresses sent by the source host of the flow.
29804	FlowSensorSourceEmailInMessages PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email messages successfully received by the source host of the flow.
29805	FlowSensorSourceEmailOutMessages PEN(8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email messages successfully sent by the source host of the flow.

Element ID	Name	Description
29806	FlowSensorSourceEmailInTrys PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email message attempts received by the source host of the flow.
29807	FlowSensorSourceEmailOutTrys PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email message attempts sent by the source host of the flow.
29808	FlowSensorDestinationEmailIn PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email addresses received by the destination host of the flow.
29809	FlowSensorDestinationEmailOut PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email addresses sent by the destination host of the flow.
29810	FlowSensorDestinationEmailInMessages PEN(8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email messages successfully received by the destination host of the flow.
29811	FlowSensorDestinationEmailOutMessages PEN(8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email messages successfully sent by the destination host of the flow.
29812	FlowSensorDestinationEmailInTrys PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email message attempts sent

Element ID	Name	Description
		by the destination host of the flow.
29813	FlowSensorDestinationEmailOutTrys PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the number of email message attempts sent by the destination host of the flow.
29814	FlowSensorTraces PEN(8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets encountered in the flow where the TTL was below 2 and that ICMP TimeOuts were encountered.
29817	FlowSensorEmbeddedICMPProtocol PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the protocol of an embedded ICMP packet encountered in the flow.
29818	FlowSensorEmbeddedICMPType PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the ICMP Type field of an embedded ICMP packet encountered in the flow.
29819	FlowSensorEmbeddedICMPCode PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the ICMP Code field of an embedded ICMP packet encountered in the flow.
29820	FlowSensorApplicationIdentifier PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the application identifier of the application detected in the flow.

Element ID	Name	Description
29821	FlowSensorBadFlagXmas PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of Xmas (All flags set) flag combinations seen in the flow.
29822	FlowSensorBadFlagSYNFIN PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets with both the SYN and FIN flags set seen in the flow.
29823	FlowSensorBadFlagBadRST PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets with the RST flag set in invalid situations in the flow.
29824	FlowSensorBadFlagNoACK PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets without the ACK flag set when it should be in the flow.
29825	FlowSensorBadFlagURG PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets with the URG flag set in invalid situations in the flow.
29826	FlowSensorBadFlagNoFlag PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of packets with no flags set in the flow.
29828	FlowSensorShortFragAttack PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of short fragments in the flow.
29829	FlowSensorFragPacketTooShort PEN (8712:Lancope)	Lancope FlowSensor PEN field

Element ID	Name	Description
		that contains the count of fragments that are too short in the flow.
29830	FlowSensorFragPacketTooLong PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the count of fragments that are too long in the flow.
29831	FlowSensorFragPacketDifferentSizes PEN(8712:Lancope)	Lancope FlowSensor PEN field that contains the count of fragments of different sizes used in the flow.
29832	FlowSensorApplicationDetails PEN (8712:Lancope)	Lancope FlowSensor PEN overloaded field that contains either first packet payload information or the details of the detected application being used in the flow.
29833	FlowSensorTrustsecSourceIdentifier PEN (8712:Lancope)	Lancope FlowSensor PEN field that contains the Trustsec Identifier of the source host.
29844	EndpointFlowProcessAccount	Endpoint field that contains the user account running the EndpointFlowProcessName.
29845	EndpointFlowProcessName	Endpoint field that contains the name of the current process running.
29846	EndpointFlowProcessHash	Endpoint field that contains the hash of the current process running.

Element ID	Name	Description
29847	EndpointFlowParentProcessAccount	Endpoint field that contains the user account of the parent of the process running the EndpointFlowProcessName.
29848	EndpointFlowParentProcessName	Endpoint field that contains the name of the parent of the process running the EndpointFlowProcessName.
29849	EndpointFlowParentProcessHash	Endpoint field that contains the hash of the parent of the process running the EndpointFlowProcessName.
33002	ASAFirewallExtendedEvent	Cisco ASA Firewall Extended Event 0 – Ignore 1001 – Flow denied by an ingress ACL 1002 – Flow denied by an egress ACL 1003 – Flow denied an attempt to connect to an interface service 1004 – Flow denied since first packet not a TCP SYN 1005–1999 – Undocumented 2000+ – Flow deleted
34000	TrustSecSourceIdentifier	Cisco field containing the Trustsec Identifier of the source host.

Element ID	Name	Description
34001	TrustSecDestinationIdentifier	Cisco field containing the Trustsec Identifier of the destination host.
34002	TrustSecSourceName	Cisco field containing the Trustsec Name of the source host.
34003	TrustSecDestinationName	Cisco field containing the Trustsec Name of the destination host.
40000	ASAUsername	Cisco ASA Firewall username field indicating the user's name in the flow.
40001	ASAXlateSourceAddressIPV4	Cisco ASA NAT source address IPV4.
40002	ASAXlateDestinationAddressIPV4	Cisco ASA NAT destination address IPV4.
40003	ASAXlateSourcePort	Cisco ASA NAT translated source port.
40004	ASAXlateDestinationPort	Cisco ASA NAT translated destination port.
41105	ART_Server_Bytes	Byte and packet count for all the server packets (Layer 3).
41106	ART_Client_Bytes	Byte and packet count for all the client packets (Layer 3).
42040	AVCResponsesCountDelta	AVC Responses Count Delta field. Used in determining RTT and SRT.

Element ID	Name	Description
42071	AVCSummaryResponseTime	AVC Summary Response Time field. Dividing this field by the AVCResponsesCountDelta field yields RTT.
42074	AVCSummaryServerResponseTime	AVC Summary Server Response Time field. Dividing this field by the AVCResponsesCountDelta field yields SRT.
44940	ETAInitialDataPacket	ETA IDP field. Field containing the payload of the initial data packet sent in a flow. Used to grab URLs and other information prior to the connection becoming encrypted.
44941	ETASequenceofPktLengthsandTimes	ETA SLPT field. Packet lengths and times of encrypted sessions.
44944	ETAByteDistribution	ETA BD (Byte Distribution) field. Byte distributions of encrypted sessions.
45003	AVCSubApplicationValue	Cisco NBAR2 field that identifies the application used with the flow. It can also contain host and URL information which the FlowCollector pulls out and attaches to a Secure Network Analytics flow.
45004	AVC_Client_IPV4_Address	The IPv4 client address in the IP

Element ID	Name	Description
		packet header. This may be the source or destination IP address, depending on the first packet of the connection. The client is the device that triggered the session creation, and remains the same for the life of the session.
45005	AVC_Server_IPV4_Address	The IPv4 server address in the IP packet header. The server is the device that replies to the client, and remains the same for the life of the session.
45006	AVC_Client_IPV6_Address	The IPv6 client address in the IP packet header. The client is the device that triggered the session creation, and remains the same for the life of the session.
45007	AVC_Server_IPV6_Address	IPv6 server address in the IP packer header. The server is the device that replies to the client, and remains the same for the life of the session.
45008	AVC_Client_Transport_Port	Client transport port identifier. This may be the source or destination transport port. The client is the device that triggered the session creation, and remains the same for the life of the session.

Element ID	Name	Description
45009	AVC_Server_Transport_Port	Server transport port identifier. This may be the source or destination transport port. The server is the device that replies to the client, and remains the same for the life of the session.
56701	PaloAltoApplicationIdentifier PEN(25461)	Palo Alto PEN field that contains the Palo Alto application identifier being used in the flow.
56702	PaloAltoUserIdentifier PEN(25461)	Palo Alto PEN field that contains the Palo Alto user's name in the flow.

Contacting Support

If you need technical support, please do one of the following:

- Contact your local Cisco Partner
- Contact Cisco Support
- To open a case by web: http://www.cisco.com/c/en/us/support/index.html
- To open a case by email: tac@cisco.com
- For phone support: 1-800-553-2447 (U.S.)
- For worldwide support numbers: https://www.cisco.com/c/en/us/support/web/tsd-cisco-worldwide-contacts.html

Change History

Document Version	Published Date	Description
1_0	August 15, 2024	Initial version.

Copyright Information